Tell us about your PDF experience.

Windows Commands

Article • 04/26/2023

All supported versions of Windows and Windows Server have a set of Win32 console commands built in. This set of documentation describes the Windows Commands you can use to automate tasks by using scripts or scripting tools.

Command-line shells

Windows has two command-line shells: the Command shell and PowerShell. Each shell is a software program that provides direct communication between you and the operating system or application, providing an environment to automate IT operations.

The Command shell was the first shell built into Windows to automate routine tasks, like user account management or nightly backups, with batch (.bat) files. With Windows Script Host, you could run more sophisticated scripts in the Command shell. For more information, see cscript or wscript. You can perform operations more efficiently by using scripts than you can by using the user interface. Scripts accept all commands that are available at the command line.

PowerShell was designed to extend the capabilities of the Command shell to run PowerShell commands called cmdlets. Cmdlets are similar to Windows Commands but provide a more extensible scripting language. You can run both Windows Commands and PowerShell cmdlets in PowerShell, but the Command shell can only run Windows Commands and not PowerShell cmdlets.

For the most robust, up-to-date Windows automation, we recommend using PowerShell instead of Windows Commands or Windows Script Host for Windows automation.

A reference of exit and error codes for Windows Commands can be found in the Debug system error codes articles that may be helpful to understanding errors produced. Windows Commands also include command redirection operators. To learn more of their use, see Using command redirection operators.

> **Note**
>
> You can also download and install **PowerShell Core**, the open source version of PowerShell.

Command shell file and directory name automatic completion

You can configure the Command shell to automatically complete file and directory names on a computer or user session when a specified control character is pressed. By default this control character is configured to be the **tab** key for both file and directory names, although they can be different. To change this control character, run `regedit.exe` and navigate to either of the following registry keys and entries, depending on whether you wish to change the value for the current user only, or for all users of the computer.

> **⊗ Caution**
>
> Incorrectly editing the registry may severely damage your system. Before making the following changes to the registry, you should back up any valued data on the computer.

registry

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\PathCompletionChar
```

Set these values to that of the control character you wish to use. See virtual key codes for a complete list. To disable a particular completion character in the registry, use the value for **space** (0x20) as it isn't a valid control character. The type of value for this registry entry is REG_DWORD, and can also be specified by hexadecimal or decimal value.

You can also enable or disable file and directory name completion per instance of a Command shell by running `cmd.exe` with the parameter and switch `/F:ON` or `/F:OFF`. If name completion is enabled with the `/F:ON` parameter and switch, the two control characters used are `Ctrl-D` for directory name completion and `Ctrl-F` for file name completion. User-specified settings take precedence over computer settings, and command-line options take precedence over registry settings.

Command-line reference A-Z

To find information about a specific command, in the following A-Z menu, select the letter that the command starts with, and then select the command name.

A

- active
- add
- add alias
- add volume
- append
- arp
- assign
- assoc
- at
- atmadm
- attach-vdisk
- attrib
- attributes
  - attributes disk
  - attributes volume
- auditpol
  - auditpol backup
  - auditpol clear
  - auditpol get
  - auditpol list
  - auditpol remove
  - auditpol resourcesacl
  - auditpol restore
  - auditpol set
- autochk
- autoconv
- autofmt
- automount

B

- bcdboot
- bcdedit
- bdehdcfg
  - bdehdcfg driveinfo
  - bdehdcfg newdriveletter

    - bdehdcfg quiet
    - bdehdcfg restart
    - bdehdcfg size
    - bdehdcfg target
- begin backup
- begin restore
- bitsadmin
    - bitsadmin addfile
    - bitsadmin addfileset
    - bitsadmin addfilewithranges
    - bitsadmin cache
        - bitsadmin cache and delete
        - bitsadmin cache and deleteurl
        - bitsadmin cache and getexpirationtime
        - bitsadmin cache and getlimit
        - bitsadmin cache and help
        - bitsadmin cache and info
        - bitsadmin cache and list
        - bitsadmin cache and setexpirationtime
        - bitsadmin cache and setlimit
        - bitsadmin cache and clear
    - bitsadmin cancel
    - bitsadmin complete
    - bitsadmin create
    - bitsadmin examples
    - bitsadmin getaclflags
    - bitsadmin getbytestotal
    - bitsadmin getbytestransferred
    - bitsadmin getclientcertificate
    - bitsadmin getcompletiontime
    - bitsadmin getcreationtime
    - bitsadmin getcustomheaders
    - bitsadmin getdescription
    - bitsadmin getdisplayname
    - bitsadmin geterror
    - bitsadmin geterrorcount
    - bitsadmin getfilestotal
    - bitsadmin getfilestransferred
    - bitsadmin gethelpertokenflags
    - bitsadmin gethelpertokensid

- bitsadmin gethttpmethod
- bitsadmin getmaxdownloadtime
- bitsadmin getminretrydelay
- bitsadmin getmodificationtime
- bitsadmin getnoprogresstimeout
- bitsadmin getnotifycmdline
- bitsadmin getnotifyflags
- bitsadmin getnotifyinterface
- bitsadmin getowner
- bitsadmin getpeercachingflags
- bitsadmin getpriority
- bitsadmin getproxybypasslist
- bitsadmin getproxylist
- bitsadmin getproxyusage
- bitsadmin getreplydata
- bitsadmin getreplyfilename
- bitsadmin getreplyprogress
- bitsadmin getsecurityflags
- bitsadmin getstate
- bitsadmin gettemporaryname
- bitsadmin gettype
- bitsadmin getvalidationstate
- bitsadmin help
- bitsadmin info
- bitsadmin list
- bitsadmin listfiles
- bitsadmin makecustomheaderswriteonly
- bitsadmin monitor
- bitsadmin nowrap
- bitsadmin peercaching
  - bitsadmin peercaching and getconfigurationflags
  - bitsadmin peercaching and help
  - bitsadmin peercaching and setconfigurationflags
- bitsadmin peers
  - bitsadmin peers and clear
  - bitsadmin peers and discover
  - bitsadmin peers and help
  - bitsadmin peers and list
- bitsadmin rawreturn
- bitsadmin removeclientcertificate

    - bitsadmin removecredentials
    - bitsadmin replaceremoteprefix
    - bitsadmin reset
    - bitsadmin resume
    - bitsadmin setaclflag
    - bitsadmin setclientcertificatebyid
    - bitsadmin setclientcertificatebyname
    - bitsadmin setcredentials
    - bitsadmin setcustomheaders
    - bitsadmin setdescription
    - bitsadmin setdisplayname
    - bitsadmin sethelpertoken
    - bitsadmin sethelpertokenflags
    - bitsadmin sethttpmethod
    - bitsadmin setmaxdownloadtime
    - bitsadmin setminretrydelay
    - bitsadmin setnoprogresstimeout
    - bitsadmin setnotifycmdline
    - bitsadmin setnotifyflags
    - bitsadmin setpeercachingflags
    - bitsadmin setpriority
    - bitsadmin setproxysettings
    - bitsadmin setreplyfilename
    - bitsadmin setsecurityflags
    - bitsadmin setvalidationstate
    - bitsadmin suspend
    - bitsadmin takeownership
    - bitsadmin transfer
    - bitsadmin util
        - bitsadmin util and enableanalyticchannel
        - bitsadmin util and getieproxy
        - bitsadmin util and help
        - bitsadmin util and repairservice
        - bitsadmin util and setieproxy
        - bitsadmin util and version
    - bitsadmin wrap
- bootcfg
    - bootcfg addsw
    - bootcfg copy
    - bootcfg dbg1394

    - bootcfg debug
    - bootcfg default
    - bootcfg delete
    - bootcfg ems
    - bootcfg query
    - bootcfg raw
    - bootcfg rmsw
    - bootcfg timeout
- break

C

- cacls
- call
- cd
- certreq
- certutil
- change
    - change logon
    - change port
    - change user
- chcp
- chdir
- chglogon
- chgport
- chgusr
- chkdsk
- chkntfs
- choice
- cipher
- clean
- cleanmgr
- clip
- cls
- cmd
- cmdkey
- cmstp
- color
- comp
- compact

- compact vdisk
- convert
  - convert basic
  - convert dynamic
  - convert gpt
  - convert mbr
- copy
- create
  - create partition efi
  - create partition extended
  - create partition logical
  - create partition msr
  - create partition primary
  - create volume mirror
  - create volume raid
  - create volume simple
  - create volume stripe
- cscript

D

- date
- dcdiag
- dcgpofix
- defrag
- del
- delete
  - delete disk
  - delete partition
  - delete shadows
  - delete volume
- detach vdisk
- detail
  - detail disk
  - detail partition
  - detail vdisk
  - detail volume
- dfsdiag
  - dfsdiag testdcs
  - dfsdiag testdfsconfig

    - dfsdiag testdfsintegrity
    - dfsdiag testreferral
    - dfsdiag testsites
- dfsrmig
- diantz
- dir
- diskcomp
- diskcopy
- diskpart
- diskperf
- diskraid
- diskshadow
- dispdiag
- dnscmd
- doskey
- driverquery

E

- echo
- edit
- endlocal
- end restore
- erase
- eventcreate
- Evntcmd
- exec
- exit
- expand
- expand vdisk
- expose
- extend
- extract

F

- fc
- filesystems
- find
- findstr

- finger
- flattemp
- fondue
- for
- forfiles
- format
- freedisk
- fsutil
  - fsutil 8dot3name
  - fsutil behavior
  - fsutil dirty
  - fsutil file
  - fsutil fsinfo
  - fsutil hardlink
  - fsutil objectid
  - fsutil quota
  - fsutil repair
  - fsutil reparsepoint
  - fsutil resource
  - fsutil sparse
  - fsutil tiering
  - fsutil transaction
  - fsutil usn
  - fsutil volume
  - fsutil wim
- ftp
  - ftp append
  - ftp ascii
  - ftp bell
  - ftp binary
  - ftp bye
  - ftp cd
  - ftp close
  - ftp debug
  - ftp delete
  - ftp dir
  - ftp disconnect
  - ftp get
  - ftp glob
  - ftp hash

    - ftp lcd
    - ftp literal
    - ftp ls
    - ftp mget
    - ftp mkdir
    - ftp mls
    - ftp mput
    - ftp open
    - ftp prompt
    - ftp put
    - ftp pwd
    - ftp quit
    - ftp quote
    - ftp recv
    - ftp remotehelp
    - ftp rename
    - ftp rmdir
    - ftp send
    - ftp status
    - ftp trace
    - ftp type
    - ftp user
    - ftp verbose
    - ftp mdelete
    - ftp mdir
- ftype
- fveupdate

G

- getmac
- gettype
- goto
- gpfixup
- gpresult
- gpt
- gpupdate
- graftabl

H

- help
- helpctr
- hostname

I

- icacls
- if
- import (shadowdisk)
- import (diskpart)
- inactive
- ipconfig
- ipxroute
- irftp

J

- jetpack

K

- klist
- ksetup
  - ksetup addenctypeattr
  - ksetup addhosttorealmmap
  - ksetup addkdc
  - ksetup addkpasswd
  - ksetup addrealmflags
  - ksetup changepassword
  - ksetup delenctypeattr
  - ksetup delhosttorealmmap
  - ksetup delkdc
  - ksetup delkpasswd
  - ksetup delrealmflags
  - ksetup domain
  - ksetup dumpstate
  - ksetup getenctypeattr
  - ksetup listrealmflags
  - ksetup mapuser
  - ksetup removerealm

- ksetup server
- ksetup setcomputerpassword
- ksetup setenctypeattr
- ksetup setrealm
- ksetup setrealmflags
- ktmutil
- ktpass

L

- label
- list
  - list providers
  - list shadows
  - list writers
- load metadata
- lodctr
- logman
  - logman create
  - logman create alert
  - logman create api
  - logman create cfg
  - logman create counter
  - logman create trace
  - logman delete
  - logman import and logman export
  - logman query
  - logman start and logman stop
  - logman update
  - logman update alert
  - logman update api
  - logman update cfg
  - logman update counter
  - logman update trace
- logoff
- lpq
- lpr

M

- macfile
- makecab
- manage bde
  - manage bde status
  - manage bde on
  - manage bde off
  - manage bde pause
  - manage bde resume
  - manage bde lock
  - manage bde unlock
  - manage bde autounlock
  - manage bde protectors
  - manage bde tpm
  - manage bde setidentifier
  - manage bde forcerecovery
  - manage bde changepassword
  - manage bde changepin
  - manage bde changekey
  - manage bde keypackage
  - manage bde upgrade
  - manage bde wipefreespace
- mapadmin
- md
- merge vdisk
- mkdir
- mklink
- mmc
- mode
- more
- mount
- mountvol
- move
- mqbkup
- mqsvc
- mqtgsvc
- msdt
- msg
- msiexec
- msinfo32
- mstsc

N

- nbtstat
- netcfg
- netdom
- net print
- netsh
- netstat
- nfsadmin
- nfsshare
- nfsstat
- nlbmgr
- nltest
- nslookup
  - nslookup exit Command
  - nslookup finger Command
  - nslookup help
  - nslookup ls
  - nslookup lserver
  - nslookup root
  - nslookup server
  - nslookup set
  - nslookup set all
  - nslookup set class
  - nslookup set d2
  - nslookup set debug
  - nslookup set domain
  - nslookup set port
  - nslookup set querytype
  - nslookup set recurse
  - nslookup set retry
  - nslookup set root
  - nslookup set search
  - nslookup set srchlist
  - nslookup set timeout
  - nslookup set type
  - nslookup set vc
  - nslookup view
- ntbackup
- ntcmdprompt
- ntfrsutl

O

- offline
  - offline disk
  - offline volume
- online
  - online disk
  - online volume
- openfiles

P

- pagefileconfig
- path
- pathping
- pause
- pbadmin
- pentnt
- perfmon
- ping
- pktmon
- pnpunattend
- pnputil
- popd
- powershell
- powershell ise
- print
- prncnfg
- prndrvr
- prnjobs
- prnmngr
- prnport
- prnqctl
- prompt
- pubprn
- pushd
- pushprinterconnections
- pwlauncher
- pwsh

Q

- qappsrv
- qprocess
- query
  - query process
  - query session
  - query termserver
  - query user
- quser
- qwinsta

R

- rd
- rdpsign
- recover
- recover disk group
- refsutil
- reg
  - reg add
  - reg compare
  - reg copy
  - reg delete
  - reg export
  - reg import
  - reg load
  - reg query
  - reg restore
  - reg save
  - reg unload
- regini
- regsvr32
- relog
- rem
- remove
- ren
- rename
- repadmin
- repair

    - repair bde
- replace
- rescan
- reset
    - reset session
- retain
- revert
- rexec
- risetup
- rmdir
- robocopy
- route ws2008
- rpcinfo
- rpcping
- rsh
- rundll32
- rundll32 printui
- rwinsta

S

- san
- sc config
- sc create
- sc delete
- sc query
- schtasks
- scwcmd
    - scwcmd analyze
    - scwcmd configure
    - scwcmd register
    - scwcmd rollback
    - scwcmd transform
    - scwcmd view
- secedit
    - secedit analyze
    - secedit configure
    - secedit export
    - secedit generaterollback
    - secedit import

    - secedit validate
- select
    - select disk
    - select partition
    - select vdisk
    - select volume
- serverceipoptin
- servermanagercmd
- serverweroptin
- set environmental variables
- set shadow copy
    - set context
    - set id
    - setlocal
    - set metadata
    - set option
    - set verbose
- setx
- sfc
- shadow
- shift
- showmount
- shrink
- shutdown
- simulate restore
- sort
- start
- subcommand set device
- subcommand set drivergroup
- subcommand set drivergroupfilter
- subcommand set driverpackage
- subcommand set image
- subcommand set imagegroup
- subcommand set server
- subcommand set transportserver
- subcommand set multicasttransmission
- subcommand start namespace
- subcommand start server
- subcommand start transportserver
- subcommand stop server

- subcommand stop transportserver
- subst
- sxstrace
- sysocmgr
- systeminfo

T

- takeown
- tapicfg
- taskkill
- tasklist
- tcmsetup
- telnet
  - telnet close
  - telnet display
  - telnet open
  - telnet quit
  - telnet send
  - telnet set
  - telnet status
  - telnet unset
- tftp
- time
- timeout
- title
- tlntadmn
- tpmtool
- tpmvscmgr
- tracerpt
- tracert
- tree
- tscon
- tsdiscon
- tsecimp
- tskill
- tsprof
- type
- typeperf
- tzutil

U

- unexpose
- uniqueid
- unlodctr

V

- ver
- verifier
- verify
- vol
- vssadmin
  - vssadmin delete shadows
  - vssadmin list shadows
  - vssadmin list writers
  - vssadmin resize shadowstorage

W

- waitfor
- wbadmin
  - wbadmin delete catalog
  - wbadmin delete systemstatebackup
  - wbadmin disable backup
  - wbadmin enable backup
  - wbadmin get disks
  - wbadmin get items
  - wbadmin get status
  - wbadmin get versions
  - wbadmin restore catalog
  - wbadmin start backup
  - wbadmin start recovery
  - wbadmin start sysrecovery
  - wbadmin start systemstatebackup
  - wbadmin start systemstaterecovery
  - wbadmin stop job
- wdsutil
- wecutil
- wevtutil

- where
- whoami
- winnt
- winnt32
- winrs
- winsat mem
- winsat mfmedia
- wmic
- writer
- wscript

X

- xcopy

Command-line syntax key

Article • 09/08/2023

The following table describes the notation used to indicate command-line syntax.

Notation	Description
Text without brackets or braces	Items you must type as shown.
`<Text inside angle brackets>`	Placeholder for which you must supply a value.
`[Text inside square brackets]`	Optional items.
`{Text inside braces}`	Set of required items. You must choose one.
Vertical bar (`|`)	Separator for mutually exclusive items. You must choose one.
Ellipsis (`...`)	Items that can be repeated and used multiple times.

Commands by Server role

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

A server role describes the primary function of the server. Administrators can choose to dedicate an entire server to one role, or install multiple server roles and sub-roles on a single computer. Each role might include additional command-line tools, installed as part of the role. The following topics provide a list of commands associated with each server role.

- Print Command Reference
- Services for Network File System Command Reference
- Remote Desktop Services (Terminal Services) Command Reference
- Windows Server Backup Command Reference

Print command-line tool reference

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Information and links to each of the associated print command-line tools:

Command	Description
lpq	Displays the status of a print queue on a computer running Line printer Daemon (LPD).
lpr	Sends a file to a computer or printer sharing device running the Line printer Daemon (LPD) service in preparation for printing.
Net print	Displays information about a specified printer queue, displays information about a specified print job, or controls a specified print job.
print	Sends a text file to a printer.
prncnfg	Configures or displays configuration information about a printer.
prndrvr	Adds, deletes, and lists printer drivers.
prnjobs	Pauses, resumes, cancels, and lists print jobs.
prnmngr	Adds, deletes, and lists printers or printer connections, in addition to setting and displaying the default printer.
prnport	Creates, deletes, and lists standard TCP/IP printer ports, in addition to displaying and changing port configuration.
prnqctl	Prints a test page, pauses or resumes a printer, and clears a printer queue.
pubprn	Publishes a printer to the active directory directory service.
rundll32 printui.dll,printUIEntry	Enables you to automate the installation and configuration of printers using scripts or the command prompt.

Services for Network File System command-line tools

Article • 02/03/2023

Services for Network File System (NFS) provides a file sharing solution that lets you transfer files between computers running Windows Server and UNIX operating systems using the NFS protocol.

Information and links to each of the associated NFS command-line tools:

Command	Description
mapadmin	Manage User Name Mapping for Microsoft Services for Network File System.
mount	Mount Network File System (NFS) network shares.
nfsadmin	Manage Server for NFS and Client for NFS.
nfsshare	Control Network File System (NFS) shares.
nfsstat	Display or reset counts of calls made to Server for NFS.
rpcinfo	List programs on remote computers.
showmount	Display mounted directories.

Related links

- Command-Line Syntax Key

Remote Desktop Services (Terminal Services) command-line tools reference

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Learn about the available Remote Desktop Services (Terminal Services) command-line tools, with descriptions and links for more detailed information.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Command	Description
change	Changes the Remote Desktop Session Host server settings for sign in, COM port mappings, and install mode.
change logon	Enables or disables logons from client sessions on an Remote Desktop Session Host server, or displays current logon status.
change port	Lists or changes the COM port mappings to be compatible with MS-DOS applications.
change user	Changes the install mode for the Remote Desktop Session Host server.
chglogon	Enables or disables logons from client sessions on an Remote Desktop Session Host server, or displays current logon status.
chgport	Lists or changes the COM port mappings to be compatible with MS-DOS applications.
chgusr	Changes the install mode for the Remote Desktop Session Host server.
flattemp	Enables or disables flat temporary folders.
logoff	Signs out a user from a session on an Remote Desktop Session Host server and deletes the session from the server.
msg	Sends a message to a user on an Remote Desktop Session Host server.

Command	Description
mstsc	Creates connections to Remote Desktop Session Host servers or other remote computers.
qappsrv	Displays a list of all Remote Desktop Session Host servers on the network.
qprocess	Displays information about processes that are running on an Remote Desktop Session Host server.
query	Displays information about processes, sessions, and Remote Desktop Session Host servers.
query process	Displays information about processes that are running on an Remote Desktop Session Host server.
query session	Displays information about sessions on an Remote Desktop Session Host server.
query termserver	Displays a list of all Remote Desktop Session Host servers on the network.
query user	Displays information about user sessions on an Remote Desktop Session Host server.
quser	Displays information about user sessions on an Remote Desktop Session Host server.
qwinsta	Displays information about sessions on an Remote Desktop Session Host server.
rdpsign	Enables you to digitally sign a Remote Desktop Protocol (.rdp) file.
reset session	Enables you to reset (delete) a session on an Remote Desktop Session Host server.
rwinsta	Enables you to reset (delete) a session on an Remote Desktop Session Host server.
shadow	Enables you to remotely control an active session of another user on an Remote Desktop Session Host server.
tscon	Connects to another session on an Remote Desktop Session Host server.
tsdiscon	Disconnects a session from an Remote Desktop Session Host server.
tskill	Ends a process running in a session on an Remote Desktop Session Host server.
tsprof	Copies the Remote Desktop Services user configuration information from one user to another.

Related links

- Command-Line Syntax Key

Windows Server Backup Command Reference

Article • 03/03/2021

The following subcommands for **wbadmin** provide backup and recovery functionality from a command prompt.

To configure a backup schedule, you must be a member of the **Administrators** group. To perform all other tasks with this command, you must be a member of the **Backup Operators** or the **Administrators** group, or you must have been delegated the appropriate permissions.

You must run **wbadmin** from an elevated command prompt. (To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.)

Subcommand	Description
Wbadmin enable backup	Configures and enables a daily backup schedule.
Wbadmin disable backup	Disables your daily backups.
Wbadmin start backup	Runs a one-time backup. If used with no parameters, uses the settings from the daily backup schedule.
Wbadmin stop job	Stops the currently running backup or recovery operation.
Wbadmin get versions	Lists details of backups recoverable from the local computer or, if another location is specified, from another computer.
Wbadmin get items	Lists the items included in a specific backup.
Wbadmin start recovery	Runs a recovery of the volumes, applications, files, or folders specified.
Wbadmin get status	Shows the status of the currently running backup or recovery operation.
Wbadmin get disks	Lists disks that are currently online.
Wbadmin start systemstaterecovery	Runs a system state recovery.
Wbadmin start systemstatebackup	Runs a system state backup.

Subcommand	Description
Wbadmin delete systemstatebackup	Deletes one or more system state backups.
Wbadmin start sysrecovery	Runs a recovery of the full system (at least all the volumes that contain the operating system's state). This subcommand is only available if you are using the Windows Recovery Environment.
Wbadmin restore catalog	Recovers a backup catalog from a specified storage location in the case where the backup catalog on the local computer has been corrupted.
Wbadmin delete catalog	Deletes the backup catalog on the local computer. Use this command only if the backup catalog on this computer is corrupted and you have no backups stored at another location that you can use to restore the catalog.

Adprep

Article • 04/23/2024

Applies to: Windows Server (All supported versions)

The adprep command extends the Active Directory schema and updates permissions as necessary to prepare a forest and domain for a domain controller that runs Windows Server.

`Adprep.exe` is a command-line tool available in Windows Server. You must run **adprep** from an elevated command prompt. To open an elevated command prompt, select **Start**, right-select **Command Prompt**, and then select **Run as administrator**.

Adprep is available in a 32-bit version and a 64-bit version. The 64-bit version runs by default. If you need to run Adprep on a 32-bit computer, run the 32-bit version (Adprep32.exe).

For more information about running `Adprep.exe` and how to resolve errors that can occur when you run it, see Running Adprep.exe.

For examples of how this command can be used, see Examples.

For more information about running `adprep /forestprep`, see Prepare a Windows 2000 or Windows Server 2003 Forest Schema for a Domain Controller that Runs Windows Server 2008 or Windows Server 2008 R2.

For more information about running `adprep /domainprep /gpprep`, see Prepare a Windows 2000 or Windows Server 2003 Domain for a Domain Controller That Runs Windows Server 2008 or Windows Server 2008 R2.

For more information about running `adprep /rodcprep`, see Prepare a Forest for a Read-Only Domain Controller.

Syntax

adprep {/forestprep | /domainprep | /domainprep /gpprep | /rodcprep | /wssg | /silent }

Parameters

Expand table

Parameter	Description
/forestprep	Prepares a forest for the introduction of a domain controller that runs Windows Server. You run this command only once in the forest. You must run this command on the domain controller that holds the schema operations master role (also known as flexible single master operations or FSMO) for the forest. You must be a member of all the following groups to run this command: • The Enterprise Admins group • The Schema Admins group • The Domain Admins group of the domain that hosts the schema master
/domainprep	Prepares a domain for the introduction of a domain controller that runs Windows Server. You run this command after the **forestprep** command finishes and after the changes replicate to all the domain controllers in the forest. Run this command in each domain where you plan to add a domain controller that runs Windows Server. You must run this command on the domain controller that holds the infrastructure operations master role for the domain. You must be a member of the Domain Admins group to run this command.
/domainprep /gpprep	Performs similar updates to **domainprep**. However, this command also provides updates that are necessary to enable the Resultant Set of Policy (RSOP) Planning Mode functionality. In Active Directory environments that run Microsoft Windows, this command performs updates during off-peak hours. Replicating updates to file system permissions and Active Directory permissions on existing Group Policy objects (GPOs) during off-peak hours minimizes replication traffic. Run this command after the **forestprep** command finishes and after the changes replicate to all domain controllers in the forest. You must run this command on the infrastructure master for the domain. For more information about running this command in Windows Active Directory environments, see Prepare Your Infrastructure for Upgrade.
/rodcprep	This parameter updates permissions on the application directory partitions to enable replication of the partitions to read-only domain controllers (RODCs). This operation runs remotely; it contacts the infrastructure master in each domain to update the permissions. You need to run this command only once in the forest. However, you can rerun this command anytime if it fails to complete successfully because an infrastructure master isn't available. You can run this command on any computer in the forest. You must be a member of the Enterprise Admins group to run this command.
/wssg	Returns an expanded set of exit codes, instead of just 0 (Success) and 1 (Failure).
/silent	Specifies that no standard output is returned from an operation. This parameter can be used only if /wssg is also used.

Parameter	Description
quit	Returns to the prior menu.
Help	Displays Help for this command.
?	Displays Help for this command.

Remarks

- To prepare an existing Windows or Windows Server Active Directory environment for a Windows Server domain controller, run the version of adprep included in the Windows Server installation media.
- You can also perform verification steps before and after you run the **adprep** command to help ensure that the operations complete successfully. For more information, see Steps for Extending the Schema.

Exit Codes

The following table lists exit codes that Adprep can return after an operation completes.

Expand table

Return Code	Description
1	Failure
2	Schema conflict error
3	FSMO role error
4	Connection error
5	Schema upgrade error
6	Unable to modify error
7	Server busy error
8	Permission error
9	Unable to initialize log file error
10	Not a domain controller
11	In nonnative mode

Return Code	Description
12	Need to run forest update first
13	Forest update already done
14	Domain update already done
15	GPO update already done
16	Forest update wait replication

Examples

The following example prepares a forest for a domain controller that runs Windows Server:

```cli
adprep /forestprep
```

The following example prepares a domain for a domain controller that runs Windows Server:

```cli
adprep /domainprep
```

The following example prepares a domain for an RODC:

```cli
adprep /rodcprep
```

See also

Command-Line Syntax Key

append

Article • 02/03/2023

Allows programs to open data files in specified directories as if they were in the current directory. If used without parameters, **append** displays the appended directory list.

> **Note**
>
> This command not supported in Windows 10.

Syntax

```
append [[<drive>:]<path>[;...]] [/x[:on|:off]] [/path:[:on|:off] [/e]
append ;
```

Parameters

Parameter	Description
`[\<drive>:]<path>`	Specifies a drive and directory to append.
/x:on	Applies appended directories to file searches and launching applications.
/x:off	Applies appended directories only to requests to open files. The **/x:off** option is the default setting.
/path:on	Applies appended directories to file requests that already specify a path. **/path:on** is the default setting.
/path:off	Turns off the effect of **/path:on**.
/e	Stores a copy of the appended directory list in an environment variable named APPEND. **/e** may be used only the first time you use **append** after starting your system.
;	Clears the appended directory list.
/?	Displays help at the command prompt.

Examples

To clear the appended directory list, type:

```
append ;
```

To store a copy of the appended directory to an environment variable named *append*, type:

```
append /e
```

Related links

- Command-Line Syntax Key

arp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays and modifies entries in the Address Resolution Protocol (ARP) cache. The ARP cache contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer. Used without parameters, **arp** displays help information.

Syntax

```
arp [/a [<inetaddr>] [/n <ifaceaddr>]] [/g [<inetaddr>] [-n <ifaceaddr>]]
[/d <inetaddr> [<ifaceaddr>]] [/s <inetaddr> <etheraddr> [<ifaceaddr>]]
```

Parameters

Parameter	Description
`[/a [<inetaddr>] [/n <ifaceaddr>]`	Displays current arp cache tables for all interfaces. The **/n** parameter is case-sensitive. To display the arp cache entry for a specific IP address, use **arp /a** with the **inetaddr** parameter, where **inetaddr** is an IP address. If **inetaddr** is not specified, the first applicable interface is used. To display the arp cache table for a specific interface, use the **/n ifaceaddr** parameter in conjunction with the **/a** parameter where **inetaddr** is the IP address assigned to the interface.
`[/g [<inetaddr>] [/n <ifaceaddr>]`	Identical to **/a**.
`[/d <inetaddr> [<ifaceaddr>]`	Deletes an entry with a specific IP address, where **inetaddr** is the IP address. To delete an entry in a table for a specific interface, use the **ifaceaddr** parameter where **ifaceaddr** is the IP address assigned to the interface. To delete all entries, use the asterisk (*) wildcard character in place of **inetaddr**.

Parameter	Description
`[/s <inetaddr> <etheraddr> [<ifaceaddr>]`	Adds a static entry to the arp cache that resolves the IP address **inetaddr** to the physical address **etheraddr**. To add a static arp cache entry to the table for a specific interface, use the **ifaceaddr** parameter where **ifaceaddr** is an IP address assigned to the interface.
/?	Displays help at the command prompt.

Remarks

- The IP addresses for **inetaddr** and **ifaceaddr** are expressed in dotted decimal notation.
- The physical address for **etheraddr** consists of six bytes expressed in hexadecimal notation and separated by hyphens (for example, 00-AA-00-4F-2A-9C).
- Entries added with the **/s** parameter are static and do not time out of the arp cache. The entries are removed if the TCP/IP protocol is stopped and started. To create permanent static arp cache entries, place the appropriate **arp** commands in a batch file and use Scheduled Tasks to run the batch file at startup.

Examples

To display the arp cache tables for all interfaces, type:

```
arp /a
```

To display the arp cache table for the interface that is assigned the IP address *10.0.0.99*, type:

```
arp /a /n 10.0.0.99
```

To add a static arp cache entry that resolves the IP address *10.0.0.80* to the physical address *00-AA-00-4F-2A-9C*, type:

```
arp /s 10.0.0.80 00-AA-00-4F-2A-9C
```

Related links

- Command-Line Syntax Key

assoc

Article • 02/03/2023

Displays or modifies file name extension associations. If used without parameters, **assoc** displays a list of all the current file name extension associations.

> **Note**
>
> This command is only supported within cmd.exe and is not available from PowerShell. Though you can use `cmd /c assoc` as a workaround.

Syntax

```
assoc [<.[ext]>[=[<filetype>]]]
```

Parameters

Parameter	Description
`<.ext>`	Specifies the file name extension.
`<filetype>`	Specifies the file type to associate with the specified file name extension.
/?	Displays help at the command prompt.

Remarks

- To make changes in associations, you need administrator privileges.
- To remove the file type association for a file name extension, add a white space after the equal sign by pressing the SPACEBAR.
- To associate files without extension to a file type, use just a dot (see the examples).
- To view current file types that have open command strings defined, use the **ftype** command.
- To redirect the output of **assoc** to a text file, use the `>` redirection operator.

Examples

To view the current file type association for the file name extension .txt, type:

```
assoc .txt
```

To remove the file type association for the file name extension .bak, type:

```
assoc .bak=
```

> ⓘ **Note**
>
> Make sure you add a space after the equal sign.

To view the output of **assoc** one screen at a time, type:

```
assoc | more
```

To send the output of **assoc** to the file assoc.txt, type:

```
assoc>assoc.txt
```

Associatie **.log** to text files:

```
assoc .log=txtfile
```

Associatie files with no extension to text files:

```
assoc .=txtfile
```

Related links

- Command-Line Syntax Key
- ftype command

at

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Schedules commands and programs to run on a computer at a specified time and date. You can use **at** only when the Schedule service is running. Used without parameters, **at** lists scheduled commands. You must be a member of the local Administrators group to run this command.

Syntax

```
at [\computername] [[id] [/delete] | /delete [/yes]]
at [\computername] <time> [/interactive] [/every:date[,...] |
/next:date[,...]] <command>
```

Parameters

Parameter	Description
`\<computername\>`	Specifies a remote computer. If you omit this parameter, **at** schedules the commands and programs on the local computer.
`<id>`	Specifies the identification number assigned to a scheduled command.
/delete	Cancels a scheduled command. If you omit *ID*, all of the scheduled commands on the computer are canceled.
/yes	Answers yes to all queries from the system when you delete scheduled events.
`<time>`	Specifies the time when you want to run the command. time is expressed as Hours:Minutes in 24-hour notation (that is, 00:00 (midnight) through 23:59).
interactive	Allows *command* to interact with the desktop of the user who is logged on at the time *Command* runs.
every:	Runs *command* on every specified day or days of the week or month (for example, every Thursday, or the third day of every month).

Parameter	Description
`<date>`	Specifies the date when you want to run the command. You can specify one or more days of the week (that is, type **M**,**T**,**W**,**Th**,**F**,**S**,**Su**) or one or more days of the month (that is, type 1 through 31). Separate multiple date entries with commas. If you omit *date*, **at** uses the current day of the month.
next:	Runs *command* on the next occurrence of the day (for example, next Thursday).
`<command>`	Specifies the Windows command, program (that is, .exe or .com file), or batch program (that is, .bat or .cmd file) that you want to run. When the command requires a path as an argument, use the absolute path (that is, the entire path beginning with the drive letter). If the command is on a remote computer, specify Universal Naming Convention (UNC) notation for the server and share name, rather than a remote drive letter.
/?	Displays help at the command prompt.

Remarks

- This command doesn't automatically load cmd.exe before running commands. If you're not running an executable (.exe) file, you must explicitly load cmd.exe at the beginning of the command as follows:

```
cmd /c dir > c:\test.out
```

- If using this command without command-line options, scheduled tasks appear in a table formatted similar to the following:

```
Status  ID   Day        time        Command Line
OK      1    Each F     4:30 PM     net send group leads status due
OK      2    Each M     12:00 AM    chkstor > check.file
OK      3    Each F     11:59 PM    backup2.bat
```

- If including an identification number (*ID*) with this command, only information for a single entry appears in a format similar to the following:

```
Task ID: 1
Status: OK
Schedule: Each  F
```

```
Time of Day: 4:30 PM
Command: net send group leads status due
```

- After you schedule a command, especially a command that has command-line options, check that the command syntax is correct by typing **at** without any command-line options. If the information in the **Command Line** column is wrong, delete the command and retype it. If it's still incorrect, retype the command using fewer command-line options.

- Commands scheduled with **at** run as background processes. Output is not displayed on the computer screen. To redirect output to a file, use the redirection symbol `>`. If you redirect output to a file, you need to use the escape symbol `^` before the redirection symbol, whether you are using **at** at the command line or in a batch file. For example, to redirect output to *output.txt*, type:

  ```
  at 14:45 c:\test.bat ^>c:\output.txt
  ```

  The current directory for the executing command is the systemroot folder.

- If you change the system time after you schedule a command to run, synchronize the **at** scheduler with the revised system time by typing **at** without command-line options.

- Scheduled commands are stored in the registry. As a result, you don't lose scheduled tasks if you restart the Schedule service.

- Do not use a redirected drive for scheduled jobs that access the network. The Schedule service might not be able to access the redirected drive, or the redirected drive might not be present if a different user is logged on at the time the scheduled task runs. Instead, use UNC paths for scheduled jobs. For example:

  ```
  at 1:00pm my_backup \\server\share
  ```

  Do not use the following syntax, where **x:** is a connection made by the user:

  ```
  at 1:00pm my_backup x:
  ```

If you schedule an **at** command that uses a drive letter to connect to a shared directory, include an **at** command to disconnect the drive when you are finished using the drive. If the drive is not disconnected, the assigned drive letter won't be available at the command prompt.

- By default, tasks scheduled using this command will stop after 72 hours. You can modify the registry to change this default value.

  To modify the registry

  > ⊗ **Caution**
  >
  > Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

  1. Start the registry editor (regedit.exe).
  2. Locate and click the following key in the registry:
     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule`
  3. On the **Edit** menu, click **Add Value**, and then add the following registry values:
     - **Value Name.** atTaskMaxHours
     - **Data type.** reg_DWOrd
     - **Radix.** Decimal
     - **Value Data:** 0. A value of **0** in the **Value Data** field indicates no limit and doesn't not stop. Values from 1 through 99 indicates the number of hours.

- You can use the Scheduled Tasks folder to view or modify the settings of a task that was created by using this command. When you schedule a task using this command, the task is listed in the Scheduled Tasks folder, with a name such as the following:**at3478**. However, if you modify a task through the Scheduled Tasks folder, it's upgraded to a normal scheduled task. The task is no longer visible to the **at** command, and the at account setting no longer applies to it. You must explicitly enter a user account and password for the task.

Examples

To display a list of commands scheduled on the Marketing server, type:

```
at \\marketing
```

To learn more about a command with the identification number 3 on the Corp server, type:

```
at \\corp 3
```

To schedule a net share command to run on the Corp server at 8:00 A.M. and redirect the listing to the Maintenance server, in the Reports shared directory, and the Corp.txt file, type:

```
at \\corp 08:00 cmd /c net share reports=d:\marketing\reports >>
\\maintenance\reports\corp.txt
```

To back up the hard drive of the Marketing server to a tape drive at midnight every five days, create a batch program called Archive.cmd, which contains the backup commands, and then schedule the batch program to run, type:

```
at \\marketing 00:00 /every:5,10,15,20,25,30 archive
```

To cancel all commands scheduled on the current server, clear the **at** schedule information as follows:

```
at /delete
```

To run a command that is not an executable (.exe) file, precede the command with **cmd /c** to load cmd.exe as follows:

```
cmd /c dir > c:\test.out
```

Related links

- Command-Line Syntax Key
- schtasks. Another command-line scheduling tool.

atmadm

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Monitors connections and addresses that are registered by the atM call Manager on an asynchronous transfer mode (atM) network. You can use **atmadm** to display statistics for incoming and outgoing calls on atM adapters. Used without parameters, **atmadm** displays statistics for monitoring the status of active atM connections.

Syntax

```
atmadm [/c][/a][/s]
```

Parameters

Parameter	Description
/c	Displays call information for all current connections to the atM network adapter installed on this computer.
/a	Displays the registered atM network service access point (NSAP) address for each adapter installed in this computer.
/s	Displays statistics for monitoring the status of active atM connections.
/?	Displays help at the command prompt.

Remarks

- The **atmadm /c** command produces output similar to the following:

```
Windows atM call Manager Statistics
atM Connections on Interface : [009] Olicom atM PCI 155 Adapter
   Connection   VPI/VCI   remote address/
                          Media Parameters (rates in bytes/sec)
   In  PMP SVC    0/193   47000580FFE1000000F21A2E180020481A2E180B
```

```
                          Tx:UBR,Peak 0,Avg 0,MaxSdu 1516
                          Rx:UBR,Peak 16953936,Avg 16953936,MaxSdu 1516
    Out P-P SVC    0/192  47000580FFE1000000F21A2E180020481A2E180B
                          Tx:UBR,Peak 16953936,Avg 16953936,MaxSdu 1516
                          Rx:UBR,Peak 16953936,Avg 16953936,MaxSdu 1516
    In  PMP SVC    0/191  47000580FFE1000000F21A2E180020481A2E180B
                          Tx:UBR,Peak 0,Avg 0,MaxSdu 1516
                          Rx:UBR,Peak 16953936,Avg 16953936,MaxSdu 1516
    Out P-P SVC    0/190  47000580FFE1000000F21A2E180020481A2E180B
                          Tx:UBR,Peak 16953936,Avg 16953936,MaxSdu 1516
                          Rx:UBR,Peak 16953936,Avg 16953936,MaxSdu 1516
    In  P-P SVC    0/475  47000580FFE1000000F21A2E180000C110081501
                          Tx:UBR,Peak 16953984,Avg 16953984,MaxSdu 9188
                          Rx:UBR,Peak 16953936,Avg 16953936,MaxSdu 9188
    Out PMP SVC    0/194  47000580FFE1000000F21A2E180000C110081501 (0)
                          Tx:UBR,Peak 16953984,Avg 16953984,MaxSdu 9180
                          Rx:UBR,Peak 0,Avg 0,MaxSdu 0
    Out P-P SVC    0/474  4700918100000000613E5BFE010000C110081500
                          Tx:UBR,Peak 16953984,Avg 16953984,MaxSdu 9188
                          Rx:UBR,Peak 16953984,Avg 16953984,MaxSdu 9188
    In  PMP SVC    0/195  47000580FFE1000000F21A2E180000C110081500
                          Tx:UBR,Peak 0,Avg 0,MaxSdu 0
                          Rx:UBR,Peak 16953936,Avg 16953936,MaxSdu 9180
```

The following table contains descriptions of each element in the **atmadm /c** sample output.

Type of Data	Screen Display	Description
Connection Information	In/Out	Direction of the call. **In** is to the atM network adapter from another device. **Out** is from the atM network adapter to another device.
PMP	Point-to-multipoint call.	
P-P	Point-to-point call.	
SVC	Connection is on a switched virtual circuit.	
PVC	Connection is on a permanent virtual circuit.	
VPI/VCI Information	VPI/VCI	Virtual path and virtual channel of the incoming or outgoing call.

Type of Data	Screen Display	Description
Remote address/Media Parameters	47000580FFE1000000F21A2E180000C110081500	NSAP address of the calling **(In)** or called **(Out)** atM device.
Tx	The **Tx** parameter includes the following three elements: ◦ Default or specified bit-rate type (UBR, CBR, VBR, or ABR) ◦ Default or specified line speed ◦ Specified service data unit (SDU) size.	
Rx	The **Rx** parameter includes the following three elements: ◦ Default or specified bit-rate type (UBR, CBR, VBR, or ABR) ◦ Default or specified line speed ◦ Specified SDU size.	

- The **atmadm /a** command produces output similar to the following:

```
Windows atM call Manager Statistics
atM addresses for Interface : [009] Olicom atM PCI 155 Adapter
47000580FFE1000000F21A2E180000C110081500
```

- The **atmadm /s** command produces output similar to the following:

```
Windows atM call Manager Statistics
atM call Manager statistics for Interface : [009] Olicom atM PCI 155
Adapter
Current active calls                        = 4
Total successful Incoming calls             = 1332
Total successful Outgoing calls             = 1297
Unsuccessful Incoming calls                 = 1
Unsuccessful Outgoing calls                 = 1
calls Closed by remote                      = 1302
calls Closed Locally                        = 1323
Signaling and ILMI Packets Sent            = 33655
Signaling and ILMI Packets Received        = 34989
```

The following table contains descriptions of each element in the **atmadm /s** sample output.

Call Manager Statistic	Description
Current active calls	Calls currently active on the atM adapter installed on this computer.
Total successful Incoming calls	Calls successfully received from other devices on this atM network.
Total successful Outgoing calls	Calls successfully completed to other atM devices on this network from this computer.
Unsuccessful Incoming calls	Incoming calls that failed to connect to this computer.
Unsuccessful Outgoing calls	Outgoing calls that failed to connect to another device on the network.
Calls Closed by remote	Calls closed by a remote device on the network.
Calls Closed Locally	Calls closed by this computer.
Signaling and ILMI Packets Sent	Number of integrated local management interface (ILMI) packets sent to the switch to which this computer is attempting to connect.
Signaling and ILMI Packets Received	Number of ILMI packets received from the atM switch.

Examples

To display call information for all current connections to the atM network adapter installed on this computer, type:

```
atmadm /c
```

To display the registered atM network service access point (NSAP) address for each adapter installed in this computer, type:

```
atmadm /a
```

To display statistics for monitoring the status of active atM connections, type:

```
atmadm /s
```

Related links

- Command-Line Syntax Key

attrib

Article • 09/25/2023

Displays, sets, or removes attributes assigned to files or directories. If used without parameters, **attrib** displays attributes of all files in the current directory.

Syntax

```
attrib [{+|-}r] [{+|-}a] [{+|-}s] [{+|-}h] [{+|-}o] [{+|-}i] [{+|-}x]
[{+|-}p] [{+|-}u] [{+|-}b] [<drive>:][<path>][<filename>] [/s [/d] [/l]]
```

Parameters

Parameter	Description
`{+|-}r`	Sets (+) or clears (-) the Read-only file attribute.
`{+|-}a`	Sets (+) or clears (-) the Archive file attribute. This attribute set marks files that have changed since the last time they were backed up. The **xcopy** command uses archive attributes.
`{+|-}s`	Sets (+) or clears (-) the System file attribute. If a file uses this attribute set, you must clear the attribute before you can change any other attributes for the file.
`{+|-}h`	Sets (+) or clears (-) the Hidden file attribute. If a file uses this attribute set, you must clear the attribute before you can change any other attributes for the file.
`{+|-}o`	Sets (+) or clears (-) the Offline file attribute.
`{+|-}i`	Sets (+) or clears (-) the Not Content Indexed file attribute.
`{+|-}x`	Sets (+) or clears (-) the Scrub file attribute.
`{+|-}p`	Sets (+) or clears (-) the Pinned file attribute.
`{+|-}u`	Sets (+) or clears (-) the Unpinned file attribute.
`{+|-}b`	Sets (+) or clears (-) the SMR Blob file attribute.
`[<drive>:][<path>][<filename>]`	Specifies the location and name of the directory, file, or group of files that you want to view or change attributes.

Parameter	Description
	You can use the **?** and ***** wildcard characters in the *filename* parameter to display or change the attributes for a group of files.
/s	Applies **attrib** and any command-line options to matching files in the current directory and all of its subdirectories.
/d	Applies **attrib** and any command-line options to directories.
/l	Applies **attrib** and any command-line options to the Symbolic Link, rather than the target of the Symbolic Link.
/?	Displays help at the command prompt.

Examples

To display the attributes of a file named News86 that is located in the current directory, type:

```
attrib news86
```

To assign the Read-only attribute to the file named report.txt, type:

```
attrib +r report.txt
```

To remove the Read-only attribute from files in the public directory and its subdirectories on a disk in drive b:, type:

```
attrib -r b:\public\*.* /s
```

To set the Archive attribute for all files on drive a:, and then clear the Archive attribute for files with the .bak extension, type:

```
attrib +a a:*.* & attrib -a a:*.bak
```

Related links

- Command-Line Syntax Key
- xcopy command

auditpol

Article • 02/03/2023

Displays information about and performs functions to manipulate audit policies, including:

- Setting and querying a system audit policy.
- Setting and querying a per-user audit policy.
- Setting and querying auditing options.
- Setting and querying the security descriptor used to delegate access to an audit policy.
- Reporting or backing up an audit policy to a comma-separated value (CSV) text file.
- Loading an audit policy from a CSV text file.
- Configuring global resource SACLs.

Syntax

```
auditpol command [<sub-command><options>]
```

Parameters

Sub-command	Description
/get	Displays the current audit policy. For more information, see auditpol get for syntax and options.
/set	Sets the audit policy. For more information, see auditpol set for syntax and options.
/list	Displays selectable policy elements. For more information, see auditpol list for syntax and options.
/backup	Saves the audit policy to a file. For more information, see auditpol backup for syntax and options.

Sub-command	Description
/restore	Restores the audit policy from a file that was previously created by using auditpol /backup. For more information, see auditpol restore for syntax and options.
/clear	Clears the audit policy. For more information, see auditpol clear for syntax and options.
/remove	Removes all per-user audit policy settings and disables all system audit policy settings. For more information, see auditpol remove for syntax and options.
/resourceSACL	Configures global resource system access control lists (SACLs). **Note:** Applies only to Windows 7 and Windows Server 2008 R2. For more information, see auditpol resourceSACL.
/?	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

auditpol backup

Article • 05/22/2023

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

The auditpol backup command backs up system audit policy settings, per-user audit policy settings for all users, and all auditing options to a comma-separated value (CSV) text file.

To perform *backup* operations on the *per-user* and *system* policies, you need **Write** or **Full Control** permissions for that object set in the security descriptor. You can also perform *backup* operations if you have the **Manage auditing and security log** (SeSecurityPrivilege) user right. However, this right allows access that isn't necessary to perform the overall *backup* operations.

Syntax

```
auditpol /backup /file:<filename>
```

Parameters

Parameter	Description
/file	Specifies the file name of the for the back up.
/?	Displays help at the command prompt.

Examples

You can back up the following settings to a CSV-formatted text file:

- Per-user audit policy settings for all users
- System audit policy settings
- All auditing options

To back up these settings to a file named auditpolicy.csv, type the following command:

```
auditpol /backup /file:C:\auditpolicy.csv
```

> **Note**
>
> If no drive is specified, the current directory is used.

Related links

- Command-Line Syntax Key
- auditpol restore
- auditpol commands

auditpol clear

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Deletes the per-user audit policy for all users, resets (disables) the system audit policy for all subcategories, and sets all the auditing options to disabled.

To perform *clear* operations on the *per-user* and *system* policies, you must have **Write** or **Full Control** permission for that object set in the security descriptor. You can also perform *clear* operations if you have the **Manage auditing and security log** (SeSecurityPrivilege) user right. However, this right allows additional access that is not necessary to perform the overall *clear* operations.

Syntax

```
auditpol /clear [/y]
```

Parameters

Parameter	Description
/y	Suppresses the prompt to confirm if all audit policy settings should be cleared.
/?	Displays help at the command prompt.

Examples

To delete the per-user audit policy for all users, reset (disable) the system audit policy for all subcategories, and set all the audit policy settings to disabled, at a confirmation prompt, type:

```
auditpol /clear
```

To delete the per-user audit policy for all users, reset the system audit policy settings for all subcategories, and set all the audit policy settings to disabled, without a confirmation prompt, type:

```
auditpol /clear /y
```

> **Note**
>
> The preceding example is useful when using a script to perform this operation.

Related links

- Command-Line Syntax Key
- auditpol commands

auditpol get

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server, 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves the system policy, per-user policy, auditing options, and audit security descriptor object.

To perform *get* operations on the *per-user* and *system* policies, you must have **Read** permission for that object set in the security descriptor. You can also perform *get* operations if you have the **Manage auditing and security log** (SeSecurityPrivilege) user right. However, this right allows additional access that is not necessary to perform the overall *get* operations.

Syntax

```
auditpol /get
[/user[:<username>|<{sid}>]]
[/category:*|<name>|<{guid}>[,:<name|<{guid}> ]]
[/subcategory:*|<name>|<{guid}>[,:<name|<{guid}> ]]
[/option:<option name>]
[/sd]
[/r]
```

Parameters

Parameter	Description
/user	Displays the security principal for whom the per-user audit policy is queried. Either the /category or /subcategory parameter must be specified. The user may be specified as a security identifier (SID) or name. If no user account is specified, then the system audit policy is queried.
/category	One or more audit categories specified by globally unique identifier (GUID) or name. An asterisk (*) may be used to indicate that all audit categories should be queried.
/subcategory	One or more audit subcategories specified by GUID or name.
/sd	Retrieves the security descriptor used to delegate access to the audit policy.

Parameter	Description
/option	Retrieves the existing policy for the CrashOnAuditFail, FullprivilegeAuditing, AuditBaseObjects, or AuditBasedirectories options.
/r	Displays the output in report format, comma-separated value (CSV).
/?	Displays help at the command prompt.

Remarks

All categories and subcategories can be specified by the GUID or name enclosed by quotation marks ("). Users can be specified by SID or name.

Examples

To retrieve the per-user audit policy for the Guest account and display the output for the System, detailed Tracking, and Object Access categories, type:

```
auditpol /get /user:{S-1-5-21-1443922412-3030960370-963420232-51}
/category:System,detailed Tracking,Object Access
```

> ⓘ **Note**
>
> This command is useful in two scenarios. 1) When monitoring a specific user account for suspicious activity, you can use the `/get` command to retrieve the results in specific categories by using an inclusion policy to enable additional auditing. 2) if audit settings on an account are logging numerous but superfluous events, you can use the `/get` command to filter out extraneous events for that account with an exclusion policy. For a list of all categories, use the `auditpol /list /category` command.

To retrieve the per-user audit policy for a category and a particular subcategory, which reports the inclusive and exclusive settings for that subcategory under the System category for the Guest account, type:

```
auditpol /get /user:guest /category:System /subcategory:{0ccee921a-69ae-
11d9-bed3-505054503030}
```

To display the output in report format and include the computer name, policy target, subcategory, subcategory GUID, inclusion settings, and exclusion settings, type:

```
auditpol /get /user:guest /category:detailed Tracking /r
```

To retrieve the policy for the System category and subcategories, which reports the category and subcategory policy settings for the system audit policy, type:

```
auditpol /get /category:System /subcategory:{0ccee921a-69ae-11d9-bed3-
505054503030}
```

To retrieve the policy for the detailed Tracking category and subcategories in report format and include the computer name, policy target, subcategory, subcategory GUID, inclusion settings, and exclusion settings, type:

```
auditpol /get /category:detailed Tracking /r
```

To retrieve the policy for two categories with the categories specified as GUIDs, which reports all the audit policy settings of all the subcategories under two categories, type:

```
auditpol /get /category:{69979849-797a-11d9-bed3-505054503030},{69997984a-
797a-11d9-bed3-505054503030} subcategory:{0ccee921a-69ae-11d9-bed3-
505054503030}
```

To retrieve the state, either enabled or disabled, of the AuditBaseObjects option, type:

```
auditpol /get /option:AuditBaseObjects
```

Where the available options are AuditBaseObjects, AuditBaseOperations, and FullprivilegeAuditing. To retrieve the state enabled, disabled, or 2 of the CrashOnAuditFail option, type:

```
auditpol /get /option:CrashOnAuditFail /r
```

Related links

- Command-Line Syntax Key
- auditpol commands

auditpol list

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Lists audit policy categories and subcategories, or lists users for whom a per-user audit policy is defined.

To perform *list* operations on the *per-user* policy, you must have **Read** permission for that object set in the security descriptor. You can also perform *list* operations if you have the **Manage auditing and security log** (SeSecurityPrivilege) user right. However, this right allows additional access that is not necessary to perform the overall *list* operations.

Syntax

```
auditpol /list
[/user|/category|subcategory[:<categoryname>|<{guid}>|*]]
[/v] [/r]
```

Parameters

Parameter	Description
/user	Retrieves all users for whom the per-user audit policy has been defined. If used with the /v parameter, the security identifier (SID) of the user is also displayed.
/category	Displays the names of categories understood by the system. If used with the /v parameter, the category globally unique identifier (GUID) is also displayed.
/subcategory	Displays the names of subcategories and their associated GUID.
/v	Displays the GUID with the category or subcategory, or when used with /user, displays the SID of each user.
/r	Displays the output as a report in comma-separated value (CSV) format.
/?	Displays help at the command prompt.

Examples

To list all users who have a defined audit policy, type:

```
auditpol /list /user
```

To list all users who have a defined audit policy and their associated SID, type:

```
auditpol /list /user /v
```

To list all categories and subcategories in report format, type:

```
auditpol /list /subcategory:* /r
```

To list the subcategories of the detailed Tracking and DS Access categories, type:

```
auditpol /list /subcategory:detailed Tracking,DS Access
```

Related links

- Command-Line Syntax Key
- auditpol commands

auditpol remove

Article • 05/22/2023

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

The auditpol remove command removes the per-user audit policy for a specified account or all accounts.

To perform *remove* operations on the *per-user* policy, you must have **Write** or **Full Control** permissions for that object set in the security descriptor. You can also perform *remove* operations if you have the **Manage auditing and security log** (`SeSecurityPrivilege`) user right. However, this right allows access that isn't necessary to perform the overall *remove* operations.

Syntax

```
auditpol /remove [/user[:<username>|<{SID}>]]
[/allusers]
```

Parameters

Parameter	Description
/user	Specifies the security identifier (SID) or user name for the user for whom the per-user audit policy is to be deleted.
/allusers	Removes the per-user audit policy for all users.
/?	Displays help at the command prompt.

Examples

To remove the per-user audit policy for user `mikedan` by name, type:

```
auditpol /remove /user:mikedan
```

To remove the per-user audit policy for user `mikedan` by SID, type:

```
auditpol /remove /user:{S-1-5-21-397123471-12346959}
```

To remove the per-user audit policy for all users, type:

```
auditpol /remove /allusers
```

Related links

- Command-Line Syntax Key
- auditpol commands

auditpol resourceSACL

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 7 and Windows Server 2008 R2

Configures global resource system access control lists (SACLs).

To perform *resourceSACL* operations, you must have **Write** or **Full Control** permissions for that object set in the security descriptor. You can also perform *resourceSACL* operations if you have the **Manage auditing and security log** (SeSecurityPrivilege) user right.

Syntax

```
auditpol /resourceSACL
[/set /type:<resource> [/success] [/failure] /user:<user> [/access:<access
flags>]]
[/remove /type:<resource> /user:<user> [/type:<resource>]]
[/clear [/type:<resource>]]
[/view [/user:<user>] [/type:<resource>]]
```

Parameters

Parameter	Description
/set	Adds a new entry to or updates an existing entry in the resource SACL for the resource type specified.
/remove	Removes all entries for the given user in the global object access auditing list.
/clear	Removes all entries from the global object access auditing list.
/view	Lists the global object access auditing entries in a resource SACL. The user and resource types are optional.
/?	Displays help at the command prompt.

Arguments

Argument	Description
/type	The resource for which object access auditing is being configured. The supported, case-sensitive, argument values are *File* (for directories and files) and *Key* (for registry keys).
/success	Specifies success auditing.
/failure	Specifies failure auditing.
/user	Specifies a user in one of the following forms: • DomainName\Account (such as DOM\Administrators) • StandaloneServer\Group Account (see LookupAccountName function) • {S-1-x-x-x-x} (x is expressed in decimal, and the entire SID must be enclosed in curly braces). For example: {S-1-5-21-5624481-130208933-164394174-1001} **Note:** If the SID form is used, no check is done to verify the existence of this account.
/access	Specifies a permission mask that can be specified through: Generic access rights, including: • GA - GENERIC ALL • GR - GENERIC READ • GW - GENERIC WRITE • GX - GENERIC EXECUTE Access rights for files, including: • FA - FILE ALL ACCESS • FR - FILE GENERIC READ • FW - FILE GENERIC WRITE • FX - FILE GENERIC EXECUTE Access rights for registry keys, including: • KA - KEY ALL ACCESS • KR - KEY READ • KW - KEY WRITE • KX - KEY EXECUTE For example: `/access:FRFW` enables audit events for read and write operations. A hexadecimal value representing the access mask (such as 0x1200a9) This is useful when using resource-specific bit masks that are not part of the security descriptor definition language (SDDL) standard. If omitted, Full access is used.

Examples

To set a global resource SACL to audit successful access attempts by a user on a registry key:

```
auditpol /resourceSACL /set /type:Key /user:MYDOMAIN\myuser /success
```

To set a global resource SACL to audit successful and failed attempts by a user to perform generic read and write functions on files or folders:

```
auditpol /resourceSACL /set /type:File /user:MYDOMAIN\myuser /success
/failure /access:FRFW
```

To remove all global resource SACL entries for files or folders:

```
auditpol /resourceSACL /type:File /clear
```

To remove all global resource SACL entries for a particular user from files or folders:

```
auditpol /resourceSACL /remove /type:File /user:{S-1-5-21-56248481-
1302087933-1644394174-1001}
```

To list the global object access auditing entries set on files or folders:

```
auditpol /resourceSACL /type:File /view
```

To list the global object access auditing entries for a particular user that are set on files or folders:

```
auditpol /resourceSACL /type:File /view /user:MYDOMAIN\myuser
```

Related links

- Command-Line Syntax Key
- auditpol commands

auditpol restore

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Restores system audit policy settings, per-user audit policy settings for all users, and all auditing options from a file that is syntactically consistent with the comma-separated value (CSV) file format used by the /backup option.

To perform *restore* operations on the *per-user* and *system* policies, you must have **Write** or **Full Control** permission for that object set in the security descriptor. You can also perform *restore* operations if you have the **Manage auditing and security log** (SeSecurityPrivilege) user right, which is useful when restoring the security descriptor in the event of an error or malicious attack.

Syntax

```
auditpol /restore /file:<filename>
```

Parameters

Parameter	Description
/file	Specifies the file from which the audit policy should be restored. The file must have been created by using the /backup option or must be syntactically consistent with the CSV file format used by the /backup option.
/?	Displays help at the command prompt.

Examples

To restore system audit policy settings, per-user audit policy settings for all users, and all auditing options from a file named auditpolicy.csv that was created by using the /backup command, type:

```
auditpol /restore /file:c:\auditpolicy.csv
```

Related links

- Command-Line Syntax Key
- auditpol backup
- auditpol commands

auditpol set

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets the per-user audit policy, system audit policy, or auditing options.

To perform *set* operations on the *per-user* and *system* policies, you must have **Write** or **Full Control** permission for that object set in the security descriptor. You can also perform *set* operations if you have the **Manage auditing and security log** (SeSecurityPrivilege) user right. However, this right allows additional access that is not necessary to perform the overall *set* operations.

Syntax

```
auditpol /set
[/user[:<username>|<{sid}>][/include][/exclude]]
[/category:<name>|<{guid}>[,:<name|<{guid}> ]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/subcategory:<name>|<{guid}>[,:<name|<{guid}> ]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/option:<option name> /value: <enable>|<disable>]
```

Parameters

Parameter	Description
/user	The security principal for whom the per-user audit policy specified by the category or subcategory is set. Either the category or subcategory option must be specified, as a security identifier (SID) or name.
/include	Specified with /user; indicates that the user's per-user policy will cause an audit to be generated even if it is not specified by the system audit policy. This setting is the default and is automatically applied if neither the /include nor /exclude parameters are explicitly specified.
/exclude	Specified with /user; indicates that the user's per-user policy will cause an audit to be suppressed regardless of the system audit policy. This setting is ignored for users who are members of the local Administrators group.

Parameter	Description
/category	One or more audit categories specified by globally unique identifier (GUID) or name. If no user is specified, the system policy is set.
/subcategory	One or more audit subcategories specified by GUID or name. If no user is specified, the system policy is set.
/success	Specifies success auditing. This setting is the default and is automatically applied if neither the /success nor /failure parameters are explicitly specified. This setting must be used with a parameter indicating whether to enable or disable the setting.
/failure	Specifies failure auditing. This setting must be used with a parameter indicating whether to enable or disable the setting.
/option	Sets the audit policy for the CrashOnAuditFail, FullprivilegeAuditing, AuditBaseObjects, or AuditBasedirectories options.
/sd	Sets the security descriptor used to delegate access to the audit policy. The security descriptor must be specified by using the Security Descriptor Definition Language (SDDL). The security descriptor must have a discretionary access control list (DACL).
/?	Displays help at the command prompt.

Examples

To set the per-user audit policy for all subcategories under the detailed Tracking category for the user mikedan so that all the user's successful attempts will be audited, type:

```
auditpol /set /user:mikedan /category:detailed Tracking /include
/success:enable
```

To set the per-user audit policy for categories specified by name and GUID, and subcategories specified by GUID to suppress auditing for any successful or failed attempts, type:

```
auditpol /set /user:mikedan /exclude /category:Object Access,System,
{6997984b-797a-11d9-bed3-505054503030}
/subcategory:{0ccee9210-69ae-11d9-bed3-505054503030},:{0ccee9211-69ae-11d9-
bed3-505054503030}, /success:enable /failure:enable
```

To set the per-user audit policy for the specified user for all the categories for the suppression of auditing of all but successful attempts, type:

```
auditpol /set /user:mikedan /exclude /category:* /success:enable
```

To set the system audit policy for all subcategories under the detailed Tracking category to include auditing for only successful attempts, type:

```
auditpol /set /category:detailed Tracking /success:enable
```

> **Note**
>
> The failure setting is not altered.

To set the system audit policy for the Object Access and System categories (which is implied because subcategories are listed) and subcategories specified by GUIDs for the suppression of failed attempts and the auditing of successful attempts, type:

```
auditpol /set /subcategory:{0ccee9210-69ae-11d9-bed3-505054503030},
{0ccee9211-69ae-11d9-bed3-505054503030}, /failure:disable /success:enable
```

To set the auditing options to the enabled state for the CrashOnAuditFail option, type:

```
auditpol /set /option:CrashOnAuditFail /value:enable
```

Related links

- Command-Line Syntax Key
- auditpol commands

autochk

Article • 02/03/2023

Runs when the computer is started and prior to Windows Server starting to verify the logical integrity of a file system.

Autochk.exe is a version of **chkdsk** that runs only on NTFS disks and only before Windows Server starts. **autochk** cannot be run directly from the command-line. Instead, **autochk** runs in the following situations:

- If you try to run **chkdsk** on the boot volume.
- If **chkdsk** cannot gain exclusive use of the volume.
- If the volume is flagged as dirty.

Remarks

> ⚠ **Warning**
>
> The **autochk** command-line tool cannot be directly run from the command-line. Instead, use the **chkntfs** command-line tool to configure the way you want **autochk** to run at startup.
>
> - You can use **chkntfs** with the **/x** parameter to prevent **autochk** from running on a specific volume or multiple volumes.
> - Use the **chkntfs.exe** command-line tool with the **/t** parameter to change the autochk delay from 0 seconds to up to 3 days (259,200 seconds). However, a long delay means that the computer does not start until the time elapses or until you press a key to cancel **autochk**.

Related links

- Command-Line Syntax Key
- chkdsk command
- chkntfs command

autoconv

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Converts file allocation table (Fat) and Fat32 volumes to the NTFS file system, leaving existing files and directories intact at startup after **autochk** runs. volumes converted to the NTFS file system cannot be converted back to Fat or Fat32.

> **ⓘ Important**
>
> You can't run **autoconv** from the command-line. This can only run at startup, if set through **convert.exe**.

Related links

- Command-Line Syntax Key
- autochk command
- convert command

autofmt

Article • 02/03/2023

Starts the Auto File System Format Utility, which formats a drive or partition when called from the Windows Recovery Console.

> **Important**
>
> You cannot run **autofmt** directly from the command-line.

Related links

- Command-Line Syntax Key
- Windows Recovery Environment (WinRE)
- How to use Windows Recovery Environment (WinRE) to troubleshoot common startup issues

bcdboot

Article • 02/03/2023

Enables you to quickly set up a system partition, or to repair the boot environment located on the system partition. The system partition is set up by copying a simple set of Boot Configuration Data (BCD) files to an existing empty partition.

Syntax

```
bcdboot <source> [/l] [/s]
```

Parameters

Parameter	Description
source	Specifies the location of the Windows directory to use as the source for copying boot environment files.
/l	Specifies the locale. The default locale is US English.
/s	Specifies the volume letter of the system partition. The default is the system partition identified by the firmware.

Examples

For information about where to find BCDboot and examples of how to use this command, see the BCDboot Command-Line Options topic.

Related links

- Command-Line Syntax Key

bcdedit

Article • 02/03/2023

Boot Configuration Data (BCD) files provide a store that is used to describe boot applications and boot application settings. The objects and elements in the store effectively replace Boot.ini.

BCDEdit is a command-line tool for managing BCD stores. It can be used for a variety of purposes, including creating new stores, modifying existing stores, adding boot menu parameters, and so on. BCDEdit serves essentially the same purpose as Bootcfg.exe on earlier versions of Windows, but with two major improvements:

- Exposes a wider range of boot parameters than Bootcfg.exe.
- Has improved scripting support.

> ⓘ **Note**
>
> Administrative privileges are required to use BCDEdit to modify BCD.

BCDEdit is the primary tool for editing the boot configuration of Windows Vista and later versions of Windows. It is included with the Windows Vista distribution in the %WINDIR%\System32 folder.

BCDEdit is limited to the standard data types and is designed primarily to perform single common changes to BCD. For more complex operations or nonstandard data types, consider using the BCD Windows Management Instrumentation (WMI) application programming interface (API) to create more powerful and flexible custom tools.

Syntax

```
bcdedit /command [<argument1>] [<argument2>] ...
```

Parameters

General BCDEdit Command-Line Options

Option	Description
/?	Displays a list of BCDEdit commands. Running this command without an argument displays a summary of the available commands. To display detailed help for a particular command, run **bcdedit /?** `<command>`, where `<command>` is the name of the command you are searching for more information about. For example, **bcdedit /? createstore** displays detailed help for the Createstore command.

Parameters that Operate on a Store

Option	Description
/createstore	Creates a new empty boot configuration data store. The created store is not a system store.
/export	Exports the contents of the system store into a file. This file can be used later to restore the state of the system store. This command is valid only for the system store.
/import	Restores the state of the system store by using a backup data file previously generated by using the **/export** option. This command deletes any existing entries in the system store before the import takes place. This command is valid only for the system store.
/store	This option can be used with most BCDedit commands to specify the store to be used. If this option is not specified, then BCDEdit operates on the system store. Running the **bcdedit /store** command by itself is equivalent to running the **bcdedit /enum active** command.

Parameters that Operate on Entries in a Store

Parameter	Description
/copy	Makes a copy of a specified boot entry in the same system store.
/create	Creates a new entry in the boot configuration data store. If a well-known identifier is specified, then the **/application**, **/inherit**, and **/device** parameters cannot be specified. If an identifier is not specified or not well known, an **/application**, **/inherit**, or **/device** option must be specified.
/delete	Deletes an element from a specified entry.

Parameters that Operate on Entry Options

Parameter	Description

Parameter	Description
/deletevalue	Deletes a specified element from a boot entry.
/set	Sets an entry option value.

Parameters that Control Output

Parameter	Description
/enum	Lists entries in a store. The **/enum** option is the default value for BCEdit, so running the **bcdedit** command without parameters is equivalent to running the **bcdedit /enum active** command.
/v	Verbose mode. Usually, any well-known entry identifiers are represented by their friendly shorthand form. Specifying **/v** as a command-line option displays all identifiers in full. Running the **bcdedit /v** command by itself is equivalent to running the **bcdedit /enum active /v** command.

Parameters that Control the Boot Manager

Parameter	Description
/bootsequence	Specifies a one-time display order to be used for the next boot. This command is similar to the **/displayorder** option, except that it is used only the next time the computer starts. Afterwards, the computer reverts to the original display order.
/default	Specifies the default entry that the boot manager selects when the timeout expires.
/displayorder	Specifies the display order that the boot manager uses when displaying boot parameters to a user.
/timeout	Specifies the time to wait, in seconds, before the boot manager selects the default entry.
/toolsdisplayorder	Specifies the display order for the boot manager to use when displaying the **Tools** menu.

Parameters that Control Emergency Management Services

Parameter	Description
/bootems	Enables or disables Emergency Management Services (EMS) for the specified entry.

Parameter	Description
/ems	Enables or disables EMS for the specified operating system boot entry.
/emssettings	Sets the global EMS settings for the computer. **/emssettings** does not enable or disable EMS for any particular boot entry.

Parameters that Control Debugging

Parameter	Description
/bootdebug	Enables or disables the boot debugger for a specified boot entry. Although this command works for any boot entry, it is effective only for boot applications.
/dbgsettings	Specifies or displays the global debugger settings for the system. This command does not enable or disable the kernel debugger; use the **/debug** option for that purpose. To set an individual global debugger setting, use the **bcdedit /set** `<dbgsettings> <type> <value>` command.
/debug	Enables or disables the kernel debugger for a specified boot entry.

Related links

For examples of how to use BCDEdit, see the BCDEdit Options Reference article.

To see the notation used to indicate command-line syntax, see Command-Line Syntax Key.

bdehdcfg

Article • 02/03/2023

Prepares a hard drive with the partitions necessary for BitLocker Drive Encryption. Most installations of Windows 7 will not need to use this tool because BitLocker setup includes the ability to prepare and repartition drives as required.

> ⚠ **Warning**
>
> There is a known conflict with the **Deny write access to fixed drives not protected by BitLocker** Group Policy setting located in **Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives**.
>
> If bdehdcfg is run on a computer when this policy setting is enabled, you may encounter the following issues:
>
> - If you attempted to shrink the drive and create the system drive, the drive size will be successfully reduced and a raw partition will be created. However, the raw partition will not be formatted. The following error message is displayed: The new active Drive cannot be formatted. You may need to manually prepare your drive for BitLocker.
> - If you attempted to use unallocated space to create the system drive, a raw partition will be created. However, the raw partition will not be formatted. The following error message is displayed: The new active Drive cannot be formatted. You may need to manually prepare your drive for BitLocker.
> - If you attempted to merge an existing drive into the system drive, the tool will fail to copy the required boot file onto the target drive to create the system drive. The following error message is displayed: BitLocker setup failed to copy boot files. You may need to manually prepare your drive for BitLocker.
> - If this policy setting is being enforced, a hard drive cannot be repartitioned because the drive is protected. If you are upgrading computers in your organization from a previous version of Windows and those computers were configured with a single partition, you should create the required BitLocker system partition before applying the policy setting to the computers.

Syntax

```
bdehdcfg [-driveinfo <drive_letter>] [-target {default|unallocated|
<drive_letter> shrink|<drive_letter> merge}] [-newdriveletter] [-size
<size_in_mb>] [-quiet]
```

Parameters

Parameter	Description
bdehdcfg: driveinfo	Displays the drive letter, the total size, the maximum free space, and the partition characteristics of the partitions on the drive specified. Only valid partitions are listed. Unallocated space is not listed if four primary or extended partitions already exist.
bdehdcfg: target	Defines which portion of a drive to use as the system drive and makes the portion active.
bdehdcfg: newdriveletter	Assigns a new drive letter to the portion of a drive used as the system drive.
bdehdcfg: size	Determines the size of the system partition when a new system drive is being created.
bdehdcfg: quiet	Prevents the display of all actions and errors in the command-line interface and directs bdehdcfg to use the Yes answer to any Yes/No prompts that may occur during subsequent drive preparation.
bdehdcfg: restart	Directs the computer to restart after the drive preparation has finished.
/?	Displays Help at the command prompt.

Related links

- Command-Line Syntax Key

bdehdcfg: driveinfo

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the drive letter, the total size, the maximum free space, and the partition characteristics. Only valid partitions are listed. Unallocated space is not listed if four primary or extended partitions already exist.

> **Note**
>
> This command is informational only and makes no changes to the drive.

Syntax

```
bdehdcfg -driveinfo <drive_letter>
```

Parameters

Parameter	Description
<drive_letter>	Specifies a drive letter followed by a colon.

Example

To display the drive information for the C: drive:

```
bdehdcfg  driveinfo C:
```

Related links

- Command-Line Syntax Key

- bdehdcfg

bdehdcfg: newdriveletter

Article • 02/03/2023

Assigns a new drive letter to the portion of a drive used as the system drive. As a best practice, we recommend not assigning a drive letter to your system drive.

Syntax

```
bdehdcfg -target {default|unallocated|<drive_letter> shrink|<drive_letter>
merge} -newdriveletter <drive_letter>
```

Parameters

Parameter	Description
`<drive_letter>`	Defines the drive letter that will be assigned to the specified target drive.

Examples

To assign the default drive the drive letter `P`:

```
bdehdcfg -target default -newdriveletter P:
```

Related links

- Command-Line Syntax Key
- bdehdcfg

bdehdcfg: quiet

Article • 02/03/2023

Informs the bdehdcfg command-line tool that all actions and errors are not to be displayed in the command-line interface. Any Yes/No (Y/N) prompts displayed during the drive preparation will assume a "Yes" answer. To view any error that occurred during drive preparation, review the system event log under the **Microsoft-Windows-BitLocker-DrivePreparationTool** event provider.

Syntax

```
bdehdcfg -target {default|unallocated|<drive_letter> shrink|<drive_letter>
merge} -quiet
```

Parameters

This command has no additional parameters.

Examples

To use the **quiet** command:

```
bdehdcfg -target default -quiet
```

Related links

- Command-Line Syntax Key
- bdehdcfg

bdehdcfg: restart

Article • 02/03/2023

Informs the bdehdcfg command-line tool that the computer should be restarted after the drive preparation has concluded. If other users are logged on to the computer and the **quiet** command is not specified, a prompt appears to confirm that the computer should be restarted.

Syntax

```
bdehdcfg -target {default|unallocated|<drive_letter> shrink|<drive_letter>
merge} -restart
```

Parameters

This command has no additional parameters.

Examples

To use the **restart** command:

```
bdehdcfg -target default -restart
```

Related links

- Command-Line Syntax Key
- bdehdcfg

bdehdcfg: size

Article • 02/03/2023

Specifies the size of the system partition when a new system drive is being created. If you do not specify a size, the tool will use the default value of 300 MB. The minimum size of the system drive is 100 MB. If you will store system recovery or other system tools on the system partition, you should increase the size accordingly.

> ⓘ Note
>
> The **size** command cannot be combined with the `target <drive_letter> merge` command.

Syntax

```
bdehdcfg -target {default|unallocated|<drive_letter> shrink} -size
<size_in_mb>
```

Parameters

Parameter	Description
`<size_in_mb>`	Indicates the number of megabytes (MB) to use for the new partition.

Examples

To allocate 500 MB to the default system drive:

```
bdehdcfg -target default -size 500
```

Related links

- Command-Line Syntax Key

- bdehdcfg

bdehdcfg: target

Article • 02/03/2023

Prepares a partition for use as a system drive by BitLocker and Windows Recovery. By default, this partition is created without a drive letter.

Syntax

```
bdehdcfg -target {default|unallocated|<drive_letter> shrink|<drive_letter>
merge}
```

Parameters

Parameter	Description
default	Indicates that the command-line tool will follow the same process as the BitLocker setup wizard.
unallocated	Creates the system partition out of the unallocated space available on the disk.
`<drive_letter>` shrink	Reduces the drive specified by the amount necessary to create an active system partition. To use this command, the drive specified must have at least 5 percent free space.
`<drive_letter>` merge	Uses the drive specified as the active system partition. The operating system drive cannot be a target for merge.

Examples

To designate an existing drive (P) as the system drive:

```
bdehdcfg -target P: merge
```

Related links

- Command-Line Syntax Key

- bdehdcfg

bitsadmin

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows 10

Bitsadmin is a command-line tool used to create, download or upload jobs, and to monitor their progress. The bitsadmin tool uses switches to identify the work to perform. You can call `bitsadmin /?` or `bitsadmin /help` to get a list of switches.

Most switches require a `<job>` parameter, which you set to the job's display name, or GUID. A job's display name doesn't have to be unique. The **/create** and **/list** switches return a job's GUID.

By default, you can access information about your own jobs. To access information for another user's jobs, you must have administrator privileges. If the job was created in an elevated state, then you must run **bitsadmin** from an elevated window; otherwise, you'll have read-only access to the job.

Many of the switches correspond to methods in the BITS interfaces. For additional details that may be relevant to using a switch, see the corresponding method.

Use the following switches to create a job, set and retrieve the properties of a job, and monitor the status of a job. For examples that show how to use some of these switches to perform tasks, see bitsadmin examples.

Available switches

- bitsadmin /addfile
- bitsadmin /addfileset
- bitsadmin /addfilewithranges
- bitsadmin /cache
- bitsadmin /cache /delete
- bitsadmin /cache /deleteurl
- bitsadmin /cache /getexpirationtime
- bitsadmin /cache /getlimit
- bitsadmin /cache /help
- bitsadmin /cache /info
- bitsadmin /cache /list
- bitsadmin /cache /setexpirationtime

- bitsadmin /cache /setlimit
- bitsadmin /cache /clear
- bitsadmin /cancel
- bitsadmin /complete
- bitsadmin /create
- bitsadmin /examples
- bitsadmin /getaclflags
- bitsadmin /getbytestotal
- bitsadmin /getbytestransferred
- bitsadmin /getclientcertificate
- bitsadmin /getcompletiontime
- bitsadmin /getcreationtime
- bitsadmin /getcustomheaders
- bitsadmin /getdescription
- bitsadmin /getdisplayname
- bitsadmin /geterror
- bitsadmin /geterrorcount
- bitsadmin /getfilestotal
- bitsadmin /getfilestransferred
- bitsadmin /gethelpertokenflags
- bitsadmin /gethelpertokensid
- bitsadmin /gethttpmethod
- bitsadmin /getmaxdownloadtime
- bitsadmin /getminretrydelay
- bitsadmin /getmodificationtime
- bitsadmin /getnoprogresstimeout
- bitsadmin /getnotifycmdline
- bitsadmin /getnotifyflags
- bitsadmin /getnotifyinterface
- bitsadmin /getowner
- bitsadmin /getpeercachingflags
- bitsadmin /getpriority
- bitsadmin /getproxybypasslist
- bitsadmin /getproxylist
- bitsadmin /getproxyusage
- bitsadmin /getreplydata
- bitsadmin /getreplyfilename
- bitsadmin /getreplyprogress
- bitsadmin /getsecurityflags
- bitsadmin /getstate

- bitsadmin /gettemporaryname
- bitsadmin /gettype
- bitsadmin /getvalidationstate
- bitsadmin /help
- bitsadmin /info
- bitsadmin /list
- bitsadmin /listfiles
- bitsadmin /makecustomheaderswriteonly
- bitsadmin /monitor
- bitsadmin /nowrap
- bitsadmin /peercaching
- bitsadmin /peercaching /getconfigurationflags
- bitsadmin /peercaching /help
- bitsadmin /peercaching /setconfigurationflags
- bitsadmin /peers
- bitsadmin /peers /clear
- bitsadmin /peers /discover
- bitsadmin /peers /help
- bitsadmin /peers /list
- bitsadmin /rawreturn
- bitsadmin /removeclientcertificate
- bitsadmin /removecredentials
- bitsadmin /replaceremoteprefix
- bitsadmin /reset
- bitsadmin /resume
- bitsadmin /setaclflag
- bitsadmin /setclientcertificatebyid
- bitsadmin /setclientcertificatebyname
- bitsadmin /setcredentials
- bitsadmin /setcustomheaders
- bitsadmin /setdescription
- bitsadmin /setdisplayname
- bitsadmin /sethelpertoken
- bitsadmin /sethelpertokenflags
- bitsadmin /sethttpmethod
- bitsadmin /setmaxdownloadtime
- bitsadmin /setminretrydelay
- bitsadmin /setnoprogresstimeout
- bitsadmin /setnotifycmdline
- bitsadmin /setnotifyflags

- bitsadmin /setpeercachingflags
- bitsadmin /setpriority
- bitsadmin /setproxysettings
- bitsadmin /setreplyfilename
- bitsadmin /setsecurityflags
- bitsadmin /setvalidationstate
- bitsadmin /suspend
- bitsadmin /takeownership
- bitsadmin /transfer
- bitsadmin /util
- bitsadmin /util /enableanalyticchannel
- bitsadmin /util /getieproxy
- bitsadmin /util /help
- bitsadmin /util /repairservice
- bitsadmin /util /setieproxy
- bitsadmin /util /version
- bitsadmin /wrap

bitsadmin addfile

Article • 02/03/2023

Adds a file to the specified job.

Syntax

```
bitsadmin /addfile <job> <remoteURL> <localname>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
remoteURL	The URL of the file on the server.
localname	The name of the file on the local computer. *Localname* must contain an absolute path to the file.

Examples

To add a file to the job:

```
bitsadmin /addfile myDownloadJob http://downloadsrv/10mb.zip c:\10mb.zip
```

Repeat this call for each file to add. If multiple jobs use *myDownloadJob* as their name, you must replace *myDownloadJob* with the job's GUID to uniquely identify the job.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin addfileset

Article • 02/03/2023

Adds one or more files to the specified job.

Syntax

```
bitsadmin /addfileset <job> <textfile>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
textfile	A text file, each line of which contains a remote and a local file name. **Note:** Names must space-delimited. Lines starting with a `#` character are treated as a comment.

Examples

```
bitsadmin /addfileset files.txt
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin addfilewithranges

Article • 02/03/2023

Adds a file to the specified job. BITS downloads the specified ranges from the remote file. This switch is valid only for download jobs.

Syntax

```
bitsadmin /addfilewithranges <job> <remoteURL> <localname> <rangelist>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
remoteURL	URL of the file on the server.
localname	Name of the file on the local computer. Must contain an absolute path to the file.
rangelist	Comma-delimited list of offset:length pairs. Use a colon to separate the offset value from the length value. For example, a value of `0:100,2000:100,5000:eof` tells BITS to transfer 100 bytes from offset 0, 100 bytes from offset 2000, and the remaining bytes from offset 5000 to the end of the file.

Remarks

- The token **eof** is a valid length value within the offset and length pairs in the `<rangelist>`. It instructs the service to read to the end of the specified file.
- The `addfilewithranges` command will fail with error code 0x8020002c, if a zero-length range is specified along with another range using same offset, such as:

  `c:\bits>bitsadmin /addfilewithranges j2 http://bitsdc/dload/1k.zip c:\1k.zip 100:0,100:5`

  Error message: Unable to add file to job - 0x8020002c. The list of byte ranges contains some overlapping ranges, which are not supported.

Workaround: Don't specify the zero-length range first. For example, use `bitsadmin /addfilewithranges j2 http://bitsdc/dload/1k.zip c:\1k.zip 100:5,100:0`

Examples

To transfer 100 bytes from offset 0, 100 bytes from offset 2000, and the remaining bytes from offset 5000 to the end of the file:

```
bitsadmin /addfilewithranges http://downloadsrv/10mb.zip c:\10mb.zip
0:100,2000:100,5000:eof
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin cache

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Contains a list of the bitsadmin /cache switches.

Contains a list of the bitsadmin /cache switches.

Syntax

```
bitsadmin /cache /help
bitsadmin /cache /clear
bitsadmin /cache /delete
bitsadmin /cache /deleteURL
bitsadmin /cache /list
bitsadmin /cache /info
bitsadmin /cache /getlimit
bitsadmin /cache /setlimit
bitsadmin /cache /getexpirationtime
bitsadmin /cache /setexpirationtime
```

Parameters

Parameter	Description
bitsadmin cache and help	Displays the command-line usage for the /cache switches.
bitsadmin cache and clear	Purges the local cache.
bitsadmin cache and delete	Deletes a cache entry.
bitsadmin cache and deleteURL	Deletes all cache entries for the given URL.
bitsadmin cache and list	Lists all cache entries.
bitsadmin cache and info	Dumps a specific cache entry.
bitsadmin cache and getlimit	Retrieves the cache limit.
bitsadmin cache and setlimit	Sets the cache limit.

Parameter	Description
bitsadmin cache and getexpirationtime	Retrieves the cache expiration time.
bitsadmin cache and setexpirationtime	Sets the cache expiration time.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin cache and delete

Article • 02/03/2023

Deletes a specific cache entry.

Syntax

```
bitsadmin /cache /delete recordID
```

Parameters

Parameter	Description
recordID	The GUID associated with the cache entry.

Examples

To delete the cache entry with the RecordID of {6511FB02-E195-40A2-B595-E8E2F8F47702}:

```
bitsadmin /cache /delete {6511FB02-E195-40A2-B595-E8E2F8F47702}
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and deleteURL

Article • 02/03/2023

Deletes all cache entries for the given URL.

Syntax

```
bitsadmin /deleteURL URL
```

Parameters

Parameter	Description
URL	The Uniform Resource Locator that identifies a remote file.

Examples

To delete all cache entries for `https://www.contoso.com/en/us/default.aspx`:

```
bitsadmin /deleteURL https://www.contoso.com/en/us/default.aspx
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and getexpirationtime

Article • 02/03/2023

Retrieves the cache expiration time.

Syntax

```
bitsadmin /cache /getexpirationtime
```

Examples

To retrieve the cache expiration time:

```
bitsadmin /cache /getexpirationtime
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and getlimit

Article • 01/26/2023

Retrieves the cache limit.

Syntax

```
bitsadmin /cache /getlimit
```

Examples

To retrieve the cache limit:

```
bitsadmin /cache /getlimit
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and help

Article • 02/03/2023

Displays the command-line usage for the **cache** switches.

Syntax

```
bitsadmin /cache /help
```

Examples

To show the command-line help for the **cache** switches.

```
bitsadmin /cache /help
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and info

Article • 02/03/2023

Dumps a specific cache entry.

Syntax

```
bitsadmin /cache /info recordID [/verbose]
```

Parameters

Paramreter	Description
recordID	The GUID associated with the cache entry.

Examples

To dump the cache entry with the recordID value of {6511FB02-E195-40A2-B595-E8E2F8F47702}:

```
bitsadmin /cache /info {6511FB02-E195-40A2-B595-E8E2F8F47702}
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and list

Article • 02/03/2023

Lists all cache entries.

Syntax

```
bitsadmin /cache /list [/verbose]
```

Examples

To list all cache entries in verbose format.

```
bitsadmin /cache /list /verbose
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and setexpirationtime

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets the cache expiration time.

Syntax

```
bitsadmin /cache /setexpirationtime secs
```

Parameters

Parameter	Description
secs	The number of seconds until the cache expires.

Examples

To set the cache to expire in 60 seconds:

```
bitsadmin /cache / setexpirationtime 60
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and setlimit

Article • 02/03/2023

Sets the cache size limit.

Syntax

```
bitsadmin /cache /setlimit percent
```

Parameters

Parameter	Description
percent	The cache limit defined as a percentage of the total hard disk space.

Examples

To set the cache size limit to 50%:

```
bitsadmin /cache /setlimit 50
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cache and clear

Article • 01/27/2023

Applies to: Windows Server (All supported versions)

The bitsadmin cache and clear command purges the local cache.

Syntax

```
bitsadmin /cache /clear
```

Examples

To purge the local cache:

```
bitsadmin /cache /clear
```

Related links

- Command-Line Syntax Key
- bitsadmin cache command

bitsadmin cancel

Article • 02/03/2023

Removes the job from the transfer queue and deletes all temporary files associated with the job.

Syntax

```
bitsadmin /cancel <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To remove the *myDownloadJob* job from the transfer queue:

```
bitsadmin /cancel myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin complete

Article • 02/03/2023

Completes the job. Use this switch after the job moves to the transferred state. Otherwise, only those files that have been successfully transferred will be available.

Syntax

```
bitsadmin /complete <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Example

To complete the *myDownloadJob* job, after it reaches the `TRANSFERRED` state:

```
bitsadmin /complete myDownloadJob
```

If multiple jobs use *myDownloadJob* as their name, you must use the job's GUID to uniquely identify it for completion.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin create

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates a transfer job with the given display name.

> **Note**
>
> The **/Upload** and **/Upload-Reply** parameter types aren't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /create [type] displayname
```

Parameters

Parameter	Description
type	There are three types of jobs: • **/Download.** Transfers data from a server to a local file. • **/Upload.** Transfers data from a local file to a server. • **/Upload-Reply.** Transfers data from a local file to a server and receives a reply file from the server. This parameter defaults to **/Download** if it's not specified.
displayname	The display name assigned to the newly created job.

Examples

To create a download job named *myDownloadJob*:

```
bitsadmin /create myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin resume command
- bitsadmin command

bitsadmin examples

Article • 02/03/2023

The following examples show how to use the `bitsadmin` tool to perform the most common tasks.

Transfer a file

To create a job, add files, activate the job in the transfer queue, and to complete the job:

`bitsadmin /transfer myDownloadJob /download /priority normal https://downloadsrv/10mb.zip c:\\10mb.zip`

BITSAdmin continues to show progress information in the MS-DOS window until the transfer completes or an error occurs.

Create a download job

To create a download job named *myDownloadJob*:

```
bitsadmin /create myDownloadJob
```

BITSAdmin returns a GUID that uniquely identifies the job. Use the GUID or job name in subsequent calls. The following text is sample output.

Sample output

`created job {C775D194-090F-431F-B5FB-8334D00D1CB6}`

Add files to the download job

To add a file to the job:

```
bitsadmin /addfile myDownloadJob https://downloadsrv/10mb.zip c:\\10mb.zip
```

Repeat this call for each file you want to add. If multiple jobs use *myDownloadJob* as their name, you must use the job's GUID to uniquely identify it for completion.

Activate the download job

After you create a new job, BITS automatically suspends the job. To activate the job in the transfer queue:

```
bitsadmin /resume myDownloadJob
```

If multiple jobs use *myDownloadJob* as their name, you must use the job's GUID to uniquely identify it for completion.

Determine the progress of the download job

The **/info** switch returns the state of the job and the number of files and bytes transferred. When the state is shown as `TRANSFERRED`, it means that BITS has successfully transferred all files in the job. You can also add the **/verbose** argument to get complete details of the job, and **/list** or **/monitor** to get all the jobs in the transfer queue.

To return the state of the job:

```
bitsadmin /info myDownloadJob /verbose
```

If multiple jobs use *myDownloadJob* as their name, you must use the job's GUID to uniquely identify it for completion.

Complete the download job

To complete the job after the state changes to `TRANSFERRED`:

```
bitsadmin /complete myDownloadJob
```

You must run the `/complete` switch before the files in the job become available. If multiple jobs use *myDownloadJob* as their name, you must use the job's GUID to

uniquely identify it for completion.

Monitor jobs in the transfer queue using the /list switch

To return the state of the job and the number of files and bytes transferred for all jobs in the transfer queue:

```
bitsadmin /list
```

Sample output

```
{6AF46E48-41D3-453F-B7AF-A694BBC823F7} job1 SUSPENDED 0 / 0 0 / 0
{482FCAF0-74BF-469B-8929-5CCD028C9499} job2 TRANSIENT_ERROR 0 / 1 0 /
UNKNOWN

Listed 2 job(s).
```

Monitor jobs in the transfer queue using the /monitor switch

To return the state of the job and the number of files and bytes transferred for all jobs in the transfer queue, refreshing the data every 5 seconds:

```
bitsadmin /monitor
```

> ⓘ **Note**
>
> To stop the refresh, press CTRL+C.

Sample output

```
MONITORING BACKGROUND COPY MANAGER(5 second refresh)
{6AF46E48-41D3-453F-B7AF-A694BBC823F7} job1 SUSPENDED 0 / 0 0 / 0
{482FCAF0-74BF-469B-8929-5CCD028C9499} job2 TRANSIENT_ERROR 0 / 1 0 /
UNKNOWN
{0B138008-304B-4264-B021-FD04455588FF} job3 TRANSFERRED 1 / 1 100379370 /
100379370
```

Monitor jobs in the transfer queue using the /info switch

To return the state of the job and the number of files and bytes transferred:

```

bitsadmin /info
```

Sample output

```

GUID: {482FCAF0-74BF-469B-8929-5CCD028C9499} DISPLAY: myDownloadJob
TYPE: DOWNLOAD STATE: TRANSIENT_ERROR OWNER: domain\user
PRIORITY: NORMAL FILES: 0 / 1 BYTES: 0 / UNKNOWN
CREATION TIME: 12/17/2002 1:21:17 PM MODIFICATION TIME: 12/17/2002 1:21:30
PM
COMPLETION TIME: UNKNOWN
NOTIFY INTERFACE: UNREGISTERED NOTIFICATION FLAGS: 3
RETRY DELAY: 600 NO PROGRESS TIMEOUT: 1209600 ERROR COUNT: 0
PROXY USAGE: PRECONFIG PROXY LIST: NULL PROXY BYPASS LIST: NULL
ERROR FILE:    https://downloadsrv/10mb.zip -> c:\10mb.zip
ERROR CODE:    0x80072ee7 - The server name or address could not be resolved
ERROR CONTEXT: 0x00000005 - The error occurred while the remote file was
being
processed.
DESCRIPTION:
JOB FILES:
0 / UNKNOWN WORKING https://downloadsrv/10mb.zip -> c:\10mb.zip
NOTIFICATION COMMAND LINE: none
```

Delete jobs from the transfer queue

To remove all jobs from the transfer queue, use the /reset switch:

```

```

```
bitsadmin /reset
```

Sample output

```
{DC61A20C-44AB-4768-B175-8000D02545B9} canceled.
{BB6E91F3-6EDA-4BB4-9E01-5C5CBB5411F8} canceled.
2 out of 2 jobs canceled.
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getaclflags

Article • 02/03/2023

Retrieves the access control list (ACL) propagations flags, reflecting whether items are inherited by child objects.

Syntax

```
bitsadmin /getaclflags <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Remarks

Returns one or more of the following flag values:

- **o** - Copy owner information with file.
- **g** - Copy group information with file.
- **d** - Copy discretionary access control list (DACL) information with file.
- **s** - Copy system access control list (SACL) information with file.

Examples

To retrieve the access control list propagation flags for the job named *myDownloadJob*:

```
bitsadmin /getaclflags myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getbytestotal

Article • 02/03/2023

Retrieves the size of the specified job.

Syntax

```
bitsadmin /getbytestotal <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the size of the job named *myDownloadJob*:

```
bitsadmin /getbytestotal myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getbytestransferred

Article • 02/03/2023

Retrieves the number of bytes transferred for the specified job.

Syntax

```
bitsadmin /getbytestransferred <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the number of bytes transferred for the job named *myDownloadJob*:

```
bitsadmin /getbytestransferred myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getclientcertificate

Article • 02/03/2023

Retrieves the client certificate from the job.

Syntax

```
bitsadmin /getclientcertificate <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the client certificate for the job named *myDownloadJob*:

```
bitsadmin /getclientcertificate myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getcompletiontime

Article • 02/03/2023

Retrieves the time that the job finished transferring data.

Syntax

```
bitsadmin /getcompletiontime <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the time that the job named *myDownloadJob* finished transferring data:

```
bitsadmin /getcompletiontime myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getcreationtime

Article • 02/03/2023

Retrieves the creation time for the specified job.

Syntax

```
bitsadmin /getcreationtime <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the creation time for the job named *myDownloadJob*:

```
bitsadmin /getcreationtime myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getcustomheaders

Article • 02/03/2023

Retrieves the custom HTTP headers from the job.

Syntax

```
bitsadmin /getcustomheaders <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To get the custom headers for the job named *myDownloadJob*:

```
bitsadmin /getcustomheaders myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getdescription

Article • 02/03/2023

Retrieves the description of the specified job.

Syntax

```
bitsadmin /getdescription <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the description for the job named *myDownloadJob*:

```
bitsadmin /getdescription myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getdisplayname

Article • 02/03/2023

Retrieves the display name of the specified job.

Syntax

```
bitsadmin /getdisplayname <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the display name for the job named *myDownloadJob*:

```
bitsadmin /getdisplayname myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin geterror

Article • 02/03/2023

Retrieves detailed error information for the specified job.

Syntax

```
bitsadmin /geterror <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the error information for the job named *myDownloadJob*:

```
bitsadmin /geterror myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin geterrorcount

Article • 02/03/2023

Retrieves a count of the number of times the specified job generated a transient error.

Syntax

```
bitsadmin /geterrorcount <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve error count information for the job named *myDownloadJob*:

```
bitsadmin /geterrorcount myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getfilestotal

Article • 03/03/2021

Retrieves the number of files in the specified job.

Syntax

```
bitsadmin /getfilestotal <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the number of files included in the job named *myDownloadJob*:

```
bitsadmin /getfilestotal myDownloadJob
```

See Also

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getfilestransferred

Article • 02/03/2023

Retrieves the number of files transferred for the specified job.

Syntax

```
bitsadmin /getfilestransferred <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the number of files transferred in the job named *myDownloadJob*:

```
bitsadmin /getfilestransferred myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin gethelpertokenflags

Article • 02/03/2023

Returns the usage flags for a helper token that is associated with a BITS transfer job.

> **Note**
>
> This command isn't supported by BITS 3.0 and earlier.

Syntax

```
bitsadmin /gethelpertokenflags <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Remarks

Possible return values, including:

- **0x0001.** The helper token is used to open the local file of an upload job, to create or rename the temporary file of a download job, or to create or rename the reply file of an upload-reply job.
- **0x0002.** The helper token is used to open the remote file of a Server Message Block (SMB) upload or download job, or in response to an HTTP server or proxy challenge for implicit NTLM or Kerberos credentials. You must call `/SetCredentialsJob TargetScheme NULL NULL` to allow the credentials to be sent over HTTP.

Examples

To retrieve the usage flags for a helper token associated with a BITS transfer job named *myDownloadJob*:

```
bitsadmin /gethelpertokenflags myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin gethelpertokensid

Article • 02/03/2023

Returns the SID of a BITS transfer job's helper token, if one is set.

> **Note**
>
> This command isn't supported by BITS 3.0 and earlier.

Syntax

```
bitsadmin /gethelpertokensid <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the SID of a BITS transfer job named *myDownloadJob*:

```
bitsadmin /gethelpertokensid myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin gethttpmethod

Article • 02/03/2023

Gets the HTTP verb to use with the job.

Syntax

```
bitsadmin /gethttpmethod <Job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the HTTP verb to use with the job named *myDownloadJob*:

```
bitsadmin /gethttpmethod myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getmaxdownloadtime

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves the download timeout in seconds.

Syntax

```
bitsadmin /getmaxdownloadtime <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To get the maximum download time for the job named *myDownloadJob* in seconds:

```
bitsadmin /getmaxdownloadtime myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getminretrydelay

Article • 02/03/2023

Retrieves the length of time, in seconds, that the service will wait after encountering a transient error before trying to transfer the file.

Syntax

```
bitsadmin /getminretrydelay <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the minimum retry delay for the job named *myDownloadJob*:

```
bitsadmin /getminretrydelay myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getmodificationtime

Article • 02/03/2023

Retrieves the last time the job was modified or data was successfully transferred.

Syntax

```
bitsadmin /getmodificationtime <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the last modified time for the job named *myDownloadJob*:

```
bitsadmin /getmodificationtime myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getnoprogresstimeout

Article • 02/03/2023

Retrieves the length of time, in seconds, that the service will try to transfer the file after a transient error occurs.

Syntax

```
bitsadmin /getnoprogresstimeout <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the progress time out value for the job named *myDownloadJob*:

```
bitsadmin /getnoprogresstimeout myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getnotifycmdline

Article • 02/03/2023

Retrieves the command-line command to run after the specified job finishes transferring data.

> **Note**
>
> This command isn't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /getnotifycmdline <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the command-line command used by the service when the job named *myDownloadJob* completes.

```
bitsadmin /getnotifycmdline myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getnotifyflags

Article • 02/03/2023

Retrieves the notification flags for the specified job.

Syntax

```
bitsadmin /getnotifyflags <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Remarks

The job can contain one or more of the following notification flags:

Flag	Description
0x001	Generate an event when all files in the job have been transferred.
0x002	Generate an event when an error occurs.
0x004	Disable notifications.
0x008	Generate an event when the job is modified or transfer progress is made.

Examples

To retrieve the notify flags for the job named *myDownloadJob*:

```
bitsadmin /getnotifyflags myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getnotifyinterface

Article • 02/03/2023

Determines whether another program has registered a COM callback interface (the notify interface) for the specified job.

Syntax

```
bitsadmin /getnotifyinterface <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Output

The output for this command displays either, **Registered** or **Unregistered**.

> **Note**
>
> It's not possible to determine the program that registered the callback interface.

Examples

To retrieve the notify interface for the job named *myDownloadJob*:

```
bitsadmin /getnotifyinterface myDownloadJob
```

Related links

- Command-Line Syntax Key

- bitsadmin command

bitsadmin getowner

Article • 02/03/2023

Displays the display name or GUID of the owner of the specified job.

Syntax

```
bitsadmin /getowner <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To display the owner for the job named *myDownloadJob*:

```
bitsadmin /getowner myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getpeercachingflags

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves flags that determine if the files of the job can be cached and served to peers, and if BITS can download content for the job from peers.

Syntax

```
bitsadmin /getpeercachingflags <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the flags for the job named *myDownloadJob*:

```
bitsadmin /getpeercachingflags myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getpriority

Article • 02/03/2023

Retrieves the priority of the specified job.

Syntax

```
bitsadmin /getpriority <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Output

The returned priority for this command can be:

- **FOREGROUND**
- **HIGH**
- **NORMAL**
- **LOW**
- **UNKNOWN**

Examples

To retrieve the priority for the job named *myDownloadJob*:

```
bitsadmin /getpriority myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getproxybypasslist

Article • 05/22/2023

Applies to: Applies to: Windows Server (All supported versions)

The `bitsadmin /getproxybypasslist` command retrieves the proxy bypass list for the specified job.

Syntax

```
bitsadmin /getproxybypasslist <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Remarks

The bypass list contains the host names or IP addresses, or both, that aren't routed through a proxy. The list can contain `<local>` to refer to all servers on the same LAN. The list can be semicolon (;) or space-delimited.

Examples

To retrieve the proxy bypass list for the job named *myDownloadJob*:

```
bitsadmin /getproxybypasslist myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getproxylist

Article • 02/03/2023

Retrieves the comma-delimited list of proxy servers to use for the specified job.

Syntax

```
bitsadmin /getproxylist <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the proxy list for the job named *myDownloadJob*:

```
bitsadmin /getproxylist myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getproxyusage

Article • 02/03/2023

Retrieves the proxy usage setting for the specified job.

Syntax

```
bitsadmin /getproxyusage <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Output

The returned proxy usage values can be:

- **Preconfig** - Use the owner's Internet Explorer defaults.
- **No_Proxy** - Don't use a proxy server.
- **Override** - Use an explicit proxy list.
- **Autodetect** - Automatically detect the proxy settings.

Examples

To retrieve the proxy usage for the job named *myDownloadJob*:

```
bitsadmin /getproxyusage myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getreplydata

Article • 02/03/2023

Retrieves the server's upload-reply data in hexadecimal format for the job.

> **Note**
>
> This command isn't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /getreplydata <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the upload-reply data for the job named *myDownloadJob*:

```
bitsadmin /getreplydata myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getreplyfilename

Article • 02/03/2023

Gets the path of the file that contains the server upload-reply for the job.

> **Note**
>
> This command isn't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /getreplyfilename <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the upload-reply filename for the job named *myDownloadJob*:

```
bitsadmin /getreplyfilename myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getreplyprogress

Article • 02/03/2023

Retrieves the size and progress of the server upload-reply.

> **Note**
>
> This command isn't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /getreplyprogress <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the upload-reply progress for the job named *myDownloadJob*:

```
bitsadmin /getreplyprogress myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getsecurityflags

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Reports the HTTP security flags for URL redirection and checks performed on the server certificate during the transfer.

Syntax

```
bitsadmin /getsecurityflags <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the security flags from a job named *myDownloadJob*:

```
bitsadmin /getsecurityflags myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getstate

Article • 05/22/2023

Applies to: Windows Server (All supported versions)

The `bitsadmin /getstate` command retrieves the state of a specified job.

Syntax

```
bitsadmin /getstate <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Output

The returned output values can be:

State	Description
`Queued`	The job is waiting to run.
`Connecting`	BITS is contacting the server.
`Transferring`	BITS is transferring data.
`Transferred`	BITS has successfully transferred all files in the job.
`Suspended`	The job is paused.
`Error`	A nonrecoverable error occurred; the transfer isn't retried.
`Transient_Error`	A recoverable error occurred; the transfer retries when the minimum retry delay expires.
`Acknowledged`	The job completed.
`Canceled`	The job was canceled.

Examples

To retrieve the state for the job named *myDownloadJob*:

```
bitsadmin /getstate myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin gettemporaryname

Article • 02/03/2023

Reports the temporary filename of the given file within the job.

Syntax

```
bitsadmin /gettemporaryname <job> <file_index>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
file_index	Starts from 0.

Examples

To report the temporary filename of file 2 for the job named *myDownloadJob*:

```
bitsadmin /gettemporaryname myDownloadJob 1
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin gettype

Article • 02/03/2023

Retrieves the job type of the specified job.

Syntax

```
bitsadmin /gettype <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Output

The returned output values can be:

Type	Description
Download	The job is a download.
Upload	The job is an upload.
Upload-Reply	The job is an upload-reply.
Unknown	The job has an unknown type.

Examples

To retrieve the job type for the job named *myDownloadJob*:

```
bitsadmin /gettype myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin getvalidationstate

Article • 02/03/2023

Reports the content validation state of the given file within the job.

Syntax

```
bitsadmin /getvalidationstate <job> <file_index>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
file_index	Starts from 0.

Examples

To retrieve the content validation state of file 2 within the job named *myDownloadJob*:

```
bitsadmin /getvalidationstate myDownloadJob 1
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin help

Article • 01/26/2023

Applies to: Windows Server (All supported versions)

The bitsadmin help command displays help-related information about the bitsadmin command-line parameters and options.

Syntax

```
bitsadmin /help | /?
```

Examples

To retrieve the command-line help.

```
bitsadmin /help
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin info

Article • 02/03/2023

Displays summary information about the specified job.

Syntax

```
bitsadmin /info <job> [/verbose]
```

Parameters

Parameter	Description
job	The job's display name or GUID.
/verbose	Optional. Provides detailed information about each job.

Examples

To retrieve information about the job named *myDownloadJob*:

```
bitsadmin /info myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin info

bitsadmin list

Article • 02/03/2023

Lists the transfer jobs owned by the current user.

Syntax

```
bitsadmin /list [/allusers][/verbose]
```

Parameters

Parameter	Description
/allusers	Optional. Lists jobs for all users. You must have administrator privileges to use this parameter.
/verbose	Optional. Provides detailed information about each job.

Examples

To retrieve information about jobs owned by the current user.

```
bitsadmin /list
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin listfiles

Article • 02/03/2023

Lists the files in the specified job.

Syntax

```
bitsadmin /listfiles <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve the list of files for the job named *myDownloadJob*:

```
bitsadmin /listfiles myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin makecustomheaderswriteonly

Article • 02/03/2023

Make a job's Custom HTTP Headers write-only.

> **Important**
>
> This action can't be undone.

Syntax

```
bitsadmin /makecustomheaderswriteonly <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To make Custom HTTP Headers write-only for the job named *myDownloadJob*:

```
bitsadmin /makecustomheaderswriteonly myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin monitor

Article • 02/03/2023

Monitors jobs in the transfer queue that are owned by the current user.

Syntax

```
bitsadmin /monitor [/allusers] [/refresh <seconds>]
```

Parameters

Parameter	Description
/allusers	Optional. Monitors jobs for all users. You must have administrator privileges to use this parameter.
/refresh	Optional. Refreshes the data at an interval specified by `<seconds>`. The default refresh interval is five seconds. To stop the refresh, press CTRL+C.

Examples

To monitor the transfer queue for jobs owned by the current user and refreshes the information every 60 seconds.

```
bitsadmin /monitor /refresh 60
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin nowrap

Article • 02/03/2023

Truncates any line of output text extending beyond the right-most edge of the command window. By default, all switches, except the **monitor** switch, wrap the output. Specify the **nowrap** switch before other switches.

Syntax

```
bitsadmin /nowrap
```

Examples

To retrieve the state for the job named *myDownloadJob* while not wrapping the output:

```
bitsadmin /nowrap /getstate myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin peercaching

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Lists the /peercaching switches.

Lists the /peercaching switches.

Syntax

```
bitsadmin /peercaching /help
bitsadmin /peercaching /setconfigurationflags
bitsadmin /peercaching /getconfigurationflags
```

Parameters

Parameter	Description
bitsadmin peercaching and help	Displays the command-line usage for the /peercaching switches.
bitsadmin peercaching and setconfigurationflags	Sets the configuration flags that determine if the computer can serve content to peers and if it can download content from peers.
bitsadmin peercaching and getconfigurationflags	Gets the configuration flags that determine if the computer serves content to peers and if it can download content from peers.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin peercaching and getconfigurationflags

Article • 02/03/2023

Gets the configuration flags that determine if the computer serves content to peers and if it can download content from peers.

Syntax

```
bitsadmin /peercaching /getconfigurationflags <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To get the configuration flags for the job named *myDownloadJob*:

```
bitsadmin /peercaching /getconfigurationflags myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command
- bitsadmin peercaching command

bitsadmin peercaching and help

Article • 05/22/2023

Applies to: Windows Server (All supported versions)

The `bitsadmin` command displays the command-line usage for the `/peercaching` switch when combined with `/help` switch.

Syntax

The following syntax is used:

```
CLI
```

```
bitsadmin /peercaching /help
```

Examples

To display the command-line help for the `/peercaching` switches, run the following command.

```
CLI
```

```
bitsadmin /peercaching /help
```

Related links

- Command-Line Syntax Key
- bitsadmin command
- bitsadmin peercaching command

bitsadmin peercaching and setconfigurationflags

Article • 02/03/2023

Sets the configuration flags that determine if the computer can serve content to peers and if it can download content from peers.

Syntax

```
bitsadmin /peercaching /setconfigurationflags <job> <value>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
value	An unsigned integer with the following interpretation for the bits in the binary representation: • To allow the job's data to be downloaded from a peer, set the least significant bit. • To allow the job's data to be served to peers, set the second bit from the right.

Examples

To specify the job's data to be downloaded from peers for the job named *myDownloadJob*:

```
bitsadmin /peercaching /setconfigurationflags myDownloadJob 1
```

Related links

- Command-Line Syntax Key

- bitsadmin command
- bitsadmin peercaching command

bitsadmin peers

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Lists the available /peers switches.

Lists the available /peers switches.

```
bitsadmin /peers /help
bitsadmin /peers /discover
bitsadmin /peers /clear
bitsadmin /peers /list
```

Parameters

Parameter	Description
bitsadmin peers and help	Displays the command-line usage for the /peers switches.
bitsadmin peers and discover	Discovers peers again.
bitsadmin peers and clear	Clears the peers list.
bitsadmin peers and list	Lists all peers.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin peers and clear

Article • 05/22/2023

Applies to Windows Server (All supported versions)

The `bitsadmin /peers /clear` command clears the peer list.

Syntax

```
bitsadmin /peers /clear
```

Examples

To clear the peer list.

```
bitsadmin /peers /clear
```

Related links

- Command-Line Syntax Key
- bitsadmin command
- bitsadmin peers command

bitsadmin peers and discover

Article • 01/20/2023

Applies to: Windows Server (All supported versions)

The bitsadmin peers and discover command rediscovers peers.

Syntax

```
bitsadmin /peers /discover
```

Examples

To rediscover peers:

```
bitsadmin /peers /discover
```

Related links

- Command-Line Syntax Key
- bitsadmin command
- bitsadmin peers command

bitsadmin peers and help

Article • 02/03/2023

Displays the command-line usage for the **/peers** switches.

Syntax

```
bitsadmin /peers /help
```

Examples

To display the command-line usage for the **/peers** switches:

```
bitsadmin /peers /help
```

Related links

- Command-Line Syntax Key
- bitsadmin command
- bitsadmin peers command

bitsadmin peers and list

Article • 05/22/2023

Applies to: Windows Server (All supported versions)

The `bitsadmin` command lists all peers when it's combined with the **peers** and **list** switches.

Syntax

CLI

```
bitsadmin /peers /list
```

Examples

To list all peers:

CLI

```
bitsadmin /peers /list
```

Related links

- Command-Line Syntax Key
- bitsadmin command
- bitsadmin peers command

bitsadmin rawreturn

Article • 05/22/2023

Applies to: Windows Server (All supported versions)

The bitsadmin rawreturn command returns data suitable for parsing. Typically, you use this command with the **/create** and **/get*** switches to receive only the value. You must specify this switch before other switches.

> **Note**
>
> This command strips newline characters and formatting from the output.

Syntax

```
bitsadmin /rawreturn
```

Examples

To retrieve the raw data for the state of the job named *myDownloadJob*:

```
bitsadmin /rawreturn /getstate myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin removeclientcertificate

Article • 02/03/2023

Removes the client certificate from the job.

Syntax

```
bitsadmin /removeclientcertificate <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To remove the client certificate from the job named *myDownloadJob*:

```
bitsadmin /removeclientcertificate myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin removecredentials

Article • 02/03/2023

Removes credentials from a job.

> ⓘ Note
>
> This command isn't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /removecredentials <job> <target> <scheme>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
target	Use either **SERVER** or **PROXY**.
scheme	Use one of the following: • **BASIC.** Authentication scheme where the user name and password are sent in clear-text to the server or proxy. • **DIGEST.** A challenge-response authentication scheme that uses a server-specified data string for the challenge. • **NTLM.** A challenge-response authentication scheme that uses the credentials of the user for authentication in a Windows network environment. • **NEGOTIATE (also known as the Simple and Protected Negotiation protocol).** A challenge-response authentication scheme that negotiates with the server or proxy to determine which scheme to use for authentication. Examples are the Kerberos protocol and NTLM. • **PASSPORT.** A centralized authentication service provided by Microsoft that offers a single logon for member sites.

Examples

To remove credentials from the job named *myDownloadJob*:

```
bitsadmin /removecredentials myDownloadJob SERVER BASIC
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin replaceremoteprefix

Article • 03/03/2021

Changes the remote URL for all files in the job from *oldprefix* to *newprefix*, as necessary.

Syntax

```
bitsadmin /replaceremoteprefix <job> <oldprefix> <newprefix>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
oldprefix	Existing URL prefix.
newprefix	New URL prefix.

Examples

To change the remote URL for all files in job named *myDownloadJob*, from *http://stageserver* to *http://prodserver*.

```
bitsadmin /replaceremoteprefix myDownloadJob http://stageserver
http://prodserver
```

Additional information

- Command-Line Syntax Key
- bitsadmin command

bitsadmin reset

Article • 02/03/2023

Cancels all jobs in the transfer queue owned by the current user. You can't reset jobs created by Local System. Instead, you must be an administrator and use the task scheduler to schedule this command as a task using the Local System credentials.

> **Note**
>
> If you have administrator privileges in BITSAdmin 1.5 and earlier, the /reset switch will cancel all the jobs in the queue. Additionally, the /allusers option isn't supported.

Syntax

```
bitsadmin /reset [/allusers]
```

Parameters

Parameter	Description
/allusers	Optional. Cancels all jobs in the queue owned by the current user. You must have administrator privileges to use this parameter.

Examples

To cancel all the jobs in the transfer queue for the current user.

```
bitsadmin /reset
```

Related links

- Command-Line Syntax Key

- bitsadmin command

bitsadmin resume

Article • 02/03/2023

Activates a new or suspended job in the transfer queue. If you resumed your job by mistake, or simply need to suspend your job, you can use the bitsadmin suspend switch to suspend the job.

Syntax

```
bitsadmin /resume <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To resume the job named *myDownloadJob*:

```
bitsadmin /resume myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin suspend command
- bitsadmin command

bitsadmin setaclflag

Article • 02/03/2023

Sets the access control list (ACL) propagations flags for the job. The flags indicate that you want to maintain the owner and ACL information with the file being downloaded. For example, to maintain the owner and group with the file, set the **flags** parameter to `og`.

Syntax

```
bitsadmin /setaclflag <job> <flags>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
flags	Specify one or more of the values, including: • **o** - Copy owner information with file. • **g** - Copy group information with file. • **d** - Copy discretionary access control list (DACL) information with file. • **s** - Copy system access control list (SACL) information with file.

Examples

To set the access control list propagation flags for the job named *myDownloadJob*, so it maintains the owner and group information with the downloaded files.

```
bitsadmin /setaclflags myDownloadJob og
```

Related links

- Command-Line Syntax Key

- bitsadmin command

bitsadmin setclientcertificatebyid

Article • 02/03/2023

Specifies the identifier of the client certificate to use for client authentication in an HTTPS (SSL) request.

Syntax

```
bitsadmin /setclientcertificatebyid <job> <store_location> <store_name>
<hexadecimal_cert_id>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
store_location	Identifies the location of a system store to use for looking up the certificate, including: • CURRENT_USER • LOCAL_MACHINE • CURRENT_SERVICE • SERVICES • USERS • CURRENT_USER_GROUP_POLICY • LOCAL_MACHINE_GROUP_POLICY • LOCAL_MACHINE_ENTERPRISE.
store_name	The name of the certificate store, including: • CA (Certification Authority certificates) • MY (Personal certificates) • ROOT (Root certificates) • SPC (Software Publisher Certificate).
hexadecimal_cert_id	A hexadecimal number representing the hash of the certificate.

Examples

To specify the identifier of the client certificate to use for client authentication in an HTTPS (SSL) request for the job named *myDownloadJob*:

```
bitsadmin /setclientcertificatebyid myDownloadJob
BG_CERT_STORE_LOCATION_CURRENT_USER MY A106B52356D3FBCD1853A41B619358BD
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setclientcertificatebyname

Article • 02/03/2023

Specifies the subject name of the client certificate to use for client authentication in an HTTPS (SSL) request.

Syntax

```
bitsadmin /setclientcertificatebyname <job> <store_location> <store_name>
<subject_name>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
store_location	Identifies the location of a system store to use for looking up the certificate. Possible values include: • 1 (CURRENT_USER) • 2 (LOCAL_MACHINE) • 3 (CURRENT_SERVICE) • 4 (SERVICES) • 5 (USERS) • 6 (CURRENT_USER_GROUP_POLICY) • 7 (LOCAL_MACHINE_GROUP_POLICY) • 8 (LOCAL_MACHINE_ENTERPRISE)
store_name	The name of the certificate store. Possible values include: • CA (Certification Authority certificates) • MY (Personal certificates) • ROOT (Root certificates) • SPC (Software Publisher Certificate)
subject_name	Name of the certificate.

Examples

To specify the name of the client certificate *myCertificate* to use for client authentication in an HTTPS (SSL) request for the job named *myDownloadJob*:

```
bitsadmin /setclientcertificatebyname myDownloadJob 1 MY myCertificate
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setcredentials

Article • 02/03/2023

Adds credentials to a job.

> **Note**
>
> This command isn't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /setcredentials <job> <target> <scheme> <username> <password>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
target	Use either **SERVER** or **PROXY**.
scheme	Use one of the following: • **BASIC.** Authentication scheme where the user name and password are sent in clear-text to the server or proxy. • **DIGEST.** A challenge-response authentication scheme that uses a server-specified data string for the challenge. • **NTLM.** A challenge-response authentication scheme that uses the credentials of the user for authentication in a Windows network environment. • **NEGOTIATE (also known as the Simple and Protected Negotiation protocol).** A challenge-response authentication scheme that negotiates with the server or proxy to determine which scheme to use for authentication. Examples are the Kerberos protocol and NTLM. • **PASSPORT.** A centralized authentication service provided by Microsoft that offers a single logon for member sites.
user_name	The name of the user.
password	The password associated with the provided *Username*.

Examples

To add credentials to the job named *myDownloadJob*:

```
bitsadmin /setcredentials myDownloadJob SERVER BASIC Edward password20
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setcustomheaders

Article • 02/03/2023

Add a custom HTTP header to a GET request sent to an HTTP server. For more information about GET requests, see Method Definitions and Header Field Definitions.

Syntax

```
bitsadmin /setcustomheaders <job> <header1> <header2> <...>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
`<header1> <header2>` and so on	The custom headers for the job.

Examples

To add a custom HTTP header for the job named *myDownloadJob*:

```
bitsadmin /setcustomheaders myDownloadJob accept-encoding:deflate/gzip
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setdescription

Article • 02/03/2023

Sets the description for the specified job.

Syntax

```
bitsadmin /setdescription <job> <description>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
description	Text used to describe the job.

Examples

To retrieve the description for the job named *myDownloadJob*:

```
bitsadmin /setdescription myDownloadJob music_downloads
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setdisplayname

Article • 02/03/2023

Sets the display name for the specified job.

Syntax

```
bitsadmin /setdisplayname <job> <display_name>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
display_name	Text used as the displayed name for the specific job.

Examples

To set the display name for the job to *myDownloadJob*:

```
bitsadmin /setdisplayname myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin sethelpertoken

Article • 02/03/2023

Sets the current command prompt's primary token (or an arbitrary local user account's token, if specified) as a BITS transfer job's helper token.

> **Note**
>
> This command isn't supported by BITS 3.0 and earlier.

Syntax

```
bitsadmin /sethelpertoken <job> [<user_name@domain> <password>]
```

Parameters

Parameter	Description
job	The job's display name or GUID.
`<username@domain>` `<password>`	Optional. The local user account credentials for which token to use.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin sethelpertokenflags

Article • 02/03/2023

Sets the usage flags for a helper token that is associated with a BITS transfer job.

> **Note**
>
> This command isn't supported by BITS 3.0 and earlier.

Syntax

```
bitsadmin /sethelpertokenflags <job> <flags>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
flags	Possible helper token values, including: • **0x0001.** Used to open the local file of an upload job, to create or rename the temporary file of a download job, or to create or rename the reply file of an upload-reply job. • **0x0002.** Used to open the remote file of a Server Message Block (SMB) upload or download job, or in response to an HTTP server or proxy challenge for implicit NTLM or Kerberos credentials. You must call `/setcredentialsjob targetscheme null null` to send the credentials over HTTP.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin seththttpmethod

Article • 02/03/2023

Sets the HTTP verb to use.

Syntax

```
bitsadmin /seththttpmethod <job> <httpmethod>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
httpmethod	The HTTP verb to use. For information about available verbs, see Method Definitions.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setmaxdownloadtime

Article • 02/03/2023

Sets the download timeout in seconds.

Syntax

```
bitsadmin /setmaxdownloadtime <job> <timeout>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
timeout	The length for the download timeout, in seconds.

Examples

To set the timeout for the job named *myDownloadJob* to 10 seconds.

```
bitsadmin /setmaxdownloadtime myDownloadJob 10
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setminretrydelay

Article • 02/03/2023

Sets the minimum length of time, in seconds, that BITS waits after encountering a transient error before trying to transfer the file.

Syntax

```
bitsadmin /setminretrydelay <job> <retrydelay>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
retrydelay	Minimum length of time for BITS to wait after an error during transfer, in seconds.

Examples

To set the minimum retry delay to 35 seconds for the job named *myDownloadJob*:

```
bitsadmin /setminretrydelay myDownloadJob 35
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setnoprogresstimeout

Article • 02/03/2023

Sets the length of time, in seconds, that BITS tries to transfer the file after the first transient error occurs.

Syntax

```
bitsadmin /setnoprogresstimeout <job> <timeoutvalue>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
timeoutvalue	The length of time that BITS waits to transfer a file after the first error, in seconds.

Remarks

- The "no progress" timeout interval begins when the job encounters its first transient error.
- The timeout interval stops or resets when a byte of data is successfully transferred.
- If the "no progress" timeout interval exceeds the *timeoutvalue*, then the job is placed in a fatal error state.

Examples

To set the "no progress" timeout value to 20 seconds, for the job named *myDownloadJob*:

```
bitsadmin /setnoprogresstimeout myDownloadJob 20
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setnotifycmdline

Article • 02/03/2023

Sets the command-line command that runs after the job finishes transferring data or after a job enters a specified state.

> **Note**
>
> This command isn't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /setnotifycmdline <job> <program_name> [program_parameters]
```

Parameters

Parameter	Description
job	The job's display name or GUID.
program_name	Name of the command to run when the job completes. You can set this value as NULL, but if you do, *program_parameters* must also be set to NULL.
program_parameters	Parameters that you want to pass to *program_name*. You can set this value as NULL. If *program_parameters* isn't set to NULL, then the first parameter in *program_parameters* must match the *program_name*.

Examples

To run Notepad.exe at the completion of the job named *myDownloadJob*:

```
bitsadmin /setnotifycmdline myDownloadJob c:\winnt\system32\notepad.exe NULL
```

To show the EULA text in Notepad.exe, at the completion of the job named myDownloadJob:

```
bitsadmin /setnotifycmdline myDownloadJob c:\winnt\system32\notepad.exe
notepad c:\eula.txt
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setnotifyflags

Article • 02/03/2023

Sets the event notification flags for the specified job.

Syntax

```
bitsadmin /setnotifyflags <job> <notifyflags>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
notifyflags	Can include one or more of the following notification flags, including: • **1.** Generates an event when all files in the job have been transferred. • **2.** Generates an event when an error occurs. • **3.** Generates an event when all files have completed transfer or when an error occurs. • **4.** Disables notifications.

Examples

To set the notification flags to generate an event when an error occurs, for a job named *myDownloadJob*:

```
bitsadmin /setnotifyflags myDownloadJob 2
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setpeercachingflags

Article • 02/03/2023

Sets flags that determine if the files of the job can be cached and served to peers and if the job can download content from peers.

Syntax

```
bitsadmin /setpeercachingflags <job> <value>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
value	An unsigned integer, including: • **1.** The job can download content from peers. • **2.** The files of the job can be cached and served to peers.

Examples

To allow the job named *myDownloadJob* to download content from peers:

```
bitsadmin /setpeercachingflags myDownloadJob 1
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setpriority

Article • 02/03/2023

Sets the priority of the specified job.

Syntax

```
bitsadmin /setpriority <job> <priority>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
priority	Sets the priority of the job, including: • FOREGROUND • HIGH • NORMAL • LOW

Examples

To set the priority for the job named *myDownloadJob* to normal:

```
bitsadmin /setpriority myDownloadJob NORMAL
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setproxysettings

Article • 02/03/2023

Sets the proxy settings for the specified job.

Syntax

```
bitsadmin /setproxysettings <job> <usage> [list] [bypass]
```

Parameters

Parameter	Description
job	The job's display name or GUID.
usage	Sets the proxy usage, including: • **PRECONFIG.** Use the owner's Internet Explorer defaults. • **NO_PROXY.** Don't use a proxy server. • **OVERRIDE.** Use an explicit proxy list and bypass list. The proxy list and proxy bypass information must follow. • **AUTODETECT.** Automatically detects proxy settings.
list	Used when the *Usage* parameter is set to OVERRIDE. Must contain a comma-delimited list of proxy servers to use.
bypass	Used when the *Usage* parameter is set to OVERRIDE. Must contain a space-delimited list of host names or IP addresses, or both, for which transfers are not to be routed through a proxy. This can be `<local>` to refer to all servers on the same LAN. Values of NULL may be used for an empty proxy bypass list.

Examples

To set the proxy settings using the various usage options for the job named *myDownloadJob*:

```
bitsadmin /setproxysettings myDownloadJob PRECONFIG
```

```
```

```
bitsadmin /setproxysettings myDownloadJob NO_PROXY
```

```
bitsadmin /setproxysettings myDownloadJob OVERRIDE proxy1:80
```

```
bitsadmin /setproxysettings myDownloadJob OVERRIDE proxy1,proxy2,proxy3 NULL
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setreplyfilename

Article • 02/03/2023

Specifies the path of the file that contains the server upload-reply.

> ⓘ Note
>
> This command isn't supported by BITS 1.2 and earlier.

Syntax

```
bitsadmin /setreplyfilename <job> <file_path>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
file_path	Location to put the server upload-reply.

Examples

To set the upload-reply filename file path for the job named *myDownloadJob*:

```
bitsadmin /setreplyfilename myDownloadJob c:\upload-reply
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setsecurityflags

Article • 02/03/2023

Sets security flags for HTTP to determine if BITS should check the certificate revocation list, ignore certain certificate errors, and define the policy to use when a server redirects the HTTP request. The value is an unsigned integer.

Syntax

```
bitsadmin /setsecurityflags <job> <value>
```

Parameters

Parameter	Description
job	The job's display name or GUID.
value	Can include one or more of the following notification flags, including: • Set the least significant bit to enable CRL Check. • Set the 2nd bit from the right to ignore incorrect common names in the server certificate. • Set the 3rd bit from the right to ignore incorrect dates in the server certificate. • Set the 4th bit from the right to ignore incorrect certification authorities in the server certificate. • Set the 5th bit from the right to ignore incorrect usage of the server certificate. • Set the 9th through the 11th bits from the right to implement your specified redirection policy, including: ◦ **0,0,0.** Redirects are automatically allowed. ◦ **0,0,1.** Remote name in the **IBackgroundCopyFile** interface is updated if a redirect occurs. ◦ **0,1,0.** BITS fails the job if a redirect occurs. • Set the 12th bit from the right to allow redirection from HTTPS to HTTP.

Examples

To set the security flags to enable a CRL check for the job named *myDownloadJob*:

```
bitsadmin /setsecurityflags myDownloadJob 0x0001
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin setvalidationstate

Article • 02/03/2023

Sets the content validation state of the given file within the job.

Syntax

```
bitsadmin /setvalidationstate <job> <file_index> <TRUE|FALSE>
```

Parameters

Parameter	Description
Job	The job's display name or GUID.
file_index	Starts at 0.
TRUE or FALSE	**TRUE** turns on content validation for the specified file, while **FALSE** turns it off.

Examples

To set the content validation state of file 2 to TRUE for the job named *myDownloadJob*:

```
bitsadmin /setvalidationstate myDownloadJob 2 TRUE
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin suspend

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Suspends the specified job. If you suspended your job by mistake, you can use the bitsadmin resume switch to restart the job.

Syntax

```
bitsadmin /suspend <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Example

To suspend the job named *myDownloadJob*:

```
bitsadmin /suspend myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin resume command
- bitsadmin command

bitsadmin takeownership

Article • 02/03/2023

Lets a user with administrative privileges take ownership of the specified job.

Syntax

```
bitsadmin /takeownership <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To take ownership of the job named *myDownloadJob*:

```
bitsadmin /takeownership myDownloadJob
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin transfer

Article • 02/03/2023

Transfers one or more files. By default, the BITSAdmin service creates a download job that runs at **NORMAL** priority and updates the command window with progress information until the transfer is complete or until a critical error occurs,

The service completes the job if it successfully transfers all the files and cancels the job if a critical error occurs. The service does not create the job if it is unable to add files to the job or if you specify an invalid value for *type* or *job_priority*. To transfer more than one file, specify multiple `<RemoteFileName>-<LocalFileName>` pairs. The pairs must be space-delimited.

> **Note**
>
> The BITSAdmin command continues to run if a transient error occurs. To end the command, press CTRL+C.

Syntax

```
bitsadmin /transfer <name> [<type>] [/priority <job_priority>] [/ACLflags
<flags>] [/DYNAMIC] <remotefilename> <localfilename>
```

Parameters

Parameter	Description
name	The name of the job. This command can't be a GUID.
type	Optional. Sets the type of job, including: • **/DOWNLOAD.** The default value. Choose this type for download jobs. • **/UPLOAD.** Choose this type for upload jobs.
priority	Optional. Sets the priority of the job, including: • FOREGROUND • HIGH • NORMAL • LOW

Parameter	Description
ACLflags	Optional. Indicates that you want to maintain the owner and ACL information with the file being downloaded. Specify one or more of the values, including: • **o** - Copy owner information with file. • **g** - Copy group information with file. • **d** - Copy discretionary access control list (DACL) information with file. • **s** - Copy system access control list (SACL) information with file.
/DYNAMIC	Configures the job using **BITS_JOB_PROPERTY_DYNAMIC_CONTENT**, which relaxes the server-side requirements.
remotefilename	The name of the file after it's transferred to the server.
localfilename	The name of the file that resides locally.

Examples

To start a transfer job named *myDownloadJob*:

```
bitsadmin /transfer myDownloadJob http://prodserver/audio.wma
c:\downloads\audio.wma
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin util

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Lists the **/util** switches.

Lists the **util** switches.

Syntax

```
bitsadmin /util /help
bitsadmin /util /getieproxy
bitsadmin /util /repairservice
bitsadmin /util /setieproxy
bitsadmin /util /version
```

Parameters

Parameter	Description
bitsadmin util and help	Displays the command-line usage for the /Util switches. You can also specify /?.
bitsadmin util and getieproxy	Retrieves the proxy usage for the given service account.
bitsadmin util and repairservice	Repairs known issues with BITS service.
bitsadmin util and setieproxy	Specifies proxy settings to use when transferring files using a service account.
bitsadmin util and version	Displays the version of the BITS service.

Related links

- Command-Line Syntax Key
- bitsadmin command

bitsadmin util and enableanalyticchannel

Article • 02/03/2023

Enables or disables the BITS client analytic channel.

Syntax

```
bitsadmin /util /enableanalyticchannel TRUE|FALSE
```

Parameter	Description
TRUE or FALSE	**TRUE** turns on content validation for the specified file, while **FALSE** turns it off.

Examples

To turn the BITS client analytic channel on or off.

```
bitsadmin /util / enableanalyticchannel TRUE
```

Related links

- Command-Line Syntax Key
- bitsadmin util command
- bitsadmin command

bitsadmin util and getieproxy

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves the proxy usage for the given service account. This command shows the value for each proxy usage, not just the proxy usage you specified for the service account. For details about setting the proxy usage for specific service accounts, see the bitsadmin util and setieproxy command.

Syntax

```
bitsadmin /util /getieproxy <account> [/conn <connectionname>]
```

Parameters

Parameter	Description
account	Specifies the service account whose proxy settings you want to retrieve. Possible values include: • LOCALSYSTEM • NETWORKSERVICE • LOCALSERVICE.
connectionname	Optional. Used with the **/conn** parameter to specify which modem connection to use. If you don't specify the **/conn** parameter, BITS uses the LAN connection.

Examples

To display the proxy usage for the NETWORK SERVICE account:

```
bitsadmin /util /getieproxy NETWORKSERVICE
```

Related links

- Command-Line Syntax Key
- bitsadmin util command
- bitsadmin command

bitsadmin util and help

Article • 05/22/2023

Applies to: Windows Server (All supported versions)

Display help for the `bitsadmin util` command switch when combined with the **help** switch.

Syntax

```
bitsadmin /util /help
```

Examples

Display the command-line help for the **/util** switches by running the following command.

CLI

```
bitsadmin /util /help
```

Related links

- Command-Line Syntax Key
- bitsadmin util command
- bitsadmin command

bitsadmin util and repairservice

Article • 02/03/2023

If BITS fails to start, this switch attempts to resolve errors related to incorrect service configuration and dependencies on Windows services (such as LANManworkstation) and the network directory. This switch also generates output that indicates if the issues that were resolved.

> **Note**
>
> This command isn't supported by BITS 1.5 and earlier.

Syntax

```
bitsadmin /util /repairservice [/force]
```

Parameters

Parameter	Description
/force	Optional. Deletes and creates the service again.

> **Note**
>
> If BITS creates the service again, the service description string might be set to English even in a localized system.

Examples

To repair the BITS service configuration:

```
bitsadmin /util /repairservice
```

Related links

- Command-Line Syntax Key
- bitsadmin util command
- bitsadmin command

bitsadmin util and setieproxy

Article • 02/03/2023

Set the proxy settings to use when transferring files using a service account. You must run this command from an elevated command prompt for it to complete successfully.

> **Note**
>
> This command isn't supported by BITS 1.5 and earlier.

Syntax

```
bitsadmin /util /setieproxy <account> <usage> [/conn <connectionname>]
```

Parameters

Parameter	Description
account	Specifies the service account whose proxy settings you want to define. Possible values include: • LOCALSYSTEM • NETWORKSERVICE • LOCALSERVICE.

Parameter	Description
usage	Specifies the form of proxy detection to use. Possible values include: • **NO_PROXY.** Don't use a proxy server. • **AUTODETECT.** Automatically detect the proxy settings. • **MANUAL_PROXY.** Use a specified proxy list and bypass list. You must specify your lists immediately after the usage tag. For example, `MANUAL_PROXY proxy1,proxy2 NULL`. ◦ **Proxy list.** A comma-delimited list of proxy servers to use. ◦ **Bypass list.** A space-delimited list of host names or IP addresses, or both, for which transfers are not to be routed through a proxy. This can be <local> to refer to all servers on the same LAN. Values of NULL or may be used for an empty proxy bypass list. • **AUTOSCRIPT.** Same as **AUTODETECT**, except it also runs a script. You must specify the script URL immediately after the usage tag. For example, `AUTOSCRIPT http://server/proxy.js`. • **RESET.** Same as **NO_PROXY**, except it removes the manual proxy URLs (if specified) and any URLs discovered using automatic detection.
connectionname	Optional. Used with the **/conn** parameter to specify which modem connection to use. If you don't specify the **/conn** parameter, BITS uses the LAN connection.

Remarks

Each successive call using this switch replaces the previously specified usage, but not the parameters of the previously defined usage. For example, if you specify **NO_PROXY**, **AUTODETECT**, and **MANUAL_PROXY** on separate calls, BITS uses the last supplied usage, but keeps the parameters from the previously defined usage.

Examples

To set the proxy usage for the LOCALSYSTEM account:

```
bitsadmin /util /setieproxy localsystem AUTODETECT
```

```
bitsadmin /util /setieproxy localsystem MANUAL_PROXY proxy1,proxy2,proxy3
NULL
```

```
bitsadmin /util /setieproxy localsystem MANUAL_PROXY proxy1:80
```

Related links

- Command-Line Syntax Key
- bitsadmin util command
- bitsadmin command

bitsadmin util and version

Article • 02/03/2023

Displays the version of BITS service (for example, 2.0).

> **Note**
>
> This command isn't supported by BITS 1.5 and earlier.

Syntax

```
bitsadmin /util /version [/verbose]
```

Parameters

Parameter	Description
/verbose	Use this switch to display the file version for each BITS-related DLL and to verify whether the BITS service can start.

Examples

To display the version of the BITS Service.

```
bitsadmin /util /version
```

Related links

- Command-Line Syntax Key
- bitsadmin util command
- bitsadmin command

bitsadmin wrap

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Wraps any line of output text extending beyond the rightmost edge of the command window to the next line. You must specify this switch before any other switches.

By default, all switches except the bitsadmin monitor switch, wrap the output text.

Syntax

```
bitsadmin /wrap <job>
```

Parameters

Parameter	Description
job	The job's display name or GUID.

Examples

To retrieve information for the job named *myDownloadJob* and wrap the output text:

```
bitsadmin /wrap /info myDownloadJob /verbose
```

Related links

- Command-Line Syntax Key
- bitsadmin command

bootcfg

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configures, queries, or changes Boot.ini file settings.

Syntax

```
bootcfg <parameter> [arguments...]
```

Parameters

Parameter	Description
bootcfg addsw	Adds operating system load options for a specified operating system entry.
bootcfg copy	Makes a copy of an existing boot entry, to which you can add command-line options.
bootcfg dbg1394	Configures 1394 port debugging for a specified operating system entry.
bootcfg debug	Adds or changes the debug settings for a specified operating system entry.
bootcfg default	Specifies the operating system entry to designate as the default.
bootcfg delete	Deletes an operating system entry in the [operating systems] section of the Boot.ini file.
bootcfg ems	Enables the user to add or change the settings for redirection of the Emergency Management Services console to a remote computer.
bootcfg query	Queries and displays the [boot loader] and [operating systems] section entries from Boot.ini.
bootcfg raw	Adds operating system load options specified as a string to an operating system entry in the [operating systems] section of the Boot.ini file.

Parameter	Description
bootcfg rmsw	Removes operating system load options for a specified operating system entry.
bootcfg timeout	Changes the operating system time-out value.

bootcfg addsw

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds operating system load options for a specified operating system entry.

Syntax

```
bootcfg /addsw [/s <computer> [/u <domain>\<user> /p <password>]] [/mm
<maximumram>] [/bv] [/so] [/ng] /id <osentrylinenum>
```

Parameters

Term	Definition
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
`/mm <maximumram>`	Specifies the maximum amount of RAM, in megabytes, that the operating system can use. The value must be equal to or greater than 32 Megabytes.
/bv	Adds the **/basevideo** option to the specified `<osentrylinenum>`, directing the operating system to use standard VGA mode for the installed video driver.
/so	Adds the **/sos** option to the specified `<osentrylinenum>`, directing the operating system to display device driver names while they are being loaded.
/ng	Adds the **/noguiboot** option to the specified `<osentrylinenum>`, disabling the progress bar that appears before the CTRL+ALT+DEL logon prompt.
`/id <osentrylinenum>`	Specifies the operating system entry line number in the [operating systems] section of the Boot.ini file to which the operating system load options are added. The first line after the [operating systems] section header is 1.

Term	Definition
/?	Displays help at the command prompt.

Examples

To use the **bootcfg /addsw** command:

```
bootcfg /addsw /mm 64 /id 2
bootcfg /addsw /so /id 3
bootcfg /addsw /so /ng /s srvmain /u hiropln /id 2
bootcfg /addsw /ng /id 2
bootcfg /addsw /mm 96 /ng /s srvmain /u maindom\hiropln /p p@ssW23 /id 2
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg copy

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Makes a copy of an existing boot entry, to which you can add command-line options.

Syntax

```
bootcfg /copy [/s <computer> [/u <domain>\<user> /p <password>]] [/d
<description>] [/id <osentrylinenum>]
```

Parameters

Parameter	Description
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
`/d <description>`	Specifies the description for the new operating system entry.
`/id <osentrylinenum>`	Specifies the operating system entry line number in the [operating systems] section of the Boot.ini file to which the operating system load options are added. The first line after the [operating systems] section header is 1.
/?	Displays help at the command prompt.

Examples

To copy boot entry 1 and enter \ABC Server\ as the description:

```
bootcfg /copy /d \ABC Server\ /id 1
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg dbg1394

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configures 1394 port debugging for a specified operating system entry.

Syntax

```
bootcfg /dbg1394 {on | off}[/s <computer> [/u <domain>\<user> /p
<password>]] [/ch <channel>] /id <osentrylinenum>
```

Parameters

Parameter	Description
`{on | off}`	Specifies the value for 1394 port debugging, including: • **on.** Enables remote debugging support by adding the /dbg1394 option to the specified `<osentrylinenum>`. • **off.** Disables remote debugging support by removing the /dbg1394 option from the specified `<osentrylinenum>`.
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
`/ch <channel>`	Specifies the channel to use for debugging. Valid values include integers, between 1 and 64. Don't use this parameter if 1394 port debugging is disabled.
`/id <osentrylinenum>`	Specifies the operating system entry line number in the [operating systems] section of the Boot.ini file to which the operating system load options are added. The first line after the [operating systems] section header is 1.

Parameter	Description
/?	Displays help at the command prompt.

Examples

To use the **bootcfg /dbg1394**command:

```
bootcfg /dbg1394 /id 2
bootcfg /dbg1394 on /ch 1 /id 3
bootcfg /dbg1394 edit /ch 8 /id 2
bootcfg /s srvmain /u maindom\hiropln /p p@ssW23 /dbg1394 off /id 2
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg debug

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds or changes the debug settings for a specified operating system entry.

> **Note**
>
> If you're attempting to debug port 1394, use the **bootcfg dbg1394** command instead.

Syntax

```
bootcfg /debug {on | off | edit}[/s <computer> [/u <domain>\<user> /p
<password>]] [/port {COM1 | COM2 | COM3 | COM4}] [/baud {9600 | 19200 |
38400 | 57600 | 115200}] [/id <osentrylinenum>]
```

Parameters

Parameter	Description
`{on | off | edit}`	Specifies the value for port debugging, including: • **on.** Enables remote debugging support by adding the /debug option to the specified `<osentrylinenum>`. • **off.** Disables remote debugging support by removing the /debug option from the specified `<osentrylinenum>`. • **edit.** Allows changes to port and baud rate settings by changing the values associated with the /debug option for the specified `<osentrylinenum>`.
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.

Parameter	Description
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
`/port {COM1 | COM2 | COM3 | COM4}`	Specifies the COM port to be used for debugging. Don't use this parameter if debugging is disabled.
`/baud {9600 | 19200 | 38400 | 57600 | 115200}`	Specifies the baud rate to be used for debugging. Don't use this parameter if debugging is disabled.
`/id <osentrylinenum>`	Specifies the operating system entry line number in the [operating systems] section of the Boot.ini file to which the operating system load options are added. The first line after the [operating systems] section header is 1.
/?	Displays help at the command prompt.

Examples

To use the **bootcfg /debug** command:

```
bootcfg /debug on /port com1 /id 2
bootcfg /debug edit /port com2 /baud 19200 /id 2
bootcfg /s srvmain /u maindom\hiropln /p p@ssW23 /debug off /id 2
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg default

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Specifies the operating system entry to designate as the default.

Syntax

```
bootcfg /default [/s <computer> [/u <domain>\<user> /p <password>]] [/id
<osentrylinenum>]
```

Parameters

Parameter	Description
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
`/id <osentrylinenum>`	Specifies the operating system entry line number in the [operating systems] section of the Boot.ini file to which the operating system load options are added. The first line after the [operating systems] section header is 1.
/?	Displays help at the command prompt.

Examples

To use the **bootcfg /default** command:

```
bootcfg /default /id 2
bootcfg /default /s srvmain /u maindom\hiropln /p p@ssW23 /id 2
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg delete

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Deletes an operating system entry in the [operating systems] section of the Boot.ini file.

Syntax

```
bootcfg /delete [/s <computer> [/u <domain>\<user> /p <password>]] [/id
<osentrylinenum>]
```

Parameters

Parameter	Description
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
`/id <osentrylinenum>`	Specifies the operating system entry line number in the [operating systems] section of the Boot.ini file to which the operating system load options are added. The first line after the [operating systems] section header is 1.
/?	Displays help at the command prompt.

Examples

To use the **bootcfg /delete** command:

```
bootcfg /delete /id 1
bootcfg /delete /s srvmain /u maindom\hiropln /p p@ssW23 /id 3
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg ems

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables the user to add or change the settings for redirection of the Emergency Management Services console to a remote computer. Enabling Emergency Management Services, adds a `redirect=Port#` line to the [boot loader] section of the Boot.ini file along with a /redirect option to the specified operating system entry line. The Emergency Management Services feature is enabled only on servers.

Syntax

```
bootcfg /ems {on | off | edit}[/s <computer> [/u <domain>\<user> /p
<password>]] [/port {COM1 | COM2 | COM3 | COM4 | BIOSSET}] [/baud {9600 |
19200 | 38400 | 57600 | 115200}] [/id <osentrylinenum>]
```

Parameters

Parameter	Description
`{on | off | edit}`	Specifies the value for Emergency Management Services redirection, including: • **on.** Enables remote output for the specified `<osentrylinenum>`. Also adds a /redirect option to the specified `<osentrylinenum>` and a `redirect=com<X>` setting to the [boot loader] section. The value of `com<X>` is set by the **/port** parameter. • **off.** Disables output to a remote computer. Also removes the /redirect option to the specified `<osentrylinenum>` and the `redirect=com<X>` setting from the [boot loader] section. • **edit.** Allows changes to port settings by changing the `redirect=com<X>` setting in the [boot loader] section. The value of `com<X>` is set by the **/port** parameter.
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.

Parameter	Description
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
`/port {COM1 | COM2 | COM3 | COM4 | BIOSSET}`	Specifies the COM port to be used for redirection. The BIOSSET parameter directs Emergency Management Services to get the BIOS settings to determine which port should be used for redirection. Don't use this parameter if remotely administered output is disabled.
`/baud {9600 | 19200 | 38400 | 57600 | 115200}`	Specifies the baud rate to be used for redirection. Don't use this parameter if remotely administered output is disabled.
`/id <osentrylinenum>`	Specifies the operating system entry line number to which the Emergency Management Services option is added in the [operating systems] section of the Boot.ini file. The first line after the [operating systems] section header is 1. This parameter is required when the Emergency Management Services value is set to **on** or **off**.
/?	Displays help at the command prompt.

Examples

To use the **bootcfg /ems** command:

```
bootcfg /ems on /port com1 /baud 19200 /id 2
bootcfg /ems on /port bioset /id 3
bootcfg /s srvmain /ems off /id 2
bootcfg /ems edit /port com2 /baud 115200
bootcfg /s srvmain /u maindom\hiropln /p p@ssW23 /ems off /id 2
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg query

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Queries and displays the [boot loader] and [operating systems] section entries from Boot.ini.

Syntax

```
bootcfg /query [/s <computer> [/u <domain>\<user> /p <password>]]
```

Parameters

Parameter	Description
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
/?	Displays help at the command prompt.

Sample output

Sample output for the **bootcfg /query** command:

```
Boot Loader Settings
----------
timeout: 30
default: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
Boot Entries
```

```
------
Boot entry ID:   1
Friendly Name:
path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
OS Load Options: /fastdetect /debug /debugport=com1:
```

- The **Boot Loader Settings** area shows each entry in the [boot loader] section of Boot.ini.
- The **Boot Entries** area shows more details for each operating system entry in the [operating systems] section of the Boot.ini

Examples

To use the **bootcfg /query** command:

```
bootcfg /query
bootcfg /query /s srvmain /u maindom\hiropln /p p@ssW23
bootcfg /query /u hiropln /p p@ssW23
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg raw

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds operating system load options specified as a string to an operating system entry in the [operating systems] section of the Boot.ini file. This command overwrites any existing operating system entry options.

Syntax

```
bootcfg /raw [/s <computer> [/u <domain>\<user> /p <password>]]
<osloadoptionsstring> [/id <osentrylinenum>] [/a]
```

Parameters

Parameter	Description
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
`<osloadoptionsstring>`	Specifies the operating system load options to add to the operating system entry. These load options replace any existing load options associated with the operating system entry. There is no validation against the `<osloadoptions>` parameter.
`/id <osentrylinenum>`	Specifies the operating system entry line number in the [operating systems] section of the Boot.ini file to which the operating system load options are added. The first line after the [operating systems] section header is 1.
/a	Specifies which operating system options should be appended to any existing operating system options.

Parameter	Description
/?	Displays help at the command prompt.

Examples

This text should contain valid OS Load Options such as **/debug**, **/fastdetect**, **/nodebug**, **/baudrate**, **/crashdebug**, and **/sos**.

To add **/debug /fastdetect** to the end of the first operating system entry, replacing any previous operating system entry options:

```
bootcfg /raw /debug /fastdetect /id 1
```

To use the **bootcfg /raw** command:

```
bootcfg /raw /debug /sos /id 2
bootcfg /raw /s srvmain /u maindom\hiropln /p p@ssW23 /crashdebug  /id 2
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg rmsw

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes operating system load options for a specified operating system entry.

Syntax

```
bootcfg /rmsw [/s <computer> [/u <domain>\<user> /p <password>]] [/mm] [/bv] [/so] [/ng] /id <osentrylinenum>
```

Parameters

Parameter	Description
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
/mm	Removes the /maxmem option and its associated maximum memory value from the specified `<osentrylinenum>`. The /maxmem option specifies the maximum amount of RAM that the operating system can use.
/bv	Removes the /basevideo option from the specified `<osentrylinenum>`. The /basevideo option directs the operating system to use standard VGA mode for the installed video driver.
/so	Removes the /sos option from the specified `<osentrylinenum>`. The /sos option directs the operating system to display device driver names while they are being loaded.
/ng	Removes the /noguiboot option from the specified `<osentrylinenum>`. The /noguiboot option disables the progress bar that appears before the CTRL+ALT+DEL logon prompt.

Parameter	Description
`/id <osentrylinenum>`	Specifies the operating system entry line number in the [operating systems] section of the Boot.ini file to which the operating system load options are added. The first line after the [operating systems] section header is 1.
/?	Displays help at the command prompt.

Examples

To use the **bootcfg /rmsw** command:

```
bootcfg /rmsw /mm 64 /id 2
bootcfg /rmsw /so /id 3
bootcfg /rmsw /so /ng /s srvmain /u hiropln /id 2
bootcfg /rmsw /ng /id 2
bootcfg /rmsw /mm 96 /ng /s srvmain /u maindom\hiropln /p p@ssW23 /id 2
```

Related links

- Command-Line Syntax Key
- bootcfg command

bootcfg timeout

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the operating system time-out value.

Syntax

```
bootcfg /timeout <timeoutvalue> [/s <computer> [/u <domain>\<user> /p
<password>]]
```

Parameters

Parameter	Description
`/timeout <timeoutvalue>`	Specifies the timeout value in the [boot loader] section. The `<timeoutvalue>` is the number of seconds the user has to select an operating system from the boot loader screen before NTLDR loads the default. The valid range for `<timeoutvalue>` is 0-999. If the value is 0, NTLDR immediately starts the default operating system without displaying the boot loader screen.
`/s <computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer.
`/u <domain>\<user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain>\<user>`. The default is the permissions of the current logged on user on the computer issuing the command.
`/p <password>`	Specifies the password of the user account that is specified in the **/u** parameter.
/?	Displays help at the command prompt.

Examples

To use the **bootcfg /timeout** command:

```
bootcfg /timeout 30
bootcfg /s srvmain /u maindom\hiropln /p p@ssW23 /timeout 50
```

Related links

- Command-Line Syntax Key
- bootcfg command

break

Article • 02/03/2023

> **Important**
>
> This command is no longer in use. It is included only to preserve compatibility with existing MS-DOS files, but it has no effect at the command line because the functionality is automatic.

Sets or clears extended CTRL+C checking on MS-DOS systems. If used without parameters, **break** displays the existing setting value.

If command extensions are enabled and running on the Windows platform, inserting the **break** command into a batch file enters a hard-coded breakpoint if being debugged by a debugger.

Syntax

```
break=[on|off]
```

> **Note**
>
> Because the break command has no effect, it is often used to create empty files or delete the content of an existing file. For example:

```
rem -- cleans the content of the file --
break>log
```

Related links

- Command-Line Syntax Key
- break command

cacls

Article • 02/03/2023

> **Important**
>
> This command has been deprecated. Please use **icacls** instead.

Displays or modifies discretionary access control lists (DACL) on specified files.

Syntax

```
cacls <filename> [/t] [/m] [/l] [/s[:sddl]] [/e] [/c] [/g user:<perm>] [/r
user [...]] [/p user:<perm> [...]] [/d user [...]]
```

Parameters

Parameter	Description
`<filename>`	Required. Displays ACLs of specified files.
/t	Changes ACLs of specified files in the current directory and all subdirectories.
/m	Changes ACLs of volumes mounted to a directory.
/l	Works on the Symbolic Link itself instead of the target.
/s:sddl	Replaces the ACLs with those specified in the SDDL string. This parameter is not valid for use with the **/e**, **/g**, **/r**, **/p**, or **/d** parameters.
/e	Edit an ACL instead of replacing it.
/c	Continue after access denied errors.
`/g user:<perm>`	Grants specified user access rights, including these valid values for permission: • **n** - None • **r** - Read • **w** - Write • **c** - Change (write) • **f** - Full control
/r user [...]	Revoke specified user's access rights. Only valid when used with the **/e** parameter.

Parameter	Description
`[/p user:<perm> [...]`	Replace specified user's access rights, including these valid values for permission: • **n** - None • **r** - Read • **w** - Write • **c** - Change (write) • **f** - Full control
[/d user [...]	Deny specified user access.
/?	Displays help at the command prompt.

Sample output

Output	Access control entry (ACE) applies to
OI	Object inherit. This folder and files.
CI	Container inherit. This folder and subfolders.
IO	Inherit only. The ACE does not apply to the current file/directory.
No output message	This folder only.
(OI)(CI)	This folder, subfolders, and files.
(OI)(CI)(IO)	Subfolders and files only.
(CI)(IO)	Subfolders only.
(OI)(IO)	Files only.

Remarks

- You can use wildcards (**?** and *) to specify multiple files.
- You can specify more than one user.

Related links

- Command-Line Syntax Key
- icacls

call

Article • 02/03/2023

Calls one batch program from another without stopping the parent batch program. The **call** command accepts labels as the target of the call.

> **Note**
>
> Call has no effect at the command prompt when it is used outside of a script or batch file.

Syntax

```
call [drive:][path]<filename> [<batchparameters>]]
call [:<label> [<arguments>]]
```

Parameters

Parameter	Description
`[<drive>:][<path>]<filename>`	Specifies the location and name of the batch program that you want to call. The `<filename>` parameter is required, and it must have a .bat or .cmd extension.
`<batchparameters>`	Specifies any command-line information required by the batch program.
`:<label>`	Specifies the label that you want a batch program control to jump to.
`<arguments>`	Specifies the command-line information to be passed to the new instance of the batch program, beginning at `:<label>`.
/?	Displays help at the command prompt.

Batch parameters

The batch script argument references (**%0**, **%1**, ...) are listed in the following tables.

Using the %* value in a batch script refers to all the arguments (for example, **%1**, **%2**, **%3**...).

You can use the following optional syntaxes as substitutions for batch parameters (%**n**):

Batch Parameter	Description
%~1	Expands %**1** and removes surrounding quotation marks.
%~f1	Expands %**1** to a fully qualified path.
%~d1	Expands %**1** to a drive letter only.
%~p1	Expands %**1** to a path only.
%~n1	Expands %**1** to a file name only.
%~x1	Expands %**1** to a file name extension only.
%~s1	Expands %**1** to a fully qualified path that contains short names only.
%~a1	Expands %**1** to the file attributes.
%~t1	Expands %**1** to the date and time of file.
%~z1	Expands %**1** to the size of the file.
%~$PATH:1	Searches the directories listed in the PATH environment variable, and expands %**1** to the fully qualified name of the first directory found. If the environment variable name is not defined or the file is not found by the search, then this modifier expands to the empty string.

The following table shows how you can combine modifiers with the batch parameters for compound results:

Batch Parameter with Modifier	Description
%~dp1	Expands %**1** to a drive letter and path only.
%~nx1	Expands %**1** to a file name and extension only.
%~dp$PATH:1	Searches the directories listed in the PATH environment variable for %**1**, and then expands to the drive letter and path of the first directory found.
%~ftza1	Expands %**1** to display output similar to the **dir** command.

In the above examples, %**1** and PATH can be replaced by other valid values. The %~ syntax is terminated by a valid argument number. The %~ modifiers cannot be used with %*.

Remarks

- Using batch parameters:

  Batch parameters can contain any information that you can pass to a batch program, including command-line options, file names, the batch parameters **%0** through **%9**, and variables (for example, **%baud%**).

- Using the `<label>` parameter:

  By using **call** with the `<label>` parameter, you create a new batch file context and pass control to the statement after the specified label. The first time the end of the batch file is encountered (that is, after jumping to the label), control returns to the statement after the **call** statement. The second time the end of the batch file is encountered, the batch script is exited.

- Using pipes and redirection symbols:

  Do not use pipes `(|)` or redirection symbols (`<` or `>`) with **call**.

- Making a recursive call

  You can create a batch program that calls itself. However, you must provide an exit condition. Otherwise, the parent and child batch programs can loop endlessly.

- Working with command extensions

  If command extensions are enabled, **call** accepts `<label>` as the target of the call. The correct syntax is `call :<label> <arguments>`.

Examples

To run the checknew.bat program from another batch program, type the following command in the parent batch program:

```
call checknew
```

If the parent batch program accepts two batch parameters and you want it to pass those parameters to checknew.bat, type the following command in the parent batch program:

```
```

```
call checknew %1 %2
```

Related links

- Command-Line Syntax Key

cd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the name of the current directory or changes the current directory. If used with only a drive letter (for example, `cd C:`), **cd** displays the names of the current directory in the specified drive. If used without parameters, **cd** displays the current drive and directory.

> **Note**
>
> This command is the same as the **chdir command**.

Syntax

```
cd [/d] [<drive>:][<path>]
cd [..]
chdir [/d] [<drive>:][<path>]
chdir [..]
```

Parameters

Parameter	Description
/d	Changes the current drive as well as the current directory for a drive.
`<drive>:`	Specifies the drive to display or change (if different from the current drive).
`<path>`	Specifies the path to the directory that you want to display or change.
[..]	Specifies that you want to change to the parent folder.
/?	Displays help at the command prompt.

Remarks

If command extensions are enabled, the following conditions apply to the **cd** command:

- The current directory string is converted to use the same case as the names on the disk. For example, `cd c:\temp` would set the current directory to C:\Temp if that is the case on the disk.
- Spaces aren't treated as delimiters, so `<path>` can contain spaces without enclosing quotation marks. For example:

  ```
  cd username\programs\start menu
  ```

  is the same as:

  ```
  cd "username\programs\start menu"
  ```

  If extensions are disabled, the quotation marks are required.
- To disable command extensions, type:

  ```
  cmd /e:off
  ```

Examples

To return to the root directory, the top of the directory hierarchy for a drive:

```
cd\
```

To change the default directory on a drive that is different from the one you are on:

```
cd [<drive>:[<directory>]]
```

To verify the change to the directory, type:

```
cd [<drive>:]
```

Related links

- Command-Line Syntax Key
- chdir command

certreq

Article • 09/21/2023

The certreq command can be used to request certificates from a certification authority (CA), to retrieve a response to a previous request from a CA, to create a new request from an .inf file, to accept and install a response to a request, to construct a cross-certification or qualified subordination request from an existing CA certificate or request, and to sign a cross-certification or qualified subordination request.

> **ⓘ Important**
>
> Earlier versions of the certreq command might not provide all of the options described here. To see the options supported based on specific versions of certreq, run the command-line help option, `certreq -v -?`.
>
> The certreq command doesn't support creating a new certificate request based on a Key Attestation template when in a CEP/CES environment.

> **⚠ Warning**
>
> The content for this topic is based on the default settings for Windows Server; for example, setting the key length to 2048, selecting Microsoft Software Key Storage Provider as the CSP, and using Secure Hash Algorithm 1 (SHA1). Evaluate these selections against the requirements of your company's security policy.

Syntax

```
certreq [-submit] [options] [requestfilein [certfileout [certchainfileout [fullresponsefileOut]]]]
certreq -retrieve [options] requestid [certfileout [certchainfileout [fullresponsefileOut]]]
certreq -new [options] [policyfilein [requestfileout]]
certreq -accept [options] [certchainfilein | fullresponsefilein | certfilein]
certreq -sign [options] [requestfilein [requestfileout]]
certreq –enroll [options] templatename
certreq –enroll –cert certId [options] renew [reusekeys]
```

Parameters

Parameter	Description
-submit	Submits a request to a certificate authority.
-retrieve `<requestid>`	Retrieves a response to a previous request from a certificate authority.
-new	Creates a new request from an .inf file.
-accept	Accepts and installs a response to a certificate request.
-policy	Sets the policy for a request.
-sign	Signs a cross-certification or qualified subordination request.
-enroll	Enrolls for or renews a certificate.
-?	Displays a list of certreq syntax, options, and descriptions.
`<parameter>` -?	Displays help for the parameter specified.
-v -?	Displays a verbose list of the certreq syntax, options, and descriptions.

Examples

certreq -submit

To submit a basic certificate request:

```
certreq –submit certrequest.req certnew.cer certnew.pfx
```

Remarks

- This is the default certreq.exe parameter. If no option is specified at the command-line prompt, certreq.exe attempts to submit a certificate request to a certificate authority. You must specify a certificate request file when using the **–submit** option. If this parameter is omitted, a common **File Open** window appears, letting you select the appropriate certificate request file.
- To request a certificate by specifying the SAN attribute, see the *How to use the certreq.exe utility to create and submit a certificate request* section of Microsoft Knowledge Base article 931351 How to add a Subject Alternative Name to a secure LDAP certificate.

certreq -retrieve

To retrieve certificate ID 20 and to create a certificate file (.cer), named *MyCertificate*:

```
certreq -retrieve 20 MyCertificate.cer
```

Remarks

- Use certreq -retrieve *requestid* to retrieve the certificate after the certificate authority has issued it. The *requestid* PKC can be a decimal or hex with 0x prefix and it can be a certificate serial number with no 0x prefix. You can also use it to retrieve any certificate that has ever been issued by the certificate authority, including revoked or expired certificates, without considering if the certificate's request was ever in the pending state.
- If you submit a request to the certificate authority, the policy module of the certificate authority might leave the request in a pending state and return the *requestid* to the certreq caller for display. Eventually, the certificate authority's administrator issues the certificate or deny the request.

certreq -new

To create a new request:

```
[newrequest]
; At least one value must be set in this section
subject = CN=W2K8-BO-DC.contoso2.com
```

The following are some of the possible sections that may be added to the INF file:

[newrequest]

This area of the INF file is mandatory for any new certificate request templates, and must include at least one parameter with a value.

Key[1]	Description	Value[2]	Example
Subject	Several apps rely on the subject information in a certificate. We recommend specifying a value for this key. If the subject isn't set here, we recommend you include a subject name as part of the subject alternative name certificate extension.	Relative Distinguished Name string values	Subject = CN=computer1.contoso.com Subject=CN=John Smith,CN=Users,DC=Contoso,DC=com
Exportable	If set to TRUE, the private key can be exported with the certificate. To ensure a high level of security, private keys shouldn't be exportable; however, in some cases, it might be required if several computers or users must share the same private key.	`true | false`	`Exportable = TRUE`. CNG keys can distinguish between this and plaintext exportable. CAPI1 keys can't.
ExportableEncrypted	Specifies whether the private key should be set to be exportable.	`true | false`	`ExportableEncrypted = true` **Tip:** Not all public key sizes and algorithms work with all hash algorithms. The specified CSP must also support the specified hash algorithm. To see the list of supported hash algorithms, you can run the command: `certutil -oid 1 | findstr pwszCNGAlgid | findstr /v CryptOIDInfo`
HashAlgorithm	Hash Algorithm to be used for this request.	`Sha256, sha384, sha512, sha1, md5, md4, md2`	`HashAlgorithm = sha1`. To see the list of supported hash algorithms use: certutil -oid 1 | findstr pwszCNGAlgid | findstr /v CryptOIDInfo
KeyAlgorithm	The algorithm that's used by the service provider to generate a public and private key pair.	`RSA, DH, DSA, ECDH_P256, ECDH_P521, ECDSA_P256, ECDSA_P384, ECDSA_P521`	`KeyAlgorithm = RSA`
KeyContainer	We don't recommend setting this parameter for new requests where new key material is generated. The key container is automatically generated and maintained by the system. For requests where the existing key material should be used, this value can be set to the key-container name of	Random string value **Tip:** Use double quotes around any INF key value that has blanks or special characters to avoid potential INF parsing issues.	`KeyContainer = {C347BD28-7F69-4090-AA16-BC58CF4D749C}`

Key[1]	Description	Value[2]	Example
	the existing key. Use the `certutil -key` command to display the list of available key containers for the machine context. Use the `certutil -key -user` command for the current user's context.		
KeyLength	Defines the length of the public and private key. The key length has an impact on the security level of the certificate. Greater key length usually provides a higher security level; however, some applications may have limitations regarding the key length.	Any valid key length that is supported by the cryptographic service provider.	`KeyLength = 2048`
KeySpec	Determines if the key can be used for signatures, for Exchange (encryption), or for both.	`AT_NONE, AT_SIGNATURE, AT_KEYEXCHANGE`	`KeySpec = AT_KEYEXCHANGE`
KeyUsage	Defines what the certificate key should be used for.	• `CERT_DIGITAL_SIGNATURE_KEY_USAGE -- 80 (128)` • `CERT_NON_REPUDIATION_KEY_USAGE -- 40 (64)` • `CERT_KEY_ENCIPHERMENT_KEY_USAGE -- 20 (32)` • `CERT_DATA_ENCIPHERMENT_KEY_USAGE -- 10 (16)` • `CERT_KEY_AGREEMENT_KEY_USAGE -- 8` • `CERT_KEY_CERT_SIGN_KEY_USAGE -- 4` • `CERT_OFFLINE_CRL_SIGN_KEY_USAGE -- 2` • `CERT_CRL_SIGN_KEY_USAGE -- 2` • `CERT_ENCIPHER_ONLY_KEY_USAGE -- 1` • `CERT_DECIPHER_ONLY_KEY_USAGE -- 8000 (32768)`	`KeyUsage = CERT_DIGITAL_SIGNATURE_KEY_USAGE | CERT_KEY_ENCIPHERMENT_KEY_USAGE` **Tip:** Multiple values use a pipe (|) symbol separator. Ensure that you use double-quotes when using multiple values to avoid INF parsing issues. The values shown are hexadecimal (decimal) values for each bit definition. Older syntax can also be used: a single hexadecimal value with multiple bits set, instead of the symbolic representation. For example, `KeyUsage = 0xa0`.
KeyUsageProperty	Retrieves a value that identifies the specific purpose for which a private key can be used.	• `NCRYPT_ALLOW_DECRYPT_FLAG -- 1` • `NCRYPT_ALLOW_SIGNING_FLAG -- 2` • `NCRYPT_ALLOW_KEY_AGREEMENT_FLAG -- 4` • `NCRYPT_ALLOW_ALL_USAGES -- ffffff (16777215)`	`KeyUsageProperty = NCRYPT_ALLOW_DECRYPT_FLAG | NCRYPT_ALLOW_SIGNING_FLAG`
MachineKeySet	This key is important when you need to create certificates that are owned by the machine and not a user. The key material that is generated is maintained in the security context of	`true | false`. The default is false.	`MachineKeySet = true`

Key[1]	Description	Value[2]	Example
	the security principal (user or computer account) that has created the request. When an administrator creates a certificate request on behalf of a computer, the key material must be created in the machine's security context and not the administrator's security context. Otherwise, the machine couldn't access its private key since it would be in the administrator's security context.		
NotBefore	Specifies a date or date and time before which the request can't be issued. `NotBefore` can be used with `ValidityPeriod` and `ValidityPeriodUnits`.	Date or date and time	`NotBefore = 7/24/2012 10:31 AM` **Tip:** `NotBefore` and `NotAfter` are for R`equestType=cert` only. Date parsing attempts to be locale-sensitive. Using month names will disambiguate and should work in every locale.
NotAfter	Specifies a date or date and time after which the request can't be issued. `NotAfter` can't be used with `ValidityPeriod` or `ValidityPeriodUnits`.	Date or date and time	`NotAfter = 9/23/2014 10:31 AM` **Tip:** `NotBefore` and `NotAfter` are for `RequestType=cert` only. Date parsing attempts to be locale-sensitive. Using month names will disambiguate and should work in every locale.
PrivateKeyArchive	The PrivateKeyArchive setting works only if the corresponding RequestType is set to CMC because only the Certificate Management Messages over CMS (CMC) request format allows for securely transferring the requester's private key to the CA for key archival.	`true | false`	`PrivateKeyArchive = true`
EncryptionAlgorithm	The encryption algorithm to use.	Possible options vary, depending on the operating system version and the set of installed cryptographic providers. To see the list of available algorithms, run the command: `certutil -oid 2 | findstr pwszCNGAlgid`. The specified CSP used must also support the specified symmetric encryption algorithm and length.	`EncryptionAlgorithm = 3des`
EncryptionLength	Length of encryption algorithm to use.	Any length allowed by the specified EncryptionAlgorithm.	`EncryptionLength = 128`

Key[1]	Description	Value[2]	Example
ProviderName	The provider name is the display name of the CSP.	If you don't know the provider name of the CSP you're using, run `certutil –csplist` from a command line. The command displays the names of all CSPs that are available on the local system	`ProviderName = Microsoft RSA SChannel Cryptographic Provider`
ProviderType	The provider type is used to select specific providers based on specific algorithm capability such as RSA Full.	If you don't know the provider type of the CSP you're using, run `certutil –csplist` from a command-line prompt. The command displays the provider type of all CSPs that are available on the local system.	`ProviderType = 1`
RenewalCert	If you need to renew a certificate that exists on the system where the certificate request is generated, you must specify its certificate hash as the value for this key.	The certificate hash of any certificate that is available at the computer where the certificate request is created. If you don't know the certificate hash, use the Certificates MMC Snap-In and look at the certificate that should be renewed. Open the certificate properties and see the `Thumbprint` attribute of the certificate. Certificate renewal requires either a `PKCS#7` or a `CMC` request format.	`RenewalCert = 4EDF274BD2919C6E9EC6A522F0F3B153E9B1582D`
RequesterName	Makes the request to enroll on behalf of another user request. The request must also be signed with an Enrollment Agent certificate, or the CA rejects the request. Use the `-cert` option to specify the enrollment agent certificate. The requester name can be specified for certificate requests if the `RequestType` is set to `PKCS#7` or `CMC`. If the `RequestType` is set to `PKCS#10`, this key is ignored. The `Requestername` can only be set as part of the request. You can't manipulate the `Requestername` in a pending request.	`Domain\User`	`Requestername = Contoso\BSmith`
RequestType	Determines the standard that is used to generate and send the certificate request.	• `PKCS10 -- 1` • `PKCS7 -- 2` • `CMC -- 3` • `Cert -- 4` • `SCEP -- fd00 (64768)` **Tip:** This option indicates a self-signed or self-issued certificate. It doesn't generate a request, but rather a new certificate and then installs the certificate. Self-signed is the default. Specify a signing cert by using the –cert option to create a self-issued certificate that isn't self-signed.	`RequestType = CMC`
SecurityDescriptor	Contains the security information associated with	`SecurityDescriptor = D:P(A;;GA;;;SY)(A;;GA;;;BA)`	

Key[1]	Description	Value[2]	Example
	securable objects. For most securable objects, you can specify an object's security descriptor in the function call that creates the object.Strings based on security descriptor definition language. **Tip:** This is relevant only for machine context non-smart card keys.		
AlternateSignatureAlgorithm	Specifies and retrieves a Boolean value that indicates whether the signature algorithm object identifier (OID) for a PKCS#10 request or certificate signature is discrete or combined.	`true | false`	`AlternateSignatureAlgorithm = false` For an RSA signature, `false` indicates a `Pkcs1 v1.5`, while `true` indicates a `v2.1` signature.
Silent	By default, this option allows the CSP access to the interactive user desktop and request information such as a smart card PIN from the user. If this key is set to TRUE, the CSP must not interact with the desktop and will be blocked from displaying any user interface to the user.	`true | false`	`Silent = true`
SMIME	If this parameter is set to TRUE, an extension with the object identifier value 1.2.840.113549.1.9.15 is added to the request. The number of object identifiers depends on the operating system version installed and CSP capability, which refers to symmetric encryption algorithms that may be used by Secure Multipurpose Internet Mail Extensions (S/MIME) applications such as Outlook.	`true | false`	`SMIME = true`

Key[1]	Description	Value[2]	Example
UseExistingKeySet	This parameter is used to specify that an existing key pair should be used in building a certificate request. If this key is set to TRUE, you must also specify a value for the RenewalCert key or the KeyContainer name. You must not set the Exportable key because you can't change the properties of an existing key. In this case, no key material is generated when the certificate request is built.	`true | false`	`UseExistingKeySet = true`
KeyProtection	Specifies a value that indicates how a private key is protected before use.	• `XCN_NCRYPT_UI_NO_PROTCTION_FLAG -- 0` • `XCN_NCRYPT_UI_PROTECT_KEY_FLAG -- 1` • `XCN_NCRYPT_UI_FORCE_HIGH_PROTECTION_FLAG -- 2`	`KeyProtection = NCRYPT_UI_FORCE_HIGH_PROTECTION_FLAG`
SuppressDefaults	Specifies a Boolean value that indicates whether the default extensions and attributes are included in the request. The defaults are represented by their object identifiers (OIDs).	`true | false`	`SuppressDefaults = true`
FriendlyName	A friendly name for the new certificate.	Text	`FriendlyName = Server1`
ValidityPeriodUnits	Specifies many units that are to be used with ValidityPeriod. Note: This is used only when the `request type=cert`.	Numeric	`ValidityPeriodUnits = 3`
ValidityPeriod	ValidityPeriod must be a US English plural time period. Note: This is used only when the request type=cert.	`Years | Months | Weeks | Days | Hours | Minutes | Seconds`	`ValidityPeriod = Years`

[1]Parameter to the left of the equal sign (=)

[2]Parameter to the right of the equal sign (=)

[Extensions]

This section is optional.

Extension OID	Definition	Example
2.5.29.17		2.5.29.17 = {text}
continue		`continue = UPN=User@Domain.com&`
continue		`continue = EMail=User@Domain.com&`
continue		`continue = DNS=host.domain.com&`
continue		`continue = DirectoryName=CN=Name,DC=Domain,DC=com&`
continue		`continue = URL=<http://host.domain.com/default.html&>`
continue		`continue = IPAddress=10.0.0.1&`
continue		`continue = RegisteredId=1.2.3.4.5&`
continue		`continue = 1.2.3.4.6.1={utf8}String&`
continue		`continue = 1.2.3.4.6.2={octet}AAECAwQFBgc=&`
continue		`continue = 1.2.3.4.6.2={octet}{hex}00 01 02 03 04 05 06 07&`
continue		`continue = 1.2.3.4.6.3={asn}BAgAAQIDBAUGBw==&`
continue		`continue = 1.2.3.4.6.3={hex}04 08 00 01 02 03 04 05 06 07`
2.5.29.37		`2.5.29.37={text}`
continue		`continue = 1.3.6.1.5.5.7`
continue		`continue = 1.3.6.1.5.5.7.3.1`
2.5.29.19		`{text}ca=0pathlength=3`
Critical		`Critical=2.5.29.19`
KeySpec		• `AT_NONE -- 0` • `AT_SIGNATURE -- 2` • `AT_KEYEXCHANGE -- 1`
RequestType		• `PKCS10 -- 1` • `PKCS7 -- 2` • `CMC -- 3` • `Cert -- 4` • `SCEP -- fd00 (64768)`
KeyUsage		• `CERT_DIGITAL_SIGNATURE_KEY_USAGE -- 80 (128)` • `CERT_NON_REPUDIATION_KEY_USAGE -- 40 (64)` • `CERT_KEY_ENCIPHERMENT_KEY_USAGE -- 20 (32)` • `CERT_DATA_ENCIPHERMENT_KEY_USAGE -- 10 (16)` • `CERT_KEY_AGREEMENT_KEY_USAGE -- 8` • `CERT_KEY_CERT_SIGN_KEY_USAGE -- 4` • `CERT_OFFLINE_CRL_SIGN_KEY_USAGE -- 2` • `CERT_CRL_SIGN_KEY_USAGE -- 2` • `CERT_ENCIPHER_ONLY_KEY_USAGE -- 1` • `CERT_DECIPHER_ONLY_KEY_USAGE -- 8000 (32768)`
KeyUsageProperty		• `NCRYPT_ALLOW_DECRYPT_FLAG -- 1` • `NCRYPT_ALLOW_SIGNING_FLAG -- 2` • `NCRYPT_ALLOW_KEY_AGREEMENT_FLAG -- 4` • `NCRYPT_ALLOW_ALL_USAGES -- ffffff (16777215)`
KeyProtection		• `NCRYPT_UI_NO_PROTECTION_FLAG -- 0` • `NCRYPT_UI_PROTECT_KEY_FLAG -- 1`

Extension OID	Definition	Example
		• `NCRYPT_UI_FORCE_HIGH_PROTECTION_FLAG -- 2`
SubjectNameFlags	template	• `CT_FLAG_SUBJECT_REQUIRE_COMMON_NAME -- 40000000 (1073741824)` • `CT_FLAG_SUBJECT_REQUIRE_DIRECTORY_PATH -- 80000000 (2147483648)` • `CT_FLAG_SUBJECT_REQUIRE_DNS_AS_CN -- 10000000 (268435456)` • `CT_FLAG_SUBJECT_REQUIRE_EMAIL -- 20000000 (536870912)` • `CT_FLAG_OLD_CERT_SUPPLIES_SUBJECT_AND_ALT_NAME -- 8` • `CT_FLAG_SUBJECT_ALT_REQUIRE_DIRECTORY_GUID -- 1000000 (16777216)` • `CT_FLAG_SUBJECT_ALT_REQUIRE_DNS -- 8000000 (134217728)` • `CT_FLAG_SUBJECT_ALT_REQUIRE_DOMAIN_DNS -- 400000 (4194304)` • `CT_FLAG_SUBJECT_ALT_REQUIRE_EMAIL -- 4000000 (67108864)` • `CT_FLAG_SUBJECT_ALT_REQUIRE_SPN -- 800000 (8388608)` • `CT_FLAG_SUBJECT_ALT_REQUIRE_UPN -- 2000000 (33554432)`
X500NameFlags		• `CERT_NAME_STR_NONE -- 0` • `CERT_OID_NAME_STR -- 2` • `CERT_X500_NAME_STR -- 3` • `CERT_NAME_STR_SEMICOLON_FLAG -- 40000000 (1073741824)` • `CERT_NAME_STR_NO_PLUS_FLAG -- 20000000 (536870912)` • `CERT_NAME_STR_NO_QUOTING_FLAG -- 10000000 (268435456)` • `CERT_NAME_STR_CRLF_FLAG -- 8000000 (134217728)` • `CERT_NAME_STR_COMMA_FLAG -- 4000000 (67108864)` • `CERT_NAME_STR_REVERSE_FLAG -- 2000000 (33554432)` • `CERT_NAME_STR_FORWARD_FLAG -- 1000000 (16777216)` • `CERT_NAME_STR_DISABLE_IE4_UTF8_FLAG -- 10000 (65536)` • `CERT_NAME_STR_ENABLE_T61_UNICODE_FLAG -- 20000 (131072)` • `CERT_NAME_STR_ENABLE_UTF8_UNICODE_FLAG -- 40000 (262144)` • `CERT_NAME_STR_FORCE_UTF8_DIR_STR_FLAG -- 80000 (524288)` • `CERT_NAME_STR_DISABLE_UTF8_DIR_STR_FLAG -- 100000 (1048576)` • `CERT_NAME_STR_ENABLE_PUNYCODE_FLAG -- 200000 (2097152)`

> **Note**
>
> `SubjectNameFlags` allows the INF file to specify which **Subject** and **SubjectAltName** extension fields should be auto-populated by certreq based on the current user or current machine properties: DNS name, UPN, and so on. Using the literal template means the template name flags are used instead. This allows a single INF file to be used in multiple contexts to generate requests with context-specific subject information.
>
> `X500NameFlags` specifies the flags to be passed directly to `CertStrToName` API when the `Subject INF keys` value is converted to an ASN.1 encoded Distinguished **Name**.

Example

To create a policy file (.inf) in Notepad and save it as *requestconfig.inf*:

```
[NewRequest]
Subject = CN=<FQDN of computer you are creating the certificate>
Exportable = TRUE
KeyLength = 2048
KeySpec = 1
KeyUsage = 0xf0
MachineKeySet = TRUE
[RequestAttributes]
CertificateTemplate=WebServer
[Extensions]
OID = 1.3.6.1.5.5.7.3.1
OID = 1.3.6.1.5.5.7.3.2
```

On the computer for which you're requesting a certificate:

```
certreq –new requestconfig.inf certrequest.req
```

To use the [Strings] section syntax for OIDs and other difficult to interpret data. The new {text} syntax example for EKU extension, which uses a comma separated list of OIDs:

```
[Version]
Signature=$Windows NT$

[Strings]
szOID_ENHANCED_KEY_USAGE = 2.5.29.37
szOID_PKIX_KP_SERVER_AUTH = 1.3.6.1.5.5.7.3.1
szOID_PKIX_KP_CLIENT_AUTH = 1.3.6.1.5.5.7.3.2

[NewRequest]
Subject = CN=TestSelfSignedCert
Requesttype = Cert

[Extensions]
%szOID_ENHANCED_KEY_USAGE%={text}%szOID_PKIX_KP_SERVER_AUTH%,
_continue_ = %szOID_PKIX_KP_CLIENT_AUTH%
```

To specify a Subject Alternate Name (SAN), add it in the [Extensions] section of your INF. For example:

```
[Version]
Signature=$Windows NT$

[Strings]
szOID_ENHANCED_KEY_USAGE = 2.5.29.37
szOID_PKIX_KP_SERVER_AUTH = 1.3.6.1.5.5.7.3.1
szOID_PKIX_KP_CLIENT_AUTH = 1.3.6.1.5.5.7.3.2

[NewRequest]
Subject = CN=TestSelfSignedCert
Requesttype = Cert

[Extensions]
2.5.29.17 = "{text}"
_continue_ = "DNS=example.com"
_continue_ = "DNS=www.example.com"
_continue_ = "IP Address=192.168.1.1"
```

In this example, `2.5.29.17` is the OID defining the SAN. To specify multiple SANs, the `_continue_` extension OID is used, which lets you separate and specify each SAN extension.

certreq -accept

The `-accept` parameter links the previously generated private key with the issued certificate and removes the pending certificate request from the system where the certificate is requested (if there's a matching request).

To manually accept a certificate:

```
certreq -accept certnew.cer
```

> ⚠ **Warning**

Using the `-accept` parameter with the `-user` and `-machine` options indicates whether the installing certificate should be installed in **user** or **machine** context. If there's an outstanding request in either context that matches the public key being installed, then these options aren't needed. If there is no outstanding request, then one of these must be specified.

certreq -policy

The policy.inf file is a configuration file that defines the constraints applied to a CA certification, when a qualified subordination is defined.

To build a cross certificate request:

```
certreq -policy certsrv.req policy.inf newcertsrv.req
```

Using `certreq -policy` without any other parameter opens a dialog window, allowing you to select the requested file (.req, .cmc, .txt, .der, .cer or .crt). After you select the requested file and click **Open**, another dialog window opens, allowing you to select the policy.inf file.

Examples

Find an example of the policy.inf file in the CAPolicy.inf Syntax.

certreq -sign

To create a new certificate request, sign it, and to submit it:

```
certreq -new policyfile.inf myrequest.req
certreq -sign myrequest.req myrequest.req
certreq -submit myrequest_sign.req myrequest_cert.cer
```

Remarks

- Using `certreq -sign` without any other parameter it opens a dialog window so you can select the requested file (req, cmc, txt, der, cer or crt).
- Signing the qualified subordination request may require **Enterprise Administrator** credentials. This is a best practice for issuing signing certificates for qualified subordination.
- The certificate used to sign the qualified subordination request uses the qualified subordination template. Enterprise Administrators have to sign the request or grant user permissions to the individuals signing the certificate.
- You might be required to have additional personnel sign the CMC request after you. This depends on the assurance level associated with the qualified subordination.
- If the parent CA of the qualified subordinate CA you're installing is offline, you must obtain the CA certificate for the qualified subordinate CA from the offline parent. If the parent CA is online, specify the CA certificate for the qualified subordinate CA during the **Certificate Services Installation** wizard.

certreq -enroll

You can use this comment to enroll or renew your certificates.

Examples

To enroll a certificate, using the *WebServer* template, and by selecting the policy server using U/I:

```
certreq -enroll –machine –policyserver * WebServer
```

To renew a certificate using a serial number:

```
certreq –enroll -machine –cert 61 2d 3c fe 00 00 00 00 00 05 renew
```

You can only renew valid certificates. Expired certificates can't be renewed and must be replaced with a new certificate.

Options

Options	Description
-any	`Force ICertRequest::Submit` to determine encoding type.
-attrib `<attributestring>`	Specifies the **Name** and **Value** string pairs, separated by a colon. Separate **Name** and **Value** string pairs using `\n` (for example, Name1:value1\nName2:value2).
-binary	Formats output files as binary instead of base64-encoded.
-policyserver `<policyserver>`	ldap: `<path>` Insert the URI or unique ID for a computer running the Certificate Enrollment Policy web service. To specify that you would like to use a request file by browsing, just use a minus (-) sign for `<policyserver>`.
-config `<ConfigString>`	Processes the operation by using the CA specified in the configuration string, which is **CAHostName\CAName**. For an https:\\ connection, specify the enrollment server URI. For the local machine store CA, use a minus (-) sign.
-anonymous	Use anonymous credentials for Certificate Enrollment web services.
-kerberos	Use Kerberos (domain) credentials for Certificate Enrollment web services.
-clientcertificate `<ClientCertId>`	You can replace the `<ClientCertId>` with a certificate thumbprint, CN, EKU, template, email, UPN, or the new `name=value` syntax.
-username `<username>`	Used with Certificate Enrollment web services. You can substitute `<username>` with the SAM name or **domain\user** value. This option is for use with the `-p` option.
-p `<password>`	Used with Certificate Enrollment web services. Substitute `<password>` with the actual user's password. This option is for use with the `-username` option.
-user	Configures the `-user` context for a new certificate request or specifies the context for a certificate acceptance. This is the default context, if none is specified in the INF or template.
-machine	Configures a new certificate request or specifies the context for an a certificate acceptance for the machine context. For new requests it must be consistent with the MachineKeyset INF key and the template context. If this option isn't specified and the template doesn't set a context, then the default is the user context.
-crl	Includes certificate revocation lists (CRLs) in the output to the base64-encoded PKCS #7 file specified by `certchainfileout` or to the base64-encoded file specified by `requestfileout`.
-rpc	Instructs Active Directory Certificate Services (AD CS) to use a remote procedure call (RPC) server connection instead of Distributed COM.
-adminforcemachine	Use the Key Service or impersonation to submit the request from Local System context. Requires that the user invoking this option be a member of Local Administrators.
-renewonbehalfof	Submit a renewal on behalf of the subject identified in the signing certificate. This sets CR_IN_ROBO when calling ICertRequest::Submit method
-f	Force existing files to be overwritten. This also bypasses caching templates and policy.

Options	Description
-q	Use silent mode; suppress all interactive prompts.
-unicode	Writes Unicode output when standard output is redirected or piped to another command, which helps when invoked from Windows PowerShell scripts.
-unicodetext	Sends Unicode output when writing base64 text encoded data blobs to files.

Formats

Formats	Description
requestfilein	Base64-encoded or binary input file name: PKCS #10 certificate request, CMS certificate request, PKCS #7 certificate renewal request, X.509 certificate to be cross-certified, or KeyGen tag format certificate request.
requestfileout	Base64-encoded output file name.
certfileout	Base64-encoded X-509 file name.
PKCS10fileout	For use with the `certreq -policy` parameter only. Base64-encoded PKCS10 output file name.
certchainfileout	Base64-encoded PKCS #7 file name.
fullresponsefileout	Base64-encoded full response file name.
policyfilein	For use with the `certreq -policy` parameter only. INF file containing a textual representation of extensions used to qualify a request.

Additional Resources

The following articles contain examples of certreq usage:

- How to add a subject alternative name to a secure LDAP certificate
- Test Lab Guide: Deploying an AD CS Two-Tier PKI Hierarchy
- Appendix 3: Certreq.exe Syntax
- How to create a web server SSL certificate manually
- Certificate Enrollment for System Center Operations Manager Agent
- Active Directory Certificate Services Overview
- How to enable LDAP over SSL with a third-party certification authority

certutil

Article • 10/19/2023

> **⊗ Caution**
>
> `Certutil` isn't recommended to be used in any production code and doesn't provide any guarantees of live site support or application compatibilities. It's a tool utilized by developers and IT administrators to view certificate content information on devices.

Certutil.exe is a command-line program installed as part of Certificate Services. You can use certutil.exe to display certification authority (CA) configuration information, configure Certificate Services, and back up and restore CA components. The program also verifies certificates, key pairs, and certificate chains.

If `certutil` is run on a certification authority without other parameters, it displays the current certification authority configuration. If `certutil` is run on a non-certification authority without other parameters, the command defaults to running the `certutil -dump` command. Not all versions of certutil provide all of the parameters and options that this document describes. You can see the choices that your version of certutil provides by running `certutil -?` or `certutil <parameter> -?`.

> **Tip**
>
> To see complete help for all certutil verbs and options, including ones that are hidden from the `-?` argument, run `certutil -v -uSAGE`. The `uSAGE` switch is case-sensitive.

Parameters

-dump

Dumps the configuration information or files.

Windows Command Prompt

```
certutil [options] [-dump]
certutil [options] [-dump] File
```

Options:

```
Windows Command Prompt

[-f] [-user] [-Silent] [-split] [-p Password] [-t Timeout]
```

-dumpPFX

Dumps the PFX structure.

```
Windows Command Prompt

certutil [options] [-dumpPFX] File
```

Options:

```
Windows Command Prompt

[-f] [-Silent] [-split] [-p Password] [-csp Provider]
```

-asn

Parses and displays the contents of a file using Abstract Syntax Notation (ASN.1) syntax. File types include .CER, .DER and PKCS #7 formatted files.

```
Windows Command Prompt

certutil [options] -asn File [type]
```

- `[type]`: numeric CRYPT_STRING_* decoding type

-decodehex

Decodes a hexadecimal-encoded file.

```
Windows Command Prompt

certutil [options] -decodehex InFile OutFile [type]
```

- `[type]`: numeric CRYPT_STRING_* decoding type

Options:

Windows Command Prompt

```
[-f]
```

-encodehex

Encodes a file in hexadecimal.

Windows Command Prompt

```
certutil [options] -encodehex InFile OutFile [type]
```

- `[type]`: numeric CRYPT_STRING_* encoding type

Options:

Windows Command Prompt

```
[-f] [-nocr] [-nocrlf] [-UnicodeText]
```

-decode

Decodes a Base64-encoded file.

Windows Command Prompt

```
certutil [options] -decode InFile OutFile
```

Options:

Windows Command Prompt

```
[-f]
```

-encode

Encodes a file to Base64.

Windows Command Prompt

```
certutil [options] -encode InFile OutFile
```

Options:

```
Windows Command Prompt

[-f] [-unicodetext]
```

-deny

Denies a pending request.

```
Windows Command Prompt

certutil [options] -deny RequestId
```

Options:

```
Windows Command Prompt

[-config Machine\CAName]
```

-resubmit

Resubmits a pending request.

```
Windows Command Prompt

certutil [options] -resubmit RequestId
```

Options:

```
Windows Command Prompt

[-config Machine\CAName]
```

-setattributes

Sets attributes for a pending certificate request.

```
Windows Command Prompt

certutil [options] -setattributes RequestId AttributeString
```

Where:

- **RequestId** is the numeric Request ID for the pending request.
- **AttributeString** is the request attribute name and value pairs.

Options:

```
Windows Command Prompt

[-config Machine\CAName]
```

Remarks

- Names and values must be colon separated, while multiple names and value pairs must be newline separated. For example: `CertificateTemplate:User\nEMail:User@Domain.com` where the `\n` sequence is converted to a newline separator.

-setextension

Set an extension for a pending certificate request.

```
Windows Command Prompt

certutil [options] -setextension RequestId ExtensionName Flags {Long | Date
| String | @InFile}
```

Where:

- **requestID** is the numeric Request ID for the pending request.
- **ExtensionName** is the ObjectId string for the extension.
- **Flags** sets the priority of the extension. `0` is recommended, while `1` sets the extension to critical, `2` disables the extension, and `3` does both.

Options:

```
Windows Command Prompt

[-config Machine\CAName]
```

Remarks

- If the last parameter is numeric, it's taken as a **Long**.
- If the last parameter can be parsed as a date, it's taken as a **Date**.
- If the last parameter starts with `\@`, the rest of the token is taken as the filename with binary data or an ascii-text hex dump.
- If the last parameter is anything else, it's taken as a String.

-revoke

Revokes a certificate.

Windows Command Prompt

```
certutil [options] -revoke SerialNumber [Reason]
```

Where:

- **SerialNumber** is a comma-separated list of certificate serial numbers to revoke.
- **Reason** is the numeric or symbolic representation of the revocation reason, including:
  - **0. CRL_REASON_UNSPECIFIED** - Unspecified (default)
  - **1. CRL_REASON_KEY_COMPROMISE** - Key compromise
  - **2. CRL_REASON_CA_COMPROMISE** - Certificate Authority compromise
  - **3. CRL_REASON_AFFILIATION_CHANGED** - Affiliation changed
  - **4. CRL_REASON_SUPERSEDED** - Superseded
  - **5. CRL_REASON_CESSATION_OF_OPERATION** - Cessation of operation
  - **6. CRL_REASON_CERTIFICATE_HOLD** - Certificate hold
  - **8. CRL_REASON_REMOVE_FROM_CRL** - Remove from CRL
  - **9: CRL_REASON_PRIVILEGE_WITHDRAWN** - Privilege withdrawn
  - **10: CRL_REASON_AA_COMPROMISE** - AA compromise
  - **-1. Unrevoke** - Unrevokes

Options:

Windows Command Prompt

```
[-config Machine\CAName]
```

-isvalid

Displays the disposition of the current certificate.

Windows Command Prompt

```
certutil [options] -isvalid SerialNumber | CertHash
```

Options:

Windows Command Prompt

```
[-config Machine\CAName]
```

-getconfig

Gets the default configuration string.

Windows Command Prompt

```
certutil [options] -getconfig
```

Options:

Windows Command Prompt

```
[-idispatch] [-config Machine\CAName]
```

-getconfig2

Gets the default configuration string via ICertGetConfig.

Windows Command Prompt

```
certutil [options] -getconfig2
```

Options:

Windows Command Prompt

```
[-idispatch]
```

-getconfig3

Gets configuration via ICertConfig.

Windows Command Prompt

```
certutil [options] -getconfig3
```

Options:

Windows Command Prompt

```
[-idispatch]
```

-ping

Attempts to contact the Active Directory Certificate Services Request interface.

Windows Command Prompt

```
certutil [options] -ping [MaxSecondsToWait | CAMachineList]
```

Where:

- **CAMachineList** is a comma-separated list of CA machine names. For a single machine, use a terminating comma. This option also displays the site cost for each CA machine.

Options:

Windows Command Prompt

```
[-config Machine\CAName] [-Anonymous] [-Kerberos] [-ClientCertificate
ClientCertId] [-UserName UserName] [-p Password]
```

-pingadmin

Attempts to contact the Active Directory Certificate Services Admin interface.

Windows Command Prompt

```
certutil [options] -pingadmin
```

Options:

Windows Command Prompt

```
[-config Machine\CAName]
```

-CAInfo

Displays information about the certification authority.

Windows Command Prompt

```
certutil [options] -CAInfo [InfoName [Index | ErrorCode]]
```

Where:

- **InfoName** indicates the CA property to display, based on the following infoname argument syntax:
  - ***** - Displays all properties
  - **ads** - Advanced Server
  - **aia [Index]** - AIA URLs
  - **cdp [Index]** - CDP URLs
  - **cert [Index]** - CA cert
  - **certchain [Index]** - CA cert chain
  - **certcount** - CA cert count
  - **certcrlchain [Index]** - CA cert chain with CRLs
  - **certstate [Index]** - CA cert
  - **certstatuscode [Index]** - CA cert verify status
  - **certversion [Index]** - CA cert version
  - **CRL [Index]** - Base CRL
  - **crlstate [Index]** - CRL
  - **crlstatus [Index]** - CRL Publish Status
  - **cross- [Index]** - Backward cross cert
  - **cross+ [Index]** - Forward cross cert
  - **crossstate- [Index]** - Backward cross cert
  - **crossstate+ [Index]** - Forward cross cert
  - **deltacrl [Index]** - Delta CRL
  - **deltacrlstatus [Index]** - Delta CRL Publish Status
  - **dns** - DNS Name
  - **dsname** - Sanitized CA short name (DS name)
  - **error1 ErrorCode** - Error message text
  - **error2 ErrorCode** - Error message text and error code
  - **exit [Index]** - Exit module description
  - **exitcount** - Exit module count

    - **file** - File version
    - **info** - CA info
    - **kra [Index]** - KRA cert
    - **kracount** - KRA cert count
    - **krastate [Index]** - KRA cert
    - **kraused** - KRA cert used count
    - **localename** - CA locale name
    - **name** - CA name
    - **ocsp [Index]** - OCSP URLs
    - **parent** - Parent CA
    - **policy** - Policy module description
    - **product** - Product version
    - **propidmax** - Maximum CA PropId
    - **role** - Role Separation
    - **sanitizedname** - Sanitized CA name
    - **sharedfolder** - Shared folder
    - **subjecttemplateoids** - Subject Template OIDs
    - **templates** - Templates
    - **type** - CA type
    - **xchg [Index]** - CA exchange cert
    - **xchgchain [Index]** - CA exchange cert chain
    - **xchgcount** - CA exchange cert count
    - **xchgcrlchain [Index]** - CA exchange cert chain with CRLs
- **index** is the optional zero-based property index.
- **errorcode** is the numeric error code.

Options:

Windows Command Prompt

```
[-f] [-split] [-config Machine\CAName]
```

-CAPropInfo

Displays CA Property Type information.

Windows Command Prompt

```
certutil [options] -CAInfo [InfoName [Index | ErrorCode]]
```

Options:

Windows Command Prompt

```
[-idispatch] [-v1] [-admin] [-config Machine\CAName]
```

-ca.cert

Retrieves the certificate for the certification authority.

Windows Command Prompt

```
certutil [options] -ca.cert OutCACertFile [Index]
```

Where:

- **OutCACertFile** is the output file.
- **Index** is the CA certificate renewal index (defaults to most recent).

Options:

Windows Command Prompt

```
[-f] [-split] [-config Machine\CAName]
```

-ca.chain

Retrieves the certificate chain for the certification authority.

Windows Command Prompt

```
certutil [options] -ca.chain OutCACertChainFile [Index]
```

Where:

- **OutCACertChainFile** is the output file.
- **Index** is the CA certificate renewal index (defaults to most recent).

Options:

Windows Command Prompt

```
[-f] [-split] [-config Machine\CAName]
```

-GetCRL

Gets a certificate revocation list (CRL).

Windows Command Prompt

```
certutil [options] -GetCRL OutFile [Index] [delta]
```

Where:

- **Index** is the CRL index or key index (defaults to CRL for most recent key).
- **delta** is the delta CRL (default is base CRL).

Options:

Windows Command Prompt

```
[-f] [-split] [-config Machine\CAName]
```

-CRL

Publishes new certificate revocation lists (CRLs) or delta CRLs.

Windows Command Prompt

```
certutil [options] -CRL [dd:hh | republish] [delta]
```

Where:

- **dd:hh** is the new CRL validity period in days and hours.
- **republish** republishes the most recent CRLs.
- **delta** publishes the delta CRLs only (default is base and delta CRLs).

Options:

Windows Command Prompt

```
[-split] [-config Machine\CAName]
```

-shutdown

Shuts down the Active Directory Certificate Services.

Windows Command Prompt

```
certutil [options] -shutdown
```

Options:

Windows Command Prompt

```
[-config Machine\CAName]
```

-installCert

Installs a certification authority certificate.

Windows Command Prompt

```
certutil [options] -installCert [CACertFile]
```

Options:

Windows Command Prompt

```
[-f] [-silent] [-config Machine\CAName]
```

-renewCert

Renews a certification authority certificate.

Windows Command Prompt

```
certutil [options] -renewCert [ReuseKeys] [Machine\ParentCAName]
```

Options:

Windows Command Prompt

```
[-f] [-silent] [-config Machine\CAName]
```

- Use `-f` to ignore an outstanding renewal request, and to generate a new request.

-schema

Dumps the schema for the certificate.

Windows Command Prompt

```
certutil [options] -schema [Ext | Attrib | CRL]
```

Where:

- The command defaults to the Request and Certificate table.
- **Ext** is the extension table.
- **Attribute** is the attribute table.
- **CRL** is the CRL table.

Options:

Windows Command Prompt

```
[-split] [-config Machine\CAName]
```

-view

Dumps the certificate view.

Windows Command Prompt

```
certutil [options] -view [Queue | Log | LogFail | Revoked | Ext | Attrib |
CRL] [csv]
```

Where:

- **Queue** dumps a specific request queue.
- **Log** dumps the issued or revoked certificates, plus any failed requests.
- **LogFail** dumps the failed requests.
- **Revoked** dumps the revoked certificates.
- **Ext** dumps the extension table.
- **Attrib** dumps the attribute table.
- **CRL** dumps the CRL table.
- **csv** provides the output using comma-separated values.

Options:

Windows Command Prompt

```
[-silent] [-split] [-config Machine\CAName] [-restrict RestrictionList] [-
out ColumnList]
```

Remarks

- To display the **StatusCode** column for all entries, type `-out StatusCode`
- To display all columns for the last entry, type: `-restrict RequestId==$`
- To display the **RequestId** and **Disposition** for three requests, type: `-restrict requestID>=37,requestID<40 -out requestID,disposition`
- To display Row IDs **Row IDs** and **CRL numbers** for all Base CRLs, type: `-restrict crlminbase=0 -out crlrowID,crlnumber crl`
- To display Base CRL number 3, type: `-v -restrict crlminbase=0,crlnumber=3 -out crlrawcrl crl`
- To display the entire CRL table, type: `CRL`
- Use `Date[+|-dd:hh]` for date restrictions.
- Use `now+dd:hh` for a date relative to the current time.
- Templates contain Extended Key Usages (EKUs), which are object identifiers (OIDs) that describe how the certificate is used. Certificates don't always include template common names or display names, but they always contain the template EKUs. You can extract the EKUs for a specific certificate template from Active Directory and then restrict views based on that extension.

-db

Dumps the raw database.

Windows Command Prompt

```
certutil [options] -db
```

Options:

Windows Command Prompt

```
[-config Machine\CAName] [-restrict RestrictionList] [-out ColumnList]
```

-deleterow

Deletes a row from the server database.

Windows Command Prompt

```
certutil [options] -deleterow RowId | Date [Request | Cert | Ext | Attrib |
CRL]
```

Where:

- **Request** deletes the failed and pending requests, based on submission date.
- **Cert** deletes the expired and revoked certificates, based on expiration date.
- **Ext** deletes the extension table.
- **Attrib** deletes the attribute table.
- **CRL** deletes the CRL table.

Options:

Windows Command Prompt

```
[-f] [-config Machine\CAName]
```

Examples

- To delete failed and pending requests submitted by January 22, 2001, type: `1/22/2001 request`
- To delete all certificates that expired by January 22, 2001, type: `1/22/2001 cert`
- To delete the certificate row, attributes, and extensions for RequestID 37, type: `37`
- To delete CRLs that expired by January 22, 2001, type: `1/22/2001 crl`

> **Note**
>
> **Date** expects the format `mm/dd/yyyy` rather then `dd/mm/yyyy`, for example `1/22/2001` rather than `22/1/2001` for January 22, 2001. If your server isn't configured with US regional settings, using the **Date** argument might produce unexpected results.

-backup

Backs up the Active Directory Certificate Services.

Windows Command Prompt

```
certutil [options] -backup BackupDirectory [Incremental] [KeepLog]
```

Where:

- **BackupDirectory** is the directory to store the backed up data.
- **Incremental** performs an incremental backup only (default is full backup).
- **KeepLog** preserves the database log files (default is to truncate log files).

Options:

Windows Command Prompt

```
[-f] [-config Machine\CAName] [-p Password] [-ProtectTo SAMNameAndSIDList]
```

-backupDB

Backs up the Active Directory Certificate Services database.

Windows Command Prompt

```
certutil [options] -backupdb BackupDirectory [Incremental] [KeepLog]
```

Where:

- **BackupDirectory** is the directory to store the backed up database files.
- **Incremental** performs an incremental backup only (default is full backup).
- **KeepLog** preserves the database log files (default is to truncate log files).

Options:

Windows Command Prompt

```
[-f] [-config Machine\CAName]
```

-backupkey

Backs up the Active Directory Certificate Services certificate and private key.

Windows Command Prompt

```
certutil [options] -backupkey BackupDirectory
```

Where:

- **BackupDirectory** is the directory to store the backed up PFX file.

Options:

```
Windows Command Prompt

[-f] [-config Machine\CAName] [-p password] [-ProtectTo SAMNameAndSIDList]
[-t Timeout]
```

-restore

Restores the Active Directory Certificate Services.

```
Windows Command Prompt

certutil [options] -restore BackupDirectory
```

Where:

- **BackupDirectory** is the directory containing the data to be restored.

Options:

```
Windows Command Prompt

[-f] [-config Machine\CAName] [-p password]
```

-restoredb

Restores the Active Directory Certificate Services database.

```
Windows Command Prompt

certutil [options] -restoredb BackupDirectory
```

Where:

- **BackupDirectory** is the directory containing the database files to be restored.

Options:

```
Windows Command Prompt
```

```
[-f] [-config Machine\CAName]
```

-restorekey

Restores the Active Directory Certificate Services certificate and private key.

Windows Command Prompt

```
certutil [options] -restorekey BackupDirectory | PFXFile
```

Where:

- **BackupDirectory** is the directory containing PFX file to be restored.
- **PFXFile** is the PFX file to be restored.

Options:

Windows Command Prompt

```
[-f] [-config Machine\CAName] [-p password]
```

-exportPFX

Exports the certificates and private keys. For more information, see the `-store` parameter in this article.

Windows Command Prompt

```
certutil [options] -exportPFX [CertificateStoreName] CertId PFXFile
[Modifiers]
```

Where:

- **CertificateStoreName** is the name of the certificate store.
- **CertId** is the certificate or CRL match token.
- **PFXFile** is the PFX file to be exported.
- **Modifiers** are the comma-separated list, which can include one or more of the following:
  - **CryptoAlgorithm=** specifies the cryptographic algorithm to use for encrypting the PFX file, such as `TripleDES-Sha1` or `Aes256-Sha256`.

- **EncryptCert** - Encrypts the private key associated with the certificate with a password.
- **ExportParameters** -Exports the private key parameters in addition to the certificate and private key.
- **ExtendedProperties** - Includes all extended properties associated with the certificate in the output file.
- **NoEncryptCert** - Exports the private key without encrypting it.
- **NoChain** - Doesn't import the certificate chain.
- **NoRoot** - Doesn't import the root certificate.

-importPFX

Imports the certificates and private keys. For more information, see the `-store` parameter in this article.

Windows Command Prompt

```
certutil [options] -importPFX [CertificateStoreName] PFXFile [Modifiers]
```

Where:

- **CertificateStoreName** is the name of the certificate store.
- **PFXFile** is the PFX file to be imported.
- **Modifiers** are the comma-separated list, which can include one or more of the following:
  - **AT_KEYEXCHANGE** - Changes the keyspec to key exchange.
  - **AT_SIGNATURE** - Changes the keyspec to signature.
  - **ExportEncrypted** - Exports the private key associated with the certificate with password encryption.
  - **FriendlyName=** - Specifies a friendly name for the imported certificate.
  - **KeyDescription=** - Specifies a description for the private key associated with the imported certificate.
  - **KeyFriendlyName=** - Specifies a friendly name for the private key associated with the imported certificate.
  - **NoCert** - Doesn't import the certificate.
  - **NoChain** - Doesn't import the certificate chain.
  - **NoExport** - Makes the private key non-exportable.
  - **NoProtect** - Doesn't password protect keys by using a password.
  - **NoRoot** - Doesn't import the root certificate.
  - **Pkcs8** - Uses PKCS8 format for the private key in the PFX file.
  - **Protect** - Protects keys by using a password.

- **ProtectHigh** - Specifies that a high-security password must be associated with the private key.
- **VSM** - Stores the private key associated with the imported certificate in the Virtual Smart Card (VSC) container.

Options:

```
Windows Command Prompt
```

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-Silent] [-p Password] [-csp
Provider]
```

Remarks

- Defaults to personal machine store.

-dynamicfilelist

Displays a dynamic file list.

```
Windows Command Prompt
```

```
certutil [options] -dynamicfilelist
```

Options:

```
Windows Command Prompt
```

```
[-config Machine\CAName]
```

-databaselocations

Displays database locations.

```
Windows Command Prompt
```

```
certutil [options] -databaselocations
```

Options:

```
Windows Command Prompt
```

```
[-config Machine\CAName]
```

-hashfile

Generates and displays a cryptographic hash over a file.

Windows Command Prompt

```
certutil [options] -hashfile InFile [HashAlgorithm]
```

-store

Dumps the certificate store.

Windows Command Prompt

```
certutil [options] -store [CertificateStoreName [CertId [OutputFile]]]
```

Where:

- **CertificateStoreName** is the certificate store name. For example:
  - `My, CA (default), Root,`
  - `ldap:///CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?one?objectClass=certificationAuthority (View Root Certificates)`
  - `ldap:///CN=CAName,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?base?objectClass=certificationAuthority (Modify Root Certificates)`
  - `ldap:///CN=CAName,CN=MachineName,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint (View CRLs)`
  - `ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?base?objectClass=certificationAuthority (Enterprise CA Certificates)`
  - `ldap: (AD computer object certificates)`
  - `-user ldap: (AD user object certificates)`
- **CertId** is the certificate or CRL match token. This ID can be a:
  - Serial number

- SHA-1 certificate
- CRL, CTL or public key hash
- Numeric cert index (0, 1, and so on)
- Numeric CRL index (.0, .1, and so on)
- Numeric CTL index (..0, ..1, and so on)
- Public key
- Signature or extension ObjectId
- Certificate subject Common Name
- E-mail address
- UPN or DNS name
- Key container name or CSP name
- Template name or ObjectId
- EKU or Application Policies ObjectId
- CRL issuer Common Name.

Many of these identifiers might result in multiple matches.

- **OutputFile** is the file used to save the matching certificates.

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-Silent] [-split] [-dc DCName]
```

- The `-user` option accesses a user store instead of a machine store.
- The `-enterprise` option accesses a machine enterprise store.
- The `-service` option accesses a machine service store.
- The `-grouppolicy` option accesses a machine group policy store.

For example:

- `-enterprise NTAuth`
- `-enterprise Root 37`
- `-user My 26e0aaaf000000000004`
- `CA .11`

> **Note**
>
> Performance issues are observed when using the `-store` parameter given these two aspects:

1. When the number of certificates in the store exceeds 10.
2. When a **CertId** is specified, it's used to match all the listed types for every certificate. For example, if a **serial number** is provided, it will also attempt to match all other listed types.

If you are concerned about performance issues, PowerShell commands are recommended where it will only match the specified certificate type.

-enumstore

Enumerates the certificate stores.

Windows Command Prompt

```
certutil [options] -enumstore [\\MachineName]
```

Where:

- **MachineName** is the remote machine name.

Options:

Windows Command Prompt

```
[-enterprise] [-user] [-grouppolicy]
```

-addstore

Adds a certificate to the store. For more information, see the `-store` parameter in this article.

Windows Command Prompt

```
certutil [options] -addstore CertificateStoreName InFile
```

Where:

- **CertificateStoreName** is the certificate store name.
- **InFile** is the certificate or CRL file you want to add to the store.

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-dc DCName]
```

-delstore

Deletes a certificate from the store. For more information, see the `-store` parameter in this article.

Windows Command Prompt

```
certutil [options] -delstore CertificateStoreName certID
```

Where:

- **CertificateStoreName** is the certificate store name.
- **CertId** is the certificate or CRL match token.

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-Silent] [-dc DCName]
```

-verifystore

Verifies a certificate in the store. For more information, see the `-store` parameter in this article.

Windows Command Prompt

```
certutil [options] -verifystore CertificateStoreName [CertId]
```

Where:

- **CertificateStoreName** is the certificate store name.
- **CertId** is the certificate or CRL match token.

Options:

Windows Command Prompt

```
[-Enterprise] [-user] [-GroupPolicy] [-Silent] [-split] [-dc DCName] [-t
Timeout]
```

-repairstore

Repairs a key association or update certificate properties or the key security descriptor. For more information, see the `-store` parameter in this article.

Windows Command Prompt

```
certutil [options] -repairstore CertificateStoreName CertIdList
[PropertyInfFile | SDDLSecurityDescriptor]
```

Where:

- **CertificateStoreName** is the certificate store name.
- **CertIdList** is the comma-separated list of certificate or CRL match tokens. For more information, see the `-store` CertId description in this article.
- **PropertyInfFile** is the INF file containing external properties, including:

  Windows Command Prompt

  ```
  [Properties]
      19 = Empty ; Add archived property, OR:
      19 =       ; Remove archived property

      11 = {text}Friendly Name ; Add friendly name property

      127 = {hex} ; Add custom hexadecimal property
          _continue_ = 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
          _continue_ = 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f

      2 = {text} ; Add Key Provider Information property
        _continue_ = Container=Container Name&
        _continue_ = Provider=Microsoft Strong Cryptographic Provider&
        _continue_ = ProviderType=1&
        _continue_ = Flags=0&
        _continue_ = KeySpec=2

      9 = {text} ; Add Enhanced Key Usage property
        _continue_ = 1.3.6.1.5.5.7.3.2,
        _continue_ = 1.3.6.1.5.5.7.3.1,
  ```

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-Silent] [-split] [-csp Provider]
```

-viewstore

Dumps the certificates store. For more information, see the `-store` parameter in this article.

Windows Command Prompt

```
certutil [options] -viewstore [CertificateStoreName [CertId [OutputFile]]]
```

Where:

- **CertificateStoreName** is the certificate store name. For example:
  - `My, CA (default), Root,`
  - `ldap:///CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?one?objectClass=certificationAuthority (View Root Certificates)`
  - `ldap:///CN=CAName,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?base?objectClass=certificationAuthority (Modify Root Certificates)`
  - `ldap:///CN=CAName,CN=MachineName,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint (View CRLs)`
  - `ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?base?objectClass=certificationAuthority (Enterprise CA Certificates)`
  - `ldap: (AD computer object certificates)`
  - `-user ldap: (AD user object certificates)`
- **CertId** is the certificate or CRL match token. This can be a:
  - Serial number
  - SHA-1 certificate
  - CRL, CTL or public key hash
  - Numeric cert index (0, 1, and so on)
  - Numeric CRL index (.0, .1, and so on)
  - Numeric CTL index (..0, ..1, and so on)
  - Public key

    - Signature or extension ObjectId
    - Certificate subject Common Name
    - E-mail address
    - UPN or DNS name
    - Key container name or CSP name
    - Template name or ObjectId
    - EKU or Application Policies ObjectId
    - CRL issuer Common Name.

Many of these may result in multiple matches.

- **OutputFile** is the file used to save the matching certificates.

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-dc DCName]
```

- The `-user` option accesses a user store instead of a machine store.
- The `-enterprise` option accesses a machine enterprise store.
- The `-service` option accesses a machine service store.
- The `-grouppolicy` option accesses a machine group policy store.

For example:

- `-enterprise NTAuth`
- `-enterprise Root 37`
- `-user My 26e0aaaf000000000004`
- `CA .11`

-viewdelstore

Deletes a certificate from the store.

Windows Command Prompt

```
certutil [options] -viewdelstore [CertificateStoreName [CertId
[OutputFile]]]
```

Where:

- **CertificateStoreName** is the certificate store name. For example:

    - `My, CA (default), Root,`
    - `ldap:///CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?one?objectClass=certificationAuthority (View Root Certificates)`
    - `ldap:///CN=CAName,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?base?objectClass=certificationAuthority (Modify Root Certificates)`
    - `ldap:///CN=CAName,CN=MachineName,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint (View CRLs)`
    - `ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=cpandl,DC=com?cACertificate?base?objectClass=certificationAuthority (Enterprise CA Certificates)`
    - `ldap: (AD computer object certificates)`
    - `-user ldap: (AD user object certificates)`

- **CertId** is the certificate or CRL match token. This can be a:
    - Serial number
    - SHA-1 certificate
    - CRL, CTL or public key hash
    - Numeric cert index (0, 1, and so on)
    - Numeric CRL index (.0, .1, and so on)
    - Numeric CTL index (..0, ..1, and so on)
    - Public key
    - Signature or extension ObjectId
    - Certificate subject Common Name
    - E-mail address
    - UPN or DNS name
    - Key container name or CSP name
    - Template name or ObjectId
    - EKU or Application Policies ObjectId
    - CRL issuer Common Name. Many of these may result in multiple matches.

- **OutputFile** is the file used to save the matching certificates.

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-dc DCName]
```

- The `-user` option accesses a user store instead of a machine store.
- The `-enterprise` option accesses a machine enterprise store.
- The `-service` option accesses a machine service store.
- The `-grouppolicy` option accesses a machine group policy store.

For example:

- `-enterprise NTAuth`
- `-enterprise Root 37`
- `-user My 26e0aaaf000000000004`
- `CA .11`

-UI

Invokes the certutil interface.

Windows Command Prompt

```
certutil [options] -UI File [import]
```

-TPMInfo

Displays Trusted Platform Module Information.

Windows Command Prompt

```
certutil [options] -TPMInfo
```

Options:

Windows Command Prompt

```
[-f] [-Silent] [-split]
```

-attest

Specifies that the certificate request file should be attested.

Windows Command Prompt

```
certutil [options] -attest RequestFile
```

Options:

```
Windows Command Prompt
[-user] [-Silent] [-split]
```

-getcert

Selects a certificate from a selection UI.

```
Windows Command Prompt
certutil [options] [ObjectId | ERA | KRA [CommonName]]
```

Options:

```
Windows Command Prompt
[-Silent] [-split]
```

-ds

Displays directory service (DS) distinguished names (DNs).

```
Windows Command Prompt
certutil [options] -ds [CommonName]
```

Options:

```
Windows Command Prompt
[-f] [-user] [-split] [-dc DCName]
```

-dsDel

Deletes DS DNs.

```
Windows Command Prompt
certutil [options] -dsDel [CommonName]
```

Options:

Windows Command Prompt

```
[-user] [-split] [-dc DCName]
```

-dsPublish

Publishes a certificate or certificate revocation list (CRL) to Active Directory.

Windows Command Prompt

```
certutil [options] -dspublish CertFile [NTAuthCA | RootCA | SubCA | CrossCA
| KRA | User | Machine]
certutil [options] -dspublish CRLfile [DSCDPContainer [DSCDPCN]]
```

Where:

- **CertFile** is the name of the certificate file to publish.
- **NTAuthCA** publishes the certificate to the DS Enterprise store.
- **RootCA** publishes the certificate to the DS Trusted Root store.
- **SubCA** publishes the CA certificate to the DS CA object.
- **CrossCA** publishes the cross-certificate to the DS CA object.
- **KRA** publishes the certificate to the DS Key Recovery Agent object.
- **User** publishes the certificate to the User DS object.
- **Machine** publishes the certificate to the Machine DS object.
- **CRLfile** is the name of the CRL file to publish.
- **DSCDPContainer** is the DS CDP container CN, usually the CA machine name.
- **DSCDPCN** is the DS CDP object CN based on the sanitized CA short name and key index.

Options:

Windows Command Prompt

```
[-f] [-user] [-dc DCName]
```

- Use `-f` to create a new DS object.

-dsCert

Displays DS certificates.

Windows Command Prompt

```
certutil [options] -dsCert [FullDSDN] | [CertId [OutFile]]
```

Options:

Windows Command Prompt

```
[-Enterprise] [-user] [-config Machine\CAName] [-dc DCName]
```

-dsCRL

Displays DS CRLs.

Windows Command Prompt

```
certutil [options] -dsCRL [FullDSDN] | [CRLIndex [OutFile]]
```

Options:

Windows Command Prompt

```
[-idispatch] [-Enterprise] [-user] [-config Machine\CAName] [-dc DCName]
```

-dsDeltaCRL

Displays DS delta CRLs.

Windows Command Prompt

```
certutil [options] -dsDeltaCRL [FullDSDN] | [CRLIndex [OutFile]]
```

Options:

Windows Command Prompt

```
[-Enterprise] [-user] [-config Machine\CAName] [-dc DCName]
```

-dsTemplate

Displays DS template attributes.

Windows Command Prompt

```
certutil [options] -dsTemplate [Template]
```

Options:

Windows Command Prompt

```
[Silent] [-dc DCName]
```

-dsAddTemplate

Adds DS templates.

Windows Command Prompt

```
certutil [options] -dsAddTemplate TemplateInfFile
```

Options:

Windows Command Prompt

```
[-dc DCName]
```

-ADTemplate

Displays Active Directory templates.

Windows Command Prompt

```
certutil [options] -ADTemplate [Template]
```

Options:

Windows Command Prompt

```
[-f] [-user] [-ut] [-mt] [-dc DCName]
```

-Template

Displays the certificate enrollment policy templates.

Options:

```
Windows Command Prompt
certutil [options] -Template [Template]
```

Options:

```
Windows Command Prompt
[-f] [-user] [-Silent] [-PolicyServer URLOrId] [-Anonymous] [-Kerberos] [-
ClientCertificate ClientCertId] [-UserName UserName] [-p Password]
```

-TemplateCAs

Displays the certification authorities (CAs) for a certificate template.

```
Windows Command Prompt
certutil [options] -TemplateCAs Template
```

Options:

```
Windows Command Prompt
[-f] [-user] [-dc DCName]
```

-CATemplates

Displays templates for the Certificate Authority.

```
Windows Command Prompt
certutil [options] -CATemplates [Template]
```

Options:

```
Windows Command Prompt
[-f] [-user] [-ut] [-mt] [-config Machine\CAName] [-dc DCName]
```

-SetCATemplates

Sets the certificate templates that the Certificate Authority can issue.

Windows Command Prompt

```
certutil [options] -SetCATemplates [+ | -] TemplateList
```

Where:

- The `+` sign adds certificate templates to the CA's available template list.
- The `-` sign removes certificate templates from the CA's available template list.

-SetCASites

Manages site names, including setting, verifying, and deleting Certificate Authority site names.

Windows Command Prompt

```
certutil [options] -SetCASites [set] [SiteName]
certutil [options] -SetCASites verify [SiteName]
certutil [options] -SetCASites delete
```

Where:

- **SiteName** is allowed only when targeting a single Certificate Authority.

Options:

Windows Command Prompt

```
[-f] [-config Machine\CAName] [-dc DCName]
```

Remarks

- The `-config` option targets a single Certificate Authority (default is all CAs).
- The `-f` option can be used to override validation errors for the specified **SiteName** or to delete all CA site names.

> ⓘ **Note**

For more information about configuring CAs for Active Directory Domain Services (AD DS) site awareness, see **AD DS Site Awareness for AD CS and PKI clients**.

-enrollmentServerURL

Displays, adds, or deletes enrollment server URLs associated with a CA.

Windows Command Prompt

```
certutil [options] -enrollmentServerURL [URL AuthenticationType [Priority]
[Modifiers]]
certutil [options] -enrollmentserverURL URL delete
```

Where:

- **AuthenticationType** specifies one of the following client authentication methods while adding a URL:
  - **Kerberos** - Use Kerberos SSL credentials.
  - **UserName** - Use a named account for SSL credentials.
  - **ClientCertificate** - Use X.509 Certificate SSL credentials.
  - **Anonymous** - Use anonymous SSL credentials.
- **delete** deletes the specified URL associated with the CA.
- **Priority** defaults to `1` if not specified when adding a URL.
- **Modifiers** is a comma-separated list, which includes one or more of the following:
  - **AllowRenewalsOnly** only renewal requests can be submitted to this CA via this URL.
  - **AllowKeyBasedRenewal** allows use of a certificate that has no associated account in the AD. This applies only with **ClientCertificate** and **AllowRenewalsOnly** mode.

Options:

Windows Command Prompt

```
[-config Machine\CAName] [-dc DCName]
```

-ADCA

Displays the Active Directory Certificate Authorities.

Windows Command Prompt

```
certutil [options] -ADCA [CAName]
```

Options:

Windows Command Prompt

```
[-f] [-split] [-dc DCName]
```

-CA

Displays the enrollment policy Certificate Authorities.

Windows Command Prompt

```
certutil [options] -CA [CAName | TemplateName]
```

Options:

Windows Command Prompt

```
[-f] [-user] [-Silent] [-split] [-PolicyServer URLOrId] [-Anonymous] [-
Kerberos] [-ClientCertificate ClientCertId] [-UserName UserName] [-p
Password]
```

-Policy

Displays the enrollment policy.

Windows Command Prompt

```
certutil [options] -Policy
```

Options:

Windows Command Prompt

```
[-f] [-user] [-Silent] [-split] [-PolicyServer URLOrId] [-Anonymous] [-
Kerberos] [-ClientCertificate ClientCertId] [-UserName UserName] [-p
Password]
```

-PolicyCache

Displays or deletes enrollment policy cache entries.

Windows Command Prompt

```
certutil [options] -PolicyCache [delete]
```

Where:

- **delete** deletes the policy server cache entries.
- **-f** deletes all cache entries

Options:

Windows Command Prompt

```
[-f] [-user] [-policyserver URLorID]
```

-CredStore

Displays, adds, or deletes Credential Store entries.

Windows Command Prompt

```
certutil [options] -CredStore [URL]
certutil [options] -CredStore URL add
certutil [options] -CredStore URL delete
```

Where:

- **URL** is the target URL. You can also use `*` to match all entries or `https://machine*` to match a URL prefix.
- **add** adds a credential store entry. Using this option also requires the use of SSL credentials.
- **delete** deletes credential store entries.
- **-f** overwrites a single entry or deletes multiple entries.

Options:

Windows Command Prompt

```
[-f] [-user] [-Silent] [-Anonymous] [-Kerberos] [-ClientCertificate
ClientCertId] [-UserName UserName] [-p Password]
```

-InstallDefaultTemplates

Installs the default certificate templates.

```
Windows Command Prompt
certutil [options] -InstallDefaultTemplates
```

Options:

```
Windows Command Prompt
[-dc DCName]
```

-URL

Verifies certificate or CRL URLs.

```
Windows Command Prompt
certutil [options] -URL InFile | URL
```

Options:

```
Windows Command Prompt
[-f] [-split]
```

-URLCache

Displays or deletes URL cache entries.

```
Windows Command Prompt
certutil [options] -URLcache [URL | CRL | * [delete]]
```

Where:

- **URL** is the cached URL.
- **CRL** runs on all cached CRL URLs only.
- * operates on all cached URLs.
- **delete** deletes relevant URLs from the current user's local cache.

- **-f** forces fetching a specific URL and updating the cache.

Options:

```
Windows Command Prompt

[-f] [-split]
```

-pulse

Pulses an autoenrollment event or NGC task.

```
Windows Command Prompt

certutil [options] -pulse [TaskName [SRKThumbprint]]
```

Where:

- **TaskName** is the task to trigger.
  - **Pregen** is the NGC Key pregen task.
  - **AIKEnroll** is the NGC AIK certificate enrollment task. (Defaults to the autoenrollment event).
- **SRKThumbprint** is the thumbprint of the Storage Root Key
- **Modifiers**:
  - Pregen
  - PregenDelay
  - AIKEnroll
  - CryptoPolicy
  - NgcPregenKey
  - DIMSRoam

Options:

```
Windows Command Prompt

[-user]
```

-MachineInfo

Displays information about the Active Directory machine object.

```
Windows Command Prompt
```

```
certutil [options] -MachineInfo DomainName\MachineName$
```

-DCInfo

Displays information about the domain controller. The default displays DC certificates without verification.

Windows Command Prompt

```
certutil [options] -DCInfo [Domain] [Verify | DeleteBad | DeleteAll]
```

- **Modifiers**:
  - Verify
  - DeleteBad
  - DeleteAll

Options:

Windows Command Prompt

```
[-f] [-user] [-urlfetch] [-dc DCName] [-t Timeout]
```

> **Tip**
>
> The ability to specify an Active Directory Domain Services (AD DS) domain **[Domain]** and to specify a domain controller (**-dc**) was added in Windows Server 2012. To successfully run the command, you must use an account that is a member of **Domain Admins** or **Enterprise Admins**. The behavior modifications of this command are as follows:
>
> - If a domain is not specified and a specific domain controller is not specified, this option returns a list of domain controllers to process from the default domain controller.
> - If a domain is not specified, but a domain controller is specified, a report of the certificates on the specified domain controller is generated.
> - If a domain is specified, but a domain controller is not specified, a list of domain controllers is generated along with reports on the certificates for each domain controller in the list.

- If the domain and domain controller are specified, a list of domain controllers is generated from the targeted domain controller. A report of the certificates for each domain controller in the list is also generated.

For example, assume there is a domain named CPANDL with a domain controller named CPANDL-DC1. You can run the following command to a retrieve a list of domain controllers and their certificates from CPANDL-DC1: `certutil -dc cpandl-dc1 -DCInfo cpandl`.

-EntInfo

Displays information about an enterprise Certificate Authority.

Windows Command Prompt

```
certutil [options] -EntInfo DomainName\MachineName$
```

Options:

Windows Command Prompt

```
[-f] [-user]
```

-TCAInfo

Displays information about the Certificate Authority.

Windows Command Prompt

```
certutil [options] -TCAInfo [DomainDN | -]
```

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-urlfetch] [-dc DCName] [-t Timeout]
```

-SCInfo

Displays information about the smart card.

Windows Command Prompt

```
certutil [options] -scinfo [ReaderName [CRYPT_DELETEKEYSET]]
```

Where:

- **CRYPT_DELETEKEYSET** deletes all keys on the smart card.

Options:

Windows Command Prompt

```
[-Silent] [-split] [-urlfetch] [-t Timeout]
```

-SCRoots

Manages smart card root certificates.

Windows Command Prompt

```
certutil [options] -SCRoots update [+][InputRootFile] [ReaderName]
certutil [options] -SCRoots save @OutputRootFile [ReaderName]
certutil [options] -SCRoots view [InputRootFile | ReaderName]
certutil [options] -SCRoots delete [ReaderName]
```

Options:

Windows Command Prompt

```
[-f] [-split] [-p Password]
```

-key

Lists the keys stored in a key container.

Windows Command Prompt

```
certutil [options] -key [KeyContainerName | -]
```

Where:

- **KeyContainerName** is the key container name for the key to verify. This option defaults to machine keys. To switch to user keys, use `-user`.

- Using the `-` sign refers to using the default key container.

Options:

Windows Command Prompt

```
[-user] [-Silent] [-split] [-csp Provider] [-Location
AlternateStorageLocation]
```

-delkey

Deletes the named key container.

Windows Command Prompt

```
certutil [options] -delkey KeyContainerName
```

Options:

Windows Command Prompt

```
[-user] [-Silent] [-split] [-csp Provider] [-Location
AlternateStorageLocation]
```

-DeleteHelloContainer

Deletes the Windows Hello container, removing all associated credentials that are stored on the device, including any WebAuthn and FIDO credentials.

Users need to sign out after using this option for it to complete.

Windows Command Prompt

```
certutil [options] -DeleteHelloContainer
```

-verifykeys

Verifies a public or private key set.

Windows Command Prompt

```
certutil [options] -verifykeys [KeyContainerName CACertFile]
```

Where:

- **KeyContainerName** is the key container name for the key to verify. This option defaults to machine keys. To switch to user keys, use `-user`.
- **CACertFile** signs or encrypts certificate files.

Options:

Windows Command Prompt

```
[-f] [-user] [-Silent] [-config Machine\CAName]
```

Remarks

- If no arguments are specified, each signing CA certificate is verified against its private key.
- This operation can only be performed against a local CA or local keys.

-verify

Verifies a certificate, certificate revocation list (CRL), or certificate chain.

Windows Command Prompt

```
certutil [options] -verify CertFile [ApplicationPolicyList | -
[IssuancePolicyList]] [Modifiers]
certutil [options] -verify CertFile [CACertFile [CrossedCACertFile]]
certutil [options] -verify CRLFile CACertFile [IssuedCertFile]
certutil [options] -verify CRLFile CACertFile [DeltaCRLFile]
```

Where:

- **CertFile** is the name of the certificate to verify.
- **ApplicationPolicyList** is the optional comma-separated list of required Application Policy ObjectIds.
- **IssuancePolicyList** is the optional comma-separated list of required Issuance Policy ObjectIds.
- **CACertFile** is the optional issuing CA certificate to verify against.
- **CrossedCACertFile** is the optional certificate cross-certified by **CertFile**.
- **CRLFile** is the CRL file used to verify the **CACertFile**.
- **IssuedCertFile** is the optional issued certificate covered by the CRLfile.
- **DeltaCRLFile** is the optional delta CRL file.
- **Modifiers**:

- Strong - Strong signature verification
- MSRoot - Must chain to a Microsoft root
- MSTestRoot - Must chain to a Microsoft test root
- AppRoot - Must chain to a Microsoft application root
- EV - Enforce Extended Validation Policy

Options:

```
Windows Command Prompt

[-f] [-Enterprise] [-user] [-Silent] [-split] [-urlfetch] [-t Timeout] [-
sslpolicy ServerName]
```

Remarks

- Using **ApplicationPolicyList** restricts chain building to only chains valid for the specified Application Policies.
- Using **IssuancePolicyList** restricts chain building to only chains valid for the specified Issuance Policies.
- Using **CACertFile** verifies the fields in the file against **CertFile** or **CRLfile**.
- If **CACertFile** isn't specified, the full chain is built and verified against **CertFile**.
- If **CACertFile** and **CrossedCACertFile** are both specified, the fields in both files are verified against **CertFile**.
- Using **IssuedCertFile** verifies the fields in the file against **CRLfile**.
- Using **DeltaCRLFile** verifies the fields in the file against **CertFile**.

-verifyCTL

Verifies the AuthRoot or Disallowed Certificates CTL.

```
Windows Command Prompt

certutil [options] -verifyCTL CTLobject [CertDir] [CertFile]
```

Where:

- **CTLObject** identifies the CTL to verify, including:
  - **AuthRootWU** reads the AuthRoot CAB and matching certificates from the URL cache. Use `-f` to download from Windows Update instead.
  - **DisallowedWU** reads the Disallowed Certificates CAB and disallowed certificate store file from the URL cache. Use `-f` to download from Windows Update instead.

    - **PinRulesWU** reads the PinRules CAB from the URL cache. Use `-f` to download from Windows Update instead.
  - **AuthRoot** reads the registry-cached AuthRoot CTL. Use with `-f` and an untrusted **CertFile** to force the registry cached **AuthRoot** and Disallowed Certificate CTLs to update.
  - **Disallowed** reads the registry-cached Disallowed Certificates CTL. Use with `-f` and an untrusted **CertFile** to force the registry cached **AuthRoot** and Disallowed Certificate CTLs to update.
    - **PinRules** reads the registry cached PinRules CTL. Using `-f` has the same behavior as with **PinRulesWU**.
  - **CTLFileName** specifies the file or http path to the CTL or CAB file.

- **CertDir** specifies the folder containing certificates matching the CTL entries. Defaults to the same folder or website as the **CTLobject**. Using an http folder path requires a path separator at the end. If you don't specify **AuthRoot** or **Disallowed**, multiple locations are searched for matching certificates, including local certificate stores, crypt32.dll resources and the local URL cache. Use `-f` to download from Windows Update, as needed.

- **CertFile** specifies the certificate(s) to verify. Certificates are matched against CTL entries, displaying the results. This option suppresses most of the default output.

Options:

Windows Command Prompt

```
[-f] [-user] [-split]
```

-syncWithWU

Syncs certificates with Windows Update.

Windows Command Prompt

```
certutil [options] -syncWithWU DestinationDir
```

Where:

- **DestinationDir** is the specified directory.
- **f** forces an overwrite.
- **Unicode** writes redirected output in Unicode.
- **gmt** displays times as GMT.

- **seconds** displays times with seconds and milliseconds.
- **v** is a verbose operation.
- **PIN** is the Smart Card PIN.
- **WELL_KNOWN_SID_TYPE** is a numeric SID:
  - 22 - Local System
  - 23 - Local Service
  - 24 - Network Service

Remarks

The following files are downloaded by using the automatic update mechanism:

- *authrootstl.cab* contains the CTLs of non-Microsoft root certificates.
- *disallowedcertstl.cab* contains the CTLs of untrusted certificates.
- *disallowedcert.sst* contains the serialized certificate store, including the untrusted certificates.
- *thumbprint.crt* contains the non-Microsoft root certificates.

For example, `certutil -syncWithWU \\server1\PKI\CTLs`.

- If you use a nonexistent local path or folder as the destination folder, you see the error: `The system can't find the file specified. 0x80070002 (WIN32: 2 ERROR_FILE_NOT_FOUND)`
- If you use a nonexistent or unavailable network location as the destination folder, you see the error: `The network name can't be found. 0x80070043 (WIN32: 67 ERROR_BAD_NET_NAME)`
- If your server can't connect over TCP port 80 to Microsoft Automatic Update servers, you receive the following error: `A connection with the server couldn't be established 0x80072efd (INet: 12029 ERROR_INTERNET_CANNOT_CONNECT)`
- If your server is unable to reach the Microsoft Automatic Update servers with the DNS name `ctldl.windowsupdate.com`, you receive the following error: `The server name or address couldn't be resolved 0x80072ee7 (INet: 12007 ERROR_INTERNET_NAME_NOT_RESOLVED).`
- If you don't use the `-f` switch, and any of the CTL files already exist in the directory, you receive a file exists error: `certutil: -syncWithWU command FAILED: 0x800700b7 (WIN32/HTTP: 183 ERROR_ALREADY_EXISTS) Certutil: Can't create a file when that file already exists.`

- If there's a change in the trusted root certificates, you see: `Warning! Encountered the following no longer trusted roots: <folder path>\<thumbprint>.crt. Use "-f" option to force the delete of the above ".crt" files. Was "authrootstl.cab" updated? If yes, consider deferring the delete until all clients have been updated.`

Options:

```
Windows Command Prompt

[-f] [-Unicode] [-gmt] [-seconds] [-v] [-privatekey] [-pin PIN] [-sid
WELL_KNOWN_SID_TYPE]
```

-generateSSTFromWU

Generates a store file that is synced with Windows Update.

```
Windows Command Prompt

certutil [options] -generateSSTFromWU SSTFile
```

Where:

- **SSTFile** is the `.sst` file to be generated that contains the Third Party Roots downloaded from Windows Update.

Options:

```
Windows Command Prompt

[-f] [-split]
```

-generatePinRulesCTL

Generates a Certificate Trust List (CTL) file that contains a list of pinning rules.

```
Windows Command Prompt

certutil [options] -generatePinRulesCTL XMLFile CTLFile [SSTFile
[QueryFilesPrefix]]
```

Where:

- **XMLFile** is the input XML file to be parsed.
- **CTLFile** is the output CTL file to be generated.
- **SSTFile** is the optional *.sst* file to be created that contains all of the certificates used for pinning.
- **QueryFilesPrefix** are optional *Domains.csv* and *Keys.csv* files to be created for database query.
  - The **QueryFilesPrefix** string is prepended to each created file.
  - The **Domains.csv** file contains rule name, domain rows.
  - The **Keys.csv** file contains rule name, key SHA256 thumbprint rows.

Options:

Windows Command Prompt

```
[-f]
```

-downloadOcsp

Downloads the OCSP responses and writes to the directory.

Windows Command Prompt

```
certutil [options] -downloadOcsp CertificateDir OcspDir [ThreadCount]
[Modifiers]
```

Where:

- **CertificateDir** is the directory of a certificate, store and PFX files.
- **OcspDir** is the directory to write OCSP responses.
- **ThreadCount** is the optional maximum number of threads for concurrent downloading. Default is **10**.
- **Modifiers** are comma separated list of one or more of the following:
  - **DownloadOnce** - Downloads once and exits.
  - **ReadOcsp** - Reads from OcspDir instead of writing.

-generateHpkpHeader

Generates the HPKP header using certificates in a specified file or directory.

Windows Command Prompt

```
certutil [options] -generateHpkpHeader CertFileOrDir MaxAge [ReportUri]
```

```
[Modifiers]
```

Where:

- **CertFileOrDir** is the file or directory of certificates, which is the source of pin-sha256.
- **MaxAge** is the max-age value in seconds.
- **ReportUri** is the optional report-uri.
- **Modifiers** are comma separated list of one or more of the following:
  - **includeSubDomains** - Appends the includeSubDomains.

-flushCache

Flushes the specified caches in selected process, such as, lsass.exe.

Windows Command Prompt

```
certutil [options] -flushCache ProcessId CacheMask [Modifiers]
```

Where:

- **ProcessId** is the numeric ID of a process to flush. Set to **0** to flush all processes where flush is enabled.
- **CacheMask** is the bit mask of caches to be flushed either numeric or the following bits:
  - **0**: ShowOnly
  - **0x01**: CERT_WNF_FLUSH_CACHE_REVOCATION
  - **0x02**: CERT_WNF_FLUSH_CACHE_OFFLINE_URL
  - **0x04**: CERT_WNF_FLUSH_CACHE_MACHINE_CHAIN_ENGINE
  - **0x08**: CERT_WNF_FLUSH_CACHE_USER_CHAIN_ENGINES
  - **0x10**: CERT_WNF_FLUSH_CACHE_SERIAL_CHAIN_CERTS
  - **0x20**: CERT_WNF_FLUSH_CACHE_SSL_TIME_CERTS
  - **0x40**: CERT_WNF_FLUSH_CACHE_OCSP_STAPLING
- **Modifiers** are comma separated list of one or more of the following:
  - **Show** - Shows the caches being flushed. Certutil must be explicitly terminated.

-addEccCurve

Adds an ECC Curve.

Windows Command Prompt

```
certutil [options] -addEccCurve [CurveClass:]CurveName CurveParameters
[CurveOID] [CurveType]
```

Where:

- **CurveClass** is the ECC Curve Class type:
  - WEIERSTRASS (Default)
  - MONTGOMERY
  - TWISTED_EDWARDS
- **CurveName** is the ECC Curve name.
- **CurveParameters** are one of the following:
  - A certificate filename containing ASN encoded parameters.
  - A file containing ASN encoded parameters.
- **CurveOID** is the ECC Curve OID and is one of the following:
  - A certificate filename containing an ASN encoded OID.
  - An explicit ECC Curve OID.
- **CurveType** is the Schannel ECC NamedCurve point (numeric).

Options:

Windows Command Prompt

```
[-f]
```

-deleteEccCurve

Deletes the ECC Curve.

Windows Command Prompt

```
certutil [options] -deleteEccCurve CurveName | CurveOID
```

Where:

- **CurveName** is the ECC Curve name.
- **CurveOID** is the ECC Curve OID.

Options:

Windows Command Prompt

```
[-f]
```

-displayEccCurve

Displays the ECC Curve.

Windows Command Prompt

```
certutil [options] -displayEccCurve [CurveName | CurveOID]
```

Where:

- **CurveName** is the ECC Curve name.
- **CurveOID** is the ECC Curve OID.

Options:

Windows Command Prompt

```
[-f]
```

-csplist

Lists the cryptographic service providers (CSPs) installed on this machine for cryptographic operations.

Windows Command Prompt

```
certutil [options] -csplist [Algorithm]
```

Options:

Windows Command Prompt

```
[-user] [-Silent] [-csp Provider]
```

-csptest

Tests the CSPs installed on this machine.

Windows Command Prompt

```
certutil [options] -csptest [Algorithm]
```

Options:

Windows Command Prompt

```
[-user] [-Silent] [-csp Provider]
```

-CNGConfig

Displays CNG cryptographic configuration on this machine.

Windows Command Prompt

```
certutil [options] -CNGConfig
```

Options:

Windows Command Prompt

```
[-Silent]
```

-sign

Re-signs a certificate revocation list (CRL) or certificate.

Windows Command Prompt

```
certutil [options] -sign InFileList | SerialNumber | CRL OutFileList
[StartDate [+ | -dd:hh] + | -dd:hh] [+SerialNumberList | -SerialNumberList |
-ObjectIdList | @ExtensionFile]
certutil [options] -sign InFileList | SerialNumber | CRL OutFileList
[#HashAlgorithm] [+AlternateSignatureAlgorithm | -
AlternateSignatureAlgorithm]
certutil [options] -sign InFileList OutFileList [Subject:CN=...] [Issuer:hex
data]
```

Where:

- **InFileList** is the comma-separated list of certificate or CRL files to modify and re-sign.

- **SerialNumber** is the serial number of the certificate to create. The validity period and other options can't be present.
- **CRL** creates an empty CRL. The validity period and other options can't be present.
- **OutFileList** is the comma-separated list of modified certificate or CRL output files. The number of files must match infilelist.
- **StartDate+dd:hh** is the new validity period for the certificate or CRL files, including:
  - optional date plus
  - optional days and hours validity period If multiple fields are used, use a (+) or (-) separator. Use `now[+dd:hh]` to start at the current time. Use `now-dd:hh+dd:hh` to start at a fixed offset from the current time and a fixed validity period. Use `never` to have no expiration date (for CRLs only).
- **SerialNumberList** is the comma-separated serial number list of the files to add or remove.
- **ObjectIdList** is the comma-separated extension ObjectId list of the files to remove.
- **@ExtensionFile** is the INF file that contains the extensions to update or remove. For example:

  Windows Command Prompt

  ```
  [Extensions]
      2.5.29.31 = ; Remove CRL Distribution Points extension
      2.5.29.15 = {hex} ; Update Key Usage extension
      _continue_=03 02 01 86
  ```

- **HashAlgorithm** is the name of the hash algorithm. This must only be the text preceded by the `#` sign.
- **AlternateSignatureAlgorithm** is the alternate signature algorithm specifier.

Options:

Windows Command Prompt

```
[-nullsign] [-f] [-user] [-Silent] [-Cert CertId] [-csp Provider]
```

Remarks

- Using the minus sign (-) removes serial numbers and extensions.

- Using the plus sign (+) adds serial numbers to a CRL.
- You can use a list to remove both serial numbers and **ObjectIds** from a CRL at the same time.
- Using the minus sign before **AlternateSignatureAlgorithm** allows you to use the legacy signature format.
- Using the plus sign allows you to use the alternate signature format.
- If you don't specify **AlternateSignatureAlgorithm**, the signature format in the certificate or CRL is used.

-vroot

Creates or deletes web virtual roots and file shares.

Windows Command Prompt

```
certutil [options] -vroot [delete]
```

-vocsproot

Creates or deletes web virtual roots for an OCSP web proxy.

Windows Command Prompt

```
certutil [options] -vocsproot [delete]
```

-addEnrollmentServer

Adds an Enrollment Server application and application pool if necessary for the specified Certificate Authority. This command doesn't install binaries or packages.

Windows Command Prompt

```
certutil [options] -addEnrollmentServer Kerberos | UserName |
ClientCertificate [AllowRenewalsOnly] [AllowKeyBasedRenewal]
```

Where:

- **addEnrollmentServer** requires you to use an authentication method for the client connection to the Certificate Enrollment Server, including:
  - **Kerberos** uses Kerberos SSL credentials.
  - **UserName** uses named account for SSL credentials.

    - **ClientCertificate** uses X.509 Certificate SSL credentials.

- **Modifiers**:
    - **AllowRenewalsOnly** allows only renewal request submissions to the Certificate Authority through the URL.
    - **AllowKeyBasedRenewal** allows use of a certificate with no associated account in Active Directory. This applies when used with **ClientCertificate** and **AllowRenewalsOnly** mode.

Options:

```
Windows Command Prompt

[-config Machine\CAName]
```

-deleteEnrollmentServer

Deletes an Enrollment Server application and application pool if necessary for the specified Certificate Authority. This command doesn't install binaries or packages.

```
Windows Command Prompt

certutil [options] -deleteEnrollmentServer Kerberos | UserName |
ClientCertificate
```

Where:

- **deleteEnrollmentServer** requires you to use an authentication method for the client connection to the Certificate Enrollment Server, including:
    - **Kerberos** uses Kerberos SSL credentials.
    - **UserName** uses named account for SSL credentials.
    - **ClientCertificate** uses X.509 Certificate SSL credentials.

Options:

```
Windows Command Prompt

[-config Machine\CAName]
```

-addPolicyServer

Add a Policy Server application and application pool, if necessary. This command doesn't install binaries or packages.

Windows Command Prompt

```
certutil [options] -addPolicyServer Kerberos | UserName | ClientCertificate
[KeyBasedRenewal]
```

Where:

- **addPolicyServer** requires you to use an authentication method for the client connection to the Certificate Policy Server, including:
  - **Kerberos** uses Kerberos SSL credentials.
  - **UserName** uses named account for SSL credentials.
  - **ClientCertificate** uses X.509 Certificate SSL credentials.
- **KeyBasedRenewal** allows use of policies returned to the client containing keybasedrenewal templates. This option applies only for **UserName** and **ClientCertificate** authentication.

-deletePolicyServer

Deletes a Policy Server application and application pool, if necessary. This command doesn't remove binaries or packages.

Windows Command Prompt

```
certutil [options] -deletePolicyServer Kerberos | UserName |
ClientCertificate [KeyBasedRenewal]
```

Where:

- **deletePolicyServer** requires you to use an authentication method for the client connection to the Certificate Policy Server, including:
  - **Kerberos** uses Kerberos SSL credentials.
  - **UserName** uses named account for SSL credentials.
  - **ClientCertificate** uses X.509 Certificate SSL credentials.
- **KeyBasedRenewal** allows use of a KeyBasedRenewal policy server.

-Class

Displays COM registry information.

Windows Command Prompt

```
certutil [options] -Class [ClassId | ProgId | DllName | *]
```

Options:

Windows Command Prompt

```
[-f]
```

-7f

Checks certificate for 0x7f length encodings.

Windows Command Prompt

```
certutil [options] -7f CertFile
```

-oid

Displays the object identifier or sets a display name.

Windows Command Prompt

```
certutil [options] -oid ObjectId [DisplayName | delete [LanguageId [type]]]
certutil [options] -oid GroupId
certutil [options] -oid AlgId | AlgorithmName [GroupId]
```

Where:

- **ObjectId** is the ID to be displayed or to add to the display name.
- **GroupId** is the GroupID number (decimal) that ObjectIds enumerate.
- **AlgId** is the hexadecimal ID that objectID looks up.
- **AlgorithmName** is the algorithm name that objectID looks up.
- **DisplayName** displays the name to store in DS.
- **Delete** deletes the display name.
- **LanguageId** is the language ID value (defaults to current: 1033).
- **Type** is the type of DS object to create, including:
  - `1` - Template (default)
  - `2` - Issuance Policy
  - `3` - Application Policy
- `-f` creates a DS object.

Options:

Windows Command Prompt

```
[-f]
```

-error

Displays the message text associated with an error code.

Windows Command Prompt

```
certutil [options] -error ErrorCode
```

-getsmtpinfo

Gets Simple Mail Transfer Protocol (SMTP) information.

Windows Command Prompt

```
certutil [options] -getsmtpinfo
```

-setsmtpinfo

Sets SMTP information.

Windows Command Prompt

```
certutil [options] -setsmtpinfo LogonName
```

Options:

Windows Command Prompt

```
[-config Machine\CAName] [-p Password]
```

-getreg

Displays a registry value.

Windows Command Prompt

```
certutil [options] -getreg [{ca | restore | policy | exit | template |
enroll | chain | PolicyServers}\[ProgId\]] [RegistryValueName]
```

Where:

- **ca** uses a Certificate Authority's registry key.
- **restore** uses Certificate Authority's restore registry key.
- **policy** uses the policy module's registry key.
- **exit** uses the first exit module's registry key.
- **template** uses the template registry key (use `-user` for user templates).
- **enroll** uses the enrollment registry key (use `-user` for user context).
- **chain** uses the chain configuration registry key.
- **PolicyServers** uses the Policy Servers registry key.
- **ProgId** uses the policy or exit module's ProgID (registry subkey name).
- **RegistryValueName** uses the registry value name (use `Name*` to prefix match).
- **value** uses the new numeric, string or date registry value or filename. If a numeric value starts with `+` or `-`, the bits specified in the new value are set or cleared in the existing registry value.

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-config Machine\CAName]
```

Remarks

- If a string value starts with `+` or `-`, and the existing value is a `REG_MULTI_SZ` value, the string is added to or removed from the existing registry value. To force creation of a `REG_MULTI_SZ` value, add `\n` to the end of the string value.
- If the value starts with `\@`, the rest of the value is the name of the file containing the hexadecimal text representation of a binary value.
- If it doesn't refer to a valid file, it's instead parsed as `[Date][+|-][dd:hh]` which is an optional date plus or minus optional days and hours.
- If both are specified, use a plus sign (+) or minus sign (-) separator. Use `now+dd:hh` for a date relative to the current time.
- Use `i64` as a suffix to create a REG_QWORD value.
- Use `chain\chaincacheresyncfiletime @now` to effectively flush cached CRLs.
- Registry aliases:
  - Config
  - CA
  - Policy - PolicyModules
  - Exit - ExitModules

- Restore - RestoreInProgress
- Template - Software\Microsoft\Cryptography\CertificateTemplateCache
- Enroll - Software\Microsoft\Cryptography\AutoEnrollment (Software\Policies\Microsoft\Cryptography\AutoEnrollment)
- MSCEP - Software\Microsoft\Cryptography\MSCEP
- Chain - Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config
- PolicyServers - Software\Microsoft\Cryptography\PolicyServers (Software\Policies\Microsoft\Cryptography\PolicyServers)
- Crypt32 - System\CurrentControlSet\Services\crypt32
- NGC - System\CurrentControlSet\Control\Cryptography\Ngc
- AutoUpdate - Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate
- Passport - Software\Policies\Microsoft\PassportForWork
- MDM - Software\Microsoft\Policies\PassportForWork

-setreg

Sets a registry value.

Windows Command Prompt

```
certutil [options] -setreg [{ca | restore | policy | exit | template |
enroll | chain | PolicyServers}\[ProgId\]] RegistryValueName Value
```

Where:

- **ca** uses a Certificate Authority's registry key.
- **restore** uses Certificate Authority's restore registry key.
- **policy** uses the policy module's registry key.
- **exit** uses the first exit module's registry key.
- **template** uses the template registry key (use `-user` for user templates).
- **enroll** uses the enrollment registry key (use `-user` for user context).
- **chain** uses the chain configuration registry key.
- **PolicyServers** uses the Policy Servers registry key.
- **ProgId** uses the policy or exit module's ProgID (registry subkey name).
- **RegistryValueName** uses the registry value name (use `Name*` to prefix match).
- **Value** uses the new numeric, string or date registry value or filename. If a numeric value starts with `+` or `-`, the bits specified in the new value are set or cleared in the existing registry value.

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-config Machine\CAName]
```

Remarks

- If a string value starts with `+` or `-`, and the existing value is a `REG_MULTI_SZ` value, the string is added to or removed from the existing registry value. To force creation of a `REG_MULTI_SZ` value, add `\n` to the end of the string value.
- If the value starts with `\@`, the rest of the value is the name of the file containing the hexadecimal text representation of a binary value.
- If it doesn't refer to a valid file, it's instead parsed as `[Date][+|-][dd:hh]` which is an optional date plus or minus optional days and hours.
- If both are specified, use a plus sign (+) or minus sign (-) separator. Use `now+dd:hh` for a date relative to the current time.
- Use `i64` as a suffix to create a REG_QWORD value.
- Use `chain\chaincacheresyncfiletime @now` to effectively flush cached CRLs.

-delreg

Deletes a registry value.

Windows Command Prompt

```
certutil [options] -delreg [{ca | restore | policy | exit | template |
enroll |chain | PolicyServers}\[ProgId\]][RegistryValueName]
```

Where:

- **ca** uses a Certificate Authority's registry key.
- **restore** uses Certificate Authority's restore registry key.
- **policy** uses the policy module's registry key.
- **exit** uses the first exit module's registry key.
- **template** uses the template registry key (use `-user` for user templates).
- **enroll** uses the enrollment registry key (use `-user` for user context).
- **chain** uses the chain configuration registry key.
- **PolicyServers** uses the Policy Servers registry key.
- **ProgId** uses the policy or exit module's ProgID (registry subkey name).
- **RegistryValueName** uses the registry value name (use `Name*` to prefix match).

- **Value** uses the new numeric, string or date registry value or filename. If a numeric value starts with `+` or `-`, the bits specified in the new value are set or cleared in the existing registry value.

Options:

Windows Command Prompt

```
[-f] [-Enterprise] [-user] [-GroupPolicy] [-config Machine\CAName]
```

Remarks

- If a string value starts with `+` or `-`, and the existing value is a `REG_MULTI_SZ` value, the string is added to or removed from the existing registry value. To force creation of a `REG_MULTI_SZ` value, add `\n` to the end of the string value.
- If the value starts with `\@`, the rest of the value is the name of the file containing the hexadecimal text representation of a binary value.
- If it doesn't refer to a valid file, it's instead parsed as `[Date][+|-][dd:hh]` which is an optional date plus or minus optional days and hours.
- If both are specified, use a plus sign (+) or minus sign (-) separator. Use `now+dd:hh` for a date relative to the current time.
- Use `i64` as a suffix to create a REG_QWORD value.
- Use `chain\chaincacheresyncfiletime @now` to effectively flush cached CRLs.
- Registry aliases:
  - Config
  - CA
  - Policy - PolicyModules
  - Exit - ExitModules
  - Restore - RestoreInProgress
  - Template - Software\Microsoft\Cryptography\CertificateTemplateCache
  - Enroll - Software\Microsoft\Cryptography\AutoEnrollment (Software\Policies\Microsoft\Cryptography\AutoEnrollment)
  - MSCEP - Software\Microsoft\Cryptography\MSCEP
  - Chain - Software\Microsoft\Cryptography\OID\EncodingType 0\CertDllCreateCertificateChainEngine\Config
  - PolicyServers - Software\Microsoft\Cryptography\PolicyServers (Software\Policies\Microsoft\Cryptography\PolicyServers)
  - Crypt32 - System\CurrentControlSet\Services\crypt32
  - NGC - System\CurrentControlSet\Control\Cryptography\Ngc
  - AutoUpdate - Software\Microsoft\SystemCertificates\AuthRoot\AutoUpdate

- Passport - Software\Policies\Microsoft\PassportForWork
- MDM - Software\Microsoft\Policies\PassportForWork

-importKMS

Imports user keys and certificates into the server database for key archival.

Windows Command Prompt

```
certutil [options] -importKMS UserKeyAndCertFile [CertId]
```

Where:

- **UserKeyAndCertFile** is a data file with user private keys and certificates that are to be archived. This file can be:
  - An Exchange Key Management Server (KMS) export file.
  - A PFX file.
- **CertId** is a KMS export file decryption certificate match token. For more information, see the `-store` parameter in this article.
- `-f` imports certificates not issued by the Certificate Authority.

Options:

Windows Command Prompt

```
[-f] [-Silent] [-split] [-config Machine\CAName] [-p Password] [-symkeyalg
SymmetricKeyAlgorithm[,KeyLength]]
```

-ImportCert

Imports a certificate file into the database.

Windows Command Prompt

```
certutil [options] -ImportCert Certfile [ExistingRow]
```

Where:

- **ExistingRow** imports the certificate in place of a pending request for the same key.
- `-f` imports certificates not issued by the Certificate Authority.

Options:

Windows Command Prompt

```
[-f] [-config Machine\CAName]
```

Remarks

The Certificate Authority may also need to be configured to support foreign certificates by running `certutil -setreg ca\KRAFlags +KRAF_ENABLEFOREIGN`.

-GetKey

Retrieves an archived private key recovery blob, generates a recovery script, or recovers archived keys.

Windows Command Prompt

```
certutil [options] -GetKey SearchToken [RecoveryBlobOutFile]
certutil [options] -GetKey SearchToken script OutputScriptFile
certutil [options] -GetKey SearchToken retrieve | recover OutputFileBaseName
```

Where:

- **script** generates a script to retrieve and recover keys (default behavior if multiple matching recovery candidates are found, or if the output file isn't specified).
- **retrieve** retrieves one or more Key Recovery Blobs (default behavior if exactly one matching recovery candidate is found, and if the output file is specified). Using this option truncates any extension and appends the certificate-specific string and the `.rec` extension for each key recovery blob. Each file contains a certificate chain and an associated private key, still encrypted to one or more Key Recovery Agent certificates.
- **recover** retrieves and recovers private keys in one step (requires Key Recovery Agent certificates and private keys). Using this option truncates any extension and appends the `.p12` extension. Each file contains the recovered certificate chains and associated private keys, stored as a PFX file.
- **SearchToken** selects the keys and certificates to be recovered, including:
  - Certificate Common Name
  - Certificate Serial Number
  - Certificate SHA-1 hash (thumbprint)
  - Certificate KeyId SHA-1 hash (Subject Key Identifier)
  - Requester Name (domain\user)
  - UPN (user@domain)

- **RecoveryBlobOutFile** outputs a file with a certificate chain and an associated private key, still encrypted to one or more Key Recovery Agent certificates.
- **OutputScriptFile** outputs a file with a batch script to retrieve and recover private keys.
- **OutputFileBaseName** outputs a file base name.

Options:

Windows Command Prompt

```
[-f] [-UnicodeText] [-Silent] [-config Machine\CAName] [-p Password] [-
ProtectTo SAMNameAndSIDList] [-csp Provider]
```

Remarks

- For **retrieve**, any extension is truncated and a certificate-specific string and the `.rec` extensions are appended for each key recovery blob. Each file contains a certificate chain and an associated private key, still encrypted to one or more Key Recovery Agent certificates.
- For **recover**, any extension is truncated and the `.p12` extension is appended. Contains the recovered certificate chains and associated private keys, stored as a PFX file.

-RecoverKey

Recovers an archived private key.

Windows Command Prompt

```
certutil [options] -RecoverKey RecoveryBlobInFile [PFXOutFile
[RecipientIndex]]
```

Options:

Windows Command Prompt

```
[-f] [-user] [-Silent] [-split] [-p Password] [-ProtectTo SAMNameAndSIDList]
[-csp Provider] [-t Timeout]
```

-mergePFX

Merges PFX files.

Windows Command Prompt

```
certutil [options] -MergePFX PFXInFileList PFXOutFile [Modifiers]
```

Where:

- **PFXInFileList** is a comma-separated list of PFX input files.
- **PFXOutFile** is the name of the PFX output file.
- **Modifiers** are comma separated lists of one or more of the following:
  - **ExtendedProperties** includes any extended properties.
  - **NoEncryptCert** specifies to not encrypt the certificates.
  - **EncryptCert** specifies to encrypt the certificates.

Options:

Windows Command Prompt

```
[-f] [-user] [-split] [-p password] [-ProtectTo SAMNameAndSIDList] [-csp
Provider]
```

Remarks

- The password specified on the command line must be a comma-separated password list.
- If more than one password is specified, the last password is used for the output file. If only one password is provided or if the last password is `*`, the user is prompted for the output file password.

-convertEPF

Converts a PFX file into an EPF file.

Windows Command Prompt

```
certutil [options] -ConvertEPF PFXInFileList EPFOutFile [cast | cast-]
[V3CACertId][,Salt]
```

Where:

- **PFXInFileList** is a comma-separated list of PFX input files.
- **EPFOutFile** is the name of the PFX output file.
- **EPF** is the name of the EPF output file.

- **cast** uses CAST 64 encryption.
- **cast-** uses CAST 64 encryption (export).
- **V3CACertId** is the V3 CA certificate match token. For more information, see the `-store` parameter in this article.
- **Salt** is the EPF output file salt string.

Options:

```
Windows Command Prompt

[-f] [-Silent] [-split] [-dc DCName] [-p Password] [-csp Provider]
```

Remarks

- The password specified on the command line must be a comma-separated password list.
- If more than one password is specified, the last password is used for the output file. If only one password is provided or if the last password is `*`, the user is prompted for the output file password.

-add-chain

Adds a certificate chain.

```
Windows Command Prompt

certutil [options] -add-chain LogId certificate OutFile
```

Options:

```
Windows Command Prompt

[-f]
```

-add-pre-chain

Adds a pre-certificate chain.

```
Windows Command Prompt

certutil [options] -add-pre-chain LogId pre-certificate OutFile
```

Options:

Windows Command Prompt

```
[-f]
```

-get-sth

Gets a signed tree head.

Windows Command Prompt

```
certutil [options] -get-sth [LogId]
```

Options:

Windows Command Prompt

```
[-f]
```

-get-sth-consistency

Gets signed tree head changes.

Windows Command Prompt

```
certutil [options] -get-sth-consistency LogId TreeSize1 TreeSize2
```

Options:

Windows Command Prompt

```
[-f]
```

-get-proof-by-hash

Gets proof of a hash from a timestamp server.

Windows Command Prompt

```
certutil [options] -get-proof-by-hash LogId Hash [TreeSize]
```

Options:

Windows Command Prompt

```
[-f]
```

-get-entries

Retrieves entries from an event log.

Windows Command Prompt

```
certutil [options] -get-entries LogId FirstIndex LastIndex
```

Options:

Windows Command Prompt

```
[-f]
```

-get-roots

Retrieves the root certificates from the certificate store.

Windows Command Prompt

```
certutil [options] -get-roots LogId
```

Options:

Windows Command Prompt

```
[-f]
```

-get-entry-and-proof

Retrieves an event log entry and its cryptographic proof.

Windows Command Prompt

```
certutil [options] -get-entry-and-proof LogId Index [TreeSize]
```

Options:

Windows Command Prompt

```
[-f]
```

-VerifyCT

Verifies a certificate against the Certificate Transparency log.

Windows Command Prompt

```
certutil [options] -VerifyCT Certificate SCT [precert]
```

Options:

Windows Command Prompt

```
[-f]
```

-?

Displays the list of parameters.

Windows Command Prompt

```
certutil -?
certutil <name_of_parameter> -?
certutil -? -v
```

Where:

- **-?** displays the list of parameters
- **-<name_of_parameter> -?** displays help content for the specified parameter.
- **-? -v** displays a verbose list of parameters and options.

Options

This section defines all of the options you're able to specify, based on the command. Each parameter includes information about which options are valid for use.

Option	Description
-admin	Use ICertAdmin2 for CA properties.
-anonymous	Use anonymous SSL credentials.
-cert CertId	Signing certificate.
-clientcertificate clientCertId	Use X.509 Certificate SSL credentials. For selection UI, use `-clientcertificate`.
-config Machine\CAName	Certificate Authority and computer name string.
-csp provider	Provider: **KSP** - Microsoft Software Key Storage Provider **TPM** - Microsoft Platform Crypto Provider **NGC** - Microsoft Passport Key Storage Provider **SC** - Microsoft Smart Card Key Storage Provider
-dc DCName	Target a specific Domain Controller.
-enterprise	Use the local machine enterprise registry certificate store.
-f	Force overwrite.
-generateSSTFromWU SSTFile	Generate SST by using the automatic update mechanism.
-gmt	Display times using GMT.
-GroupPolicy	Use the group policy certificate store.
-idispatch	Use IDispatch instead of COM native methods.
-kerberos	Use Kerberos SSL credentials.
-location alternatestoragelocation	`(-loc)` AlternateStorageLocation.
-mt	Display machine templates.
-nocr	Encode text without CR characters.
-nocrlf	Encode text without CR-LF characters.
-nullsign	Use the hash of the data as a signature.
-oldpfx	Use old PFX encryption.
-out columnlist	Comma-separated column list.
-p password	Password
-pin PIN	Smart card PIN.

Option	Description
-policyserver URLorID	Policy Server URL or ID. For selection U/I, use `-policyserver`. For all Policy Servers, use `-policyserver *`
-privatekey	Display password and private key data.
-protect	Protect keys with password.
-protectto SAMnameandSIDlist	Comma-separated SAM name/SID list.
-restrict restrictionlist	Comma-separated Restriction List. Each restriction consists of a column name, a relational operator, and a constant integer, string, or date. One column name may be preceded by a plus or minus sign to indicate the sort order. For example: `requestID = 47`, `+requestername >= a, requestername`, or `-requestername > DOMAIN, Disposition = 21`.
-reverse	Reverse Log and Queue columns.
-seconds	Display times using seconds and milliseconds.
-service	Use service certificate store.
-sid	Numeric SID: **22** - Local System **23** - Local Service **24** - Network Service
-silent	Use the `silent` flag to acquire crypt context.
-split	Split embedded ASN.1 elements, and save to files.
-sslpolicy servername	SSL Policy matching ServerName.
-symkeyalg symmetrickeyalgorithm[,keylength]	Name of the Symmetric Key Algorithm with optional key length. For example: `AES,128` or `3DES`.
-syncWithWU DestinationDir	Sync with Windows Update.
-t timeout	URL fetch timeout in milliseconds.
-Unicode	Write redirected output in Unicode.
-UnicodeText	Write output file in Unicode.
-urlfetch	Retrieve and verify AIA Certs and CDP CRLs.
-user	Use the HKEY_CURRENT_USER keys or certificate store.
-username username	Use named account for SSL credentials. For selection UI,

Option	Description
	use `-username`.
-ut	Display user templates.
-v	Provide more detailed (verbose) information.
-v1	Use V1 interfaces.

Hash algorithms: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512.

Related links

For more examples of how to use this command, see the following articles:

- Active Directory Certificate Services (AD CS)
- Certutil tasks for managing certificates
- Configure trusted roots and disallowed certificates in Windows

change

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes Remote Desktop Session Host server settings for logons, COM port mappings, and install mode.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
change logon
change port
change user
```

Parameters

Parameter	Description
change logon command	Enables or disables logons from client sessions on an Remote Desktop Session Host server, or displays current logon status.
change port command	Lists or changes the COM port mappings to be compatible with MS-DOS applications.
change user command	Changes the install mode for the Remote Desktop Session Host server.

Related links

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

change logon

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables or disables logons from client sessions, or displays current logon status. This utility is useful for system maintenance. You must be an administrator to run this command.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
change logon {/query | /enable | /disable | /drain | /drainuntilrestart}
```

Parameters

Parameter	Description
/query	Displays the current logon status, whether enabled or disabled.
/enable	Enables logons from client sessions, but not from the console.
/disable	Disables subsequent logons from client sessions, but not from the console. Does not affect currently logged on users.
/drain	Disables logons from new client sessions, but allows reconnections to existing sessions.
/drainuntilrestart	Disables logons from new client sessions until the computer is restarted, but allows reconnections to existing sessions.
/?	Displays help at the command prompt.

Remarks

- Logons are re-enabled when you restart the system.
- If you're connected to the Remote Desktop Session Host server from a client session, and then you disable logons and log off before re-enabling logons, you won't be able to reconnect to your session. To re-enable logons from client sessions, log on at the console.

Examples

- To display the current logon status, type:

```
change logon /query
```

- To enable logons from client sessions, type:

```
change logon /enable
```

- To disable client logons, type:

```
change logon /disable
```

Related links

- Command-Line Syntax Key
- change command
- Remote Desktop Services (Terminal Services) Command Reference

change port

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Lists or changes the COM port mappings to be compatible with MS-DOS applications.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
change port [<portX>=<portY>| /d <portX> | /query]
```

Parameters

Parameter	Description
`<portX>`=`<portY>`	Maps COM `<portX>` to `<portY>`
/d `<portX>`	Deletes the mapping for COM `<portX>`
/query	Displays the current port mappings.
/?	Displays help at the command prompt.

Remarks

- Most MS-DOS applications support only COM1 through COM4 serial ports. The **change port** command maps a serial port to a different port number, allowing apps that don't support high-numbered COM ports to access the serial port. Remapping works only for the current session and is not retained if you log off from a session and then log on again.

- Use **change port** without any parameters to display the available COM ports and their current mappings.

Examples

- To map COM12 to COM1 for use by an MS-DOS-based application, type:

```
change port com12=com1
```

- To display the current port mappings, type:

```
change port /query
```

Related links

- Command-Line Syntax Key
- change command
- Remote Desktop Services (Terminal Services) Command Reference

change user

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the install mode for the Remote Desktop Session Host server.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
change user {/execute | /install | /query}
```

Parameters

Parameter	Description
/execute	Enables .ini file mapping to the home directory. This is the default setting.
/install	Disables .ini file mapping to the home directory. All .ini files are read and written to the system directory. You must disable .ini file mapping when installing applications on a Remote Desktop Session Host server.
/query	Displays the current setting for .ini file mapping.
/?	Displays help at the command prompt.

Remarks

- Use **change user /install** before installing an application to create .ini files for the application in the system directory. These files are used as the source when user-specific .ini files are created. After installing the application, use **change user /execute** to revert to standard .ini file mapping.

- The first time you run the app, it searches the home directory for its .ini files. If the .ini files aren't found in the home directory, but are found in the system directory, Remote Desktop Services copies the .ini files to the home directory, ensuring that each user has a unique copy of the application .ini files. Any new .ini files are created in the home directory.

- Each user should have a unique copy of the .ini files for an application. This prevents instances where different users might have incompatible application configurations (for example, different default directories or screen resolutions).

- When the system is running **change user /install**, several things occur. All registry entries that are created are shadowed under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Terminal Server\Install**, in either the **\SOFTWARE** subkey or the **\MACHINE** subkey. Subkeys added to **HKEY_CURRENT_USER** are copied under the **\SOFTWARE** subkey, and subkeys added to **HKEY_LOCAL_MACHINE** are copied under the **\MACHINE** subkey. If the application queries the Windows directory by using system calls, such as GetWindowsdirectory, the rd Session Host server returns the systemroot directory. If any .ini file entries are added by using system calls, such as WritePrivateProfileString, they are added to the .ini files under the systemroot directory.

- When the system returns to **change user /execute**, and the application tries to read a registry entry under **HKEY_CURRENT_USER** that does not exist, Remote Desktop Services checks to see whether a copy of the key exists under the **\Terminal Server\Install** subkey. If it does, the subkeys are copied to the appropriate location under **HKEY_CURRENT_USER**. If the application tries to read from an .ini file that does not exist, Remote Desktop Services searches for that .ini file under the system root. If the .ini file is in the system root, it is copied to the \Windows subdirectory of the user's home directory. If the application queries the Windows directory, the rd Session Host server returns the \Windows subdirectory of the user's home directory.

- When you log on, Remote Desktop Services checks whether its system .ini files are newer than the .ini files on your computer. If the system version is newer, your .ini file is either replaced or merged with the newer version. This depends on whether or not the INISYNC bit, 0x40, is set for this .ini file. Your previous version of the .ini file is renamed as Inifile.ctx. If the system registry values under the **\Terminal Server\Install** subkey are newer than your version under **HKEY_CURRENT_USER**, your version of the subkeys is deleted and replaced with the new subkeys from **\Terminal Server\Install**.

Examples

- To disable .ini file mapping in the home directory, type:

```
change user /install
```

- To enable .ini file mapping in the home directory, type:

```
change user /execute
```

- To display the current setting for .ini file mapping, type:

```
change user /query
```

Related links

- Command-Line Syntax Key
- change command
- Remote Desktop Services (Terminal Services) Command Reference

chcp

Article • 02/03/2023

Changes the active console code page. If used without parameters, **chcp** displays the number of the active console code page.

Syntax

```
chcp [<nnn>]
```

Parameters

Parameter	Description
`<nnn>`	Specifies the code page.
/?	Displays help at the command prompt.

The following table lists each supported code page and its country/region or language:

Code page	Country/region or language
437	United States
850	Multilingual (Latin I)
852	Slavic (Latin II)
855	Cyrillic (Russian)
857	Turkish
860	Portuguese
861	Icelandic
863	Canadian-French
865	Nordic
866	Russian
869	Modern Greek

Code page	Country/region or language
936	Chinese

Remarks

- Only the original equipment manufacturer (OEM) code page that is installed with Windows appears correctly in a Command Prompt window that uses Raster fonts. Other code pages appear correctly in full-screen mode or in Command Prompt windows that use TrueType fonts.
- You don't need to prepare code pages (as in MS-DOS).
- Programs that you start after you assign a new code page use the new code page. However, programs (except Cmd.exe) that you started before assigning the new code page will continue to use the original code page.

Examples

To view the active code page setting, type:

```
chcp
```

A message similar to the following appears: `Active code page: 437`

To change the active code page to 850 (Multilingual), type:

```
chcp 850
```

If the specified code page is invalid, the following error message appears: `Invalid code page`

Related links

- Command-Line Syntax Key
- Code Page BitFields
- Code Page Identifiers

chdir

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the name of the current directory or changes the current directory. If used with only a drive letter (for example, `chdir C:`), **chdir** displays the names of the current directory in the specified drive. If used without parameters, **chdir** displays the current drive and directory.

> **Note**
>
> This command has been replaced by the **cd command**. For more information, including the syntax and parameter details, see cd command.

Related links

- Command-Line Syntax Key
- cd command

chglogon

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables or disables logons from client sessions on an Remote Desktop Session Host server, or displays current logon status.

> **Note**
>
> This command has been replaced by the **change log command**. For more information, including the syntax and parameter details, see **change logon command**.

Related links

- Command-Line Syntax Key
- change logon command
- Remote Desktop Services (Terminal Services) Command Reference

chgport

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Lists or changes the COM port mappings to be compatible with MS-DOS applications.

> **Note**
>
> This command has been replaced by the **change port command**. For more information, including the syntax and parameter details, see **change port command**.

Related links

- Command-Line Syntax Key
- change port command
- Remote Desktop Services (Terminal Services) Command Reference

chgusr

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the install mode for the Remote Desktop Session Host server.

> **Note**
>
> This command has been replaced by the **change user command**. For more information, including the syntax and parameter details, see **change user command**.

Related links

- Command-Line Syntax Key
- change user command
- Remote Desktop Services (Terminal Services) Command Reference

chkdsk

Article • 02/03/2023

Checks the file system and file system metadata of a volume for logical and physical errors. If used without parameters, **chkdsk** displays only the status of the volume and does not fix any errors. If used with the **/f**, **/r**, **/x**, or **/b** parameters, it fixes errors on the volume.

> **Important**
>
> Membership in the local **Administrators** group, or equivalent, is the minimum required to run **chkdsk**. To open a command prompt window as an administrator, right-click **Command prompt** in the **Start** menu, and then click **Run as administrator**.

> **Important**
>
> Interrupting **chkdsk** is not recommended. However, canceling or interrupting **chkdsk** should not leave the volume any more corrupt than it was before **chkdsk** was run. Running **chkdsk** again checks and should repair any remaining corruption on the volume.

> **Note**
>
> Chkdsk can be used only for local disks. The command cannot be used with a local drive letter that has been redirected over the network.

Syntax

Windows Command Prompt

```
chkdsk [<volume>[[<path>]<filename>]] [/f] [/v] [/r] [/x] [/i] [/c] [/l[:
<size>]] [/b]
```

Parameters

Parameter	Description

Parameter	Description
`<volume>`	Specifies the drive letter (followed by a colon), mount point, or volume name.
[`[<path>]` `<filename>`	Use with file allocation table (FAT) and FAT32 only. Specifies the location and name of a file or set of files that you want **chkdsk** to check for fragmentation. You can use the **?** and * wildcard characters to specify multiple files.
/f	Fixes errors on the disk. The disk must be locked. If **chkdsk** cannot lock the drive, a message appears that asks you if you want to check the drive the next time you restart the computer.
/v	Displays the name of each file in every directory as the disk is checked.
/r	Locates bad sectors and recovers readable information. The disk must be locked. **/r** includes the functionality of **/f**, with the additional analysis of physical disk errors.
/x	Forces the volume to dismount first, if necessary. All open handles to the drive are invalidated. **/x** also includes the functionality of **/f**.
/i	Use with NTFS only. Performs a less vigorous check of index entries, which reduces the amount of time required to run **chkdsk**.
/c	Use with NTFS only. Does not check cycles within the folder structure, which reduces the amount of time required to run **chkdsk**.
/l[:`<size>`]	Use with NTFS only. Changes the log file size to the size you type. If you omit the size parameter, **/l** displays the current size.
/b	Use with NTFS only. Clears the list of bad clusters on the volume and rescans all allocated and free clusters for errors. **/b** includes the functionality of **/r**. Use this parameter after imaging a volume to a new hard disk drive.
/scan	Use with NTFS only. Runs an online scan on the volume.
/forceofflinefix	Use with NTFS only (must be used with **/scan**). Bypass all online repair; all defects found are queued for offline repair (for example, `chkdsk /spotfix`).
/perf	Use with NTFS only (must be used with **/scan**). Uses more system resources to complete a scan as fast as possible. This may have a negative performance impact on other tasks running on the system.
/spotfix	Use with NTFS only. Runs spot fixing on the volume.
/sdcleanup	Use with NTFS only. Garbage collect unneeded security descriptor data (implies **/f**).
/offlinescanandfix	Runs an offline scan and fix on the volume.

Parameter	Description
/freeorphanedchains	Use with FAT/FAT32/exFAT only. Frees any orphaned cluster chains instead of recovering their contents.
/markclean	Use with FAT/FAT32/exFAT only. Marks the volume clean if no corruption was detected, even if **/f** was not specified.
/?	Displays help at the command prompt.

Remarks

- The **/i** or **/c** switch reduces the amount of time required to run **chkdsk** by skipping certain volume checks.
- If you want **chkdsk** to correct disk errors, you can't have open files on the drive. If files are open, the following error message appears:

  ```
  Chkdsk cannot run because the volume is in use by another process.
  Would you like to schedule this volume to be checked the next time the
  system restarts? (Y/N)
  ```

- If you choose to check the drive the next time you restart the computer, **chkdsk** checks the drive and corrects errors automatically when you restart the computer. If the drive partition is a boot partition, **chkdsk** automatically restarts the computer after it checks the drive.
- You can also use the `chkntfs /c` command to schedule the volume to be checked the next time the computer is restarted. Use the `fsutil dirty set` command to set the volume's dirty bit (indicating corruption), so that Windows runs **chkdsk** when the computer is restarted.
- You should use **chkdsk** occasionally on FAT and NTFS file systems to check for disk errors. **Chkdsk** examines disk space and disk use and provides a status report specific to each file system. The status report shows errors found in the file system. If you run **chkdsk** without the **/f** parameter on an active partition, it might report spurious errors because it cannot lock the drive.
- **Chkdsk** corrects logical disk errors only if you specify the **/f** parameter. **Chkdsk** must be able to lock the drive to correct errors.

Because repairs on FAT file systems usually change a disk's file allocation table and sometimes cause a loss of data, **chkdsk** might display a confirmation message similar to the following:

```
10 lost allocation units found in 3 chains.
Convert lost chains to files?
```

  - If you press **Y**, Windows saves each lost chain in the root directory as a file with a name in the format File`<nnnn>`.chk. When **chkdsk** finishes, you can check these files to see if they contain any data you need.
  - If you press **N**, Windows fixes the disk, but it does not save the contents of the lost allocation units.

- If you don't use the **/f** parameter, **chkdsk** displays a message that the file needs to be fixed, but it does not fix any errors.
- If you use `chkdsk /f*` on a very large disk or a disk with a very large number of files (for example, millions of files), `chkdsk /f` might take a long time to complete.
- Use the **/r** parameter to find physical disk errors in the file system and attempt to recover data from any affected disk sectors.
- If you specify the **/f** parameter, **chkdsk** displays an error message if there are open files on the disk. If you do not specify the **/f** parameter and open files exist, **chkdsk** might report lost allocation units on the disk. This could happen if open files have not yet been recorded in the file allocation table. If **chkdsk** reports the loss of a large number of allocation units, consider repairing the disk.
- Because the Shadow Copies for Shared Folders source volume cannot be locked while **Shadow Copies for Shared Folders** is enabled, running **chkdsk** against the source volume might report false errors or cause **chkdsk** to unexpectedly quit. You can, however, check shadow copies for errors by running **chkdsk** in Read-only mode (without parameters) to check the Shadow Copies for Shared Folders storage volume.
- The **chkdsk** command, with different parameters, is available from the Recovery Console.
- On servers that are infrequently restarted, you may want to use the **chkntfs** or the `fsutil dirty query` commands to determine whether the volume's dirty bit is already set before running chkdsk.

Understanding exit codes

The following table lists the exit codes that **chkdsk** reports after it has finished.

Exit code	Description
0	No errors were found.
1	Errors were found and fixed.
2	Performed disk cleanup (such as garbage collection) or did not perform cleanup because **/f** was not specified.
3	Could not check the disk, errors could not be fixed, or errors were not fixed because **/f** was not specified.

Examples

To check the disk in drive D and have Windows fix errors, type:

Windows Command Prompt

```
chkdsk d: /f
```

If it encounters errors, **chkdsk** pauses and displays messages. **Chkdsk** finishes by displaying a report that lists the status of the disk. You cannot open any files on the specified drive until **chkdsk** finishes.

To check all files on a FAT disk in the current directory for noncontiguous blocks, type:

Windows Command Prompt

```
chkdsk *.*
```

Chkdsk displays a status report, and then lists the files that match the file specifications that have noncontiguous blocks.

Viewing chkdsk logs

There are two methods that can be used to retrieve chkdsk log file(s) in Windows. View the methods described below:

Event Viewer

To view logs with Event Viewer, navigate to the following:

1. Start > **Control Panel** > **Administrative Tools** > **Event Viewer**.

   Alternatively, press **Win + R** keys to bring up the run dialog box, type **eventvwr.msc**, and select **OK**.

2. Expand **Windows Logs** > right-click on **Application** > select **Filter Current Log**.

3. Within the **Filter Current Log** window, navigate to **Event sources** drop-down menu, select **Chkdsk** and **Wininit**.

4. Click **OK** to finish filtering for these two sources.

Related links

- Command-Line Syntax Key

chkntfs

Article • 02/03/2023

Displays or modifies automatic disk checking when the computer is started. If used without options, **chkntfs** displays the file system of the specified volume. If automatic file checking is scheduled to run, **chkntfs** displays whether the specified volume is dirty or is scheduled to be checked the next time the computer is started.

> ⓘ Note
>
> To run **chkntfs**, you must be a member of the Administrators group.

Syntax

```
chkntfs <volume> [...]
chkntfs [/d]
chkntfs [/t[:<time>]]
chkntfs [/x <volume> [...]]
chkntfs [/c <volume> [...]]
```

Parameters

Parameter	Description
`<volume>` [...]	Specifies one or more volumes to check when the computer starts. Valid volumes include drive letters (followed by a colon), mount points, or volume names.
/d	Restores all **chkntfs** default settings, except the countdown time for automatic file checking. By default, all volumes are checked when the computer is started, and **chkdsk** runs on those that are dirty.
/t [`:<time>`]	Changes the Autochk.exe initiation countdown time to the amount of time specified in seconds. If you do not enter a time, **/t** displays the current countdown time.
/x `<volume>` [...]	Specifies one or more volumes to exclude from checking when the computer is started, even if the volume is marked as requiring **chkdsk**.
/c `<volume>` [...]	Schedules one or more volumes to be checked when the computer is started, and runs **chkdsk** on those that are dirty.

Parameter	Description
/?	Displays help at the command prompt.

Examples

To display the type of file system for drive C, type:

```
chkntfs c:
```

> **Note**
>
> If automatic file checking is scheduled to run, additional output will display, indicating whether the drive is dirty or has been manually scheduled to be checked the next time the computer is started.

To display the Autochk.exe initiation countdown time, type:

```
chkntfs /t
```

To change the Autochk.exe initiation countdown time to 30 seconds, type:

```
chkntfs /t:30
```

> **Note**
>
> Although you can set the Autochk.exe initiation countdown time to zero, doing so will prevent you from canceling a potentially time-consuming automatic file check.

To exclude multiple volumes from being checked, you must list each of them in a single command. For example, to exclude both the D and E volumes, type:

```
chkntfs /x d: e:
```

> **Important**
>
> The **/x** command-line option isn't accumulative. If you type it more than once, the most recent entry overrides the previous entry.

To schedule automatic file checking on the D volume, but not the C or E volumes, type the following commands in order:

```
chkntfs /d
chkntfs /x c: d: e:
chkntfs /c d:
```

> **Important**
>
> The **/c** command-line option is accumulative. If you type **/c** more than once, each entry remains. To ensure that only a particular volume is checked, reset the defaults to clear all previous commands, exclude all volumes from being checked, and then schedule automatic file checking on the desired volume.

Related links

- Command-Line Syntax Key

choice

Article • 02/03/2023

Prompts the user to select one item from a list of single-character choices in a batch program, and then returns the index of the selected choice. If used without parameters, **choice** displays the default choices **Y** and **N**.

Syntax

```
choice [/c [<choice1><choice2><…>]] [/n] [/cs] [/t <timeout> /d <choice>]
[/m <text>]
```

Parameters

Parameter	Description
/c `<choice1>` `<choice2>` `<…>`	Specifies the list of choices to be created. Valid choices include a-z, A-Z, 0-9, and extended ASCII characters (128-254). The default list is YN, which is displayed as `[Y,N]?`.
/n	Hides the list of choices, although the choices are still enabled and the message text (if specified by **/m**) is still displayed.
/cs	Specifies that the choices are case-sensitive. By default, the choices are not case-sensitive.
/t `<timeout>`	Specifies the number of seconds to pause before using the default choice specified by **/d**. Acceptable values are from **0** to **9999**. If **/t** is set to **0**, **choice** does not pause before returning the default choice.
/d `<choice>`	Specifies the default choice to use after waiting the number of seconds specified by **/t**. The default choice must be in the list of choices specified by **/c**.
/m `<text>`	Specifies a message to display before the list of choices. If **/m** is not specified, only the choice prompt is displayed.
/?	Displays help at the command prompt.

Remarks

- The **ERRORLEVEL** environment variable is set to the index of the key that the user selects from the list of choices. The first choice in the list returns a value of `1`, the second a value of `2`, and so on. If the user presses a key that is not a valid choice, **choice** sounds a warning beep.
- If **choice** detects an error condition, it returns an **ERRORLEVEL** value of `255`. If the user presses CTRL+BREAK or CTRL+C, **choice** returns an **ERRORLEVEL** value of `0`.

> ⓘ Note
>
> When you use **ERRORLEVEL** values in a batch program, you must list them in decreasing order.

Examples

To present the choices **Y**, **N**, and **C**, type the following line in a batch file:

```
choice /c ync
```

The following prompt appears when the batch file runs the **choice** command:

```
[Y,N,C]?
```

To hide the choices **Y**, **N**, and **C**, but display the text **Yes**, **No**, or **Continue**, type the following line in a batch file:

```
choice /c ync /n /m "Yes, No, or Continue?"
```

> ⓘ Note
>
> If you use the **/n** parameter, but do not use **/m**, the user is not prompted when **choice** is waiting for input.

To show both the text and the options used in the previous examples, type the following line in a batch file:

```
choice /c ync /m "Yes, No, or Continue"
```

To set a time limit of five seconds and specify **N** as the default value, type the following line in a batch file:

```
choice /c ync /t 5 /d n
```

> **Note**
>
> In this example, if the user doesn't press a key within five seconds, **choice** selects **N** by default and returns an error value of `2`. Otherwise, **choice** returns the value corresponding to the user's choice.

Related links

- Command-Line Syntax Key

cipher

Article • 02/03/2023

Displays or alters the encryption of directories and files on NTFS volumes. If used without parameters, **cipher** displays the encryption state of the current directory and any files it contains.

Syntax

```
cipher [/e | /d | /c] [/s:<directory>] [/b] [/h] [pathname [...]]
cipher /k
cipher /r:<filename> [/smartcard]
cipher /u [/n]
cipher /w:<directory>
cipher /x[:efsfile] [filename]
cipher /y
cipher /adduser [/certhash:<hash> | /certfile:<filename>] [/s:directory]
[/b] [/h] [pathname [...]]
cipher /removeuser /certhash:<hash> [/s:<directory>] [/b] [/h] [<pathname>
[...]]
cipher /rekey [pathname [...]]
```

Parameters

Parameters	Description
/b	Aborts if an error is encountered. By default, **cipher** continues to run even if errors are encountered.
/c	Displays information on the encrypted file.
/d	Decrypts the specified files or directories.
/e	Encrypts the specified files or directories. Directories are marked so that files that are added afterward will be encrypted.
/h	Displays files with hidden or system attributes. By default, these files are not encrypted or decrypted.
/k	Creates a new certificate and key for use with Encrypting File System (EFS) files. If the **/k** parameter is specified, all other parameters are ignored.

Parameters	Description
/r:`<filename>` [/smartcard]	Generates an EFS recovery agent key and certificate, then writes them to a .pfx file (containing certificate and private key) and a .cer file (containing only the certificate). If **/smartcard** is specified, it writes the recovery key and certificate to a smart card, and no .pfx file is generated.
/s:`<directory>`	Performs the specified operation on all subdirectories in the specified *directory*.
/u [/n]	Finds all encrypted files on the local drive(s). If used with the **/n** parameter, no updates are made. If used without **/n**, **/u** compares the user's file encryption key or the recovery agent's key to the current ones, and updates them if they have changed. This parameter works only with **/n**.
/w:`<directory>`	Removes data from available unused disk space on the entire volume. If you use the **/w** parameter, all other parameters are ignored. The directory specified can be located anywhere in a local volume. If it is a mount point or points to a directory in another volume, the data on that volume is removed.
/x[:efsfile] [`<FileName>`]	Backs up the EFS certificate and keys to the specified file name. If used with **:efsfile**, **/x** backs up the user's certificate(s) that were used to encrypt the file. Otherwise, the user's current EFS certificate and keys are backed up.
/y	Displays your current EFS certificate thumbnail on the local computer.
/adduser [/certhash:`<hash>`	/certfile:`<filename>`]
/rekey	Updates the specified encrypted file(s) to use the currently configured EFS key.
/removeuser /certhash:`<hash>`	Removes a user from the specified file(s). The *Hash* provided for **/certhash** must be the SHA1 hash of the certificate to remove.
/?	Displays help at the command prompt.

Remarks

- If the parent directory is not encrypted, an encrypted file could become decrypted when it is modified. Therefore, when you encrypt a file, you should also encrypt the parent directory.
- An administrator can add the contents of a .cer file to the EFS recovery policy to create the recovery agent for users, and then import the .pfx file to recover individual files.
- You can use multiple directory names and wildcards.

- You must put spaces between multiple parameters.

Examples

To display the encryption status of each of the files and subdirectories in the current directory, type:

```
cipher
```

Encrypted files and directories are marked with an **E**. Unencrypted files and directories are marked with a **U**. For example, the following output indicates that the current directory and all its contents are currently unencrypted:

```
Listing C:\Users\MainUser\Documents\
New files added to this directory will not be encrypted.
U Private
U hello.doc
U hello.txt
```

To enable encryption on the Private directory used in the previous example, type:

```
cipher /e private
```

The following output displays:

```
Encrypting files in C:\Users\MainUser\Documents\
Private             [OK]
1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.
```

The **cipher** command displays the following output:

```
Listing C:\Users\MainUser\Documents\
New files added to this directory will not be encrypted.
E Private
```

```
U hello.doc
U hello.txt
```

Where the **Private** directory is now marked as encrypted.

Related links

- Command-Line Syntax Key

cleanmgr

Article • 01/18/2024

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008 R2, Windows 11, Windows 10

Clears unnecessary files from your computer's hard disk. You can use command-line options to specify that **Cleanmgr** cleans up Temp files, Internet files, downloaded files, and Recycle Bin files. You can then schedule the task to run at a specific time by using the **Scheduled Tasks** tool.

Syntax

```
cleanmgr [/d <driveletter>] [/sageset:n]  [/sagerun:n] [/TUNEUP:n]
[/LOWDISK] [/VERYLOWDISK]
```

Parameters

Expand table

Parameter	Description
/d `<driveletter>`	Specifies the drive that you want Disk Cleanup to clean. **NOTE:** The **/d** option isn't utilized with `/sagerun:n`.
/sageset:n	Displays the **Disk Cleanup Settings** dialog box and also creates a registry key to store the settings that you select. The `n` value, which is stored in the registry, allows you to specify tasks for Disk Cleanup to run. The `n` value can be any integer value from 0 to 9999. For more information, see Registry key information.
/sagerun:n	Runs the specified tasks that are assigned to the n value if you use the **/sageset** option. All drives on the computer are enumerated and the selected profile runs against each drive.
/tuneup:n	Run **/sageset** and **/sagerun** for the same `n`.
/lowdisk	Run with the default settings.
/verylowdisk	Run with the default settings, no user prompts.

Parameter	Description
/autoclean	Automatically deletes the files that are left behind after you upgrade Windows.
/?	Displays help at the command prompt.

Options

The options for the files that you can specify for Disk Cleanup by using **/sageset** and **/sagerun** include:

- **Temporary Setup Files** - These are files that were created by a Setup program that is no longer running.
- **Downloaded Program Files** - Downloaded program files are ActiveX controls and Java programs that are downloaded automatically from the Internet when you view certain pages. These files are temporarily stored in the Downloaded Program Files folder on the hard disk. This option includes a View Files button so that you can see the files before Disk Cleanup removes them. The button opens the C:\Winnt\Downloaded Program Files folder.
- **Temporary Internet Files** - The Temporary Internet Files folder contains Web pages that are stored on your hard disk for quick viewing. Disk Cleanup removes these pages but leaves your personalized settings for Web pages intact. This option also includes a View Files button, which opens the C:\Documents and Settings\Username\Local Settings\Temporary Internet Files\Content.IE5 folder.
- **Old Chkdsk Files** - When Chkdsk checks a disk for errors, Chkdsk might save lost file fragments as files in the root folder on the disk. These files are unnecessary.
- **Recycle Bin** - The Recycle Bin contains files that you have deleted from the computer. These files aren't permanently removed until you empty the Recycle Bin. This option includes a View Files button that opens the Recycle Bin.

  Note: A Recycle Bin may appear in more than one drive, for example, not just in %SystemRoot%.
- **Temporary Files** - Programs sometimes store temporary information in a Temp folder. Before a program quits, the program usually deletes this information. You can safely delete temporary files that haven't been modified within the last week.
- **Temporary Offline Files** - Temporary offline files are local copies of recently used network files. These files are automatically cached so that you can use them after

you disconnect from the network. A **View Files** button opens the Offline Files folder.

- **Offline Files** - Offline files are local copies of network files that you specifically want to have available offline so that you can use them after you disconnect from the network. A **View Files** button opens the Offline Files folder.

- **Compress Old Files** - Windows can compress files that you haven't used recently. Compressing files saves disk space, but you can still use the files. No files are deleted. Because files are compressed at different rates, the displayed amount of disk space that you'll gain is approximate. An Options button permits you to specify the number of days to wait before Disk Cleanup compresses an unused file.

- **Catalog Files for the Content Indexer** - The Indexing service speeds up and improves file searches by maintaining an index of the files that are on the disk. These Catalog files remain from a previous indexing operation and can be deleted safely.

  Note: Catalog File may appear in more than one drive, for example, not just in `%SystemRoot%`.

> ⓘ Note
>
> If you specify cleaning up the drive that contains the Windows installation, all of these options are available on the **Disk Cleanup** tab. If you specify any other drive, only the Recycle Bin and the Catalog files for content index options are available on the **Disk Cleanup** tab.

Examples

To run the Disk Cleanup app so that you can use its dialog box to specify options for use later, saving the settings to the set **1**, type the following:

```
cleanmgr /sageset:1
```

To run Disk Cleanup and include the options that you specified with the cleanmgr /sageset:1 command, type:

```
```

```
cleanmgr /sagerun:1
```

To run `cleanmgr /sageset:1` and `cleanmgr /sagerun:1` together, type:

```
cleanmgr /tuneup:1
```

Related links

- Free up drive space in Windows 10
- Command-Line Syntax Key

clip

Article • 02/03/2023

Redirects the command output from the command line to the Windows clipboard. You can use this command to copy data directly into any application that can receive text from the Clipboard. You can also paste this text output into other programs.

Syntax

```
<command> | clip
clip < <filename>
```

Parameters

Parameter	Description
`<command>`	Specifies a command whose output you want to send to the Windows clipboard.
`<filename>`	Specifies a file whose contents you want to send to the Windows clipboard.
/?	Displays help at the command prompt.

Examples

To copy the current directory listing to the Windows clipboard, type:

```
dir | clip
```

To copy the output of a program called *generic.awk* to the Windows clipboard, type:

```
awk -f generic.awk input.txt | clip
```

To copy the contents of a file called *readme.txt* to the Windows clipboard, type:

```
clip < readme.txt
```

Related links

- Command-Line Syntax Key

cls

Article • 02/03/2023

Clears the Command Prompt window.

Syntax

```
cls
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.

Examples

To clear all information that appears in the Command Prompt window and return to a blank window, type:

```
cls
```

Related links

- Command-Line Syntax Key

cmd

Article • 09/12/2023

Starts a new instance of the command interpreter, Cmd.exe. If used without parameters, **cmd** displays the version and copyright information of the operating system.

Syntax

```
cmd [/c|/k] [/s] [/q] [/d] [/a|/u] [/t:{<b><f> | <f>}] [/e:{on | off}] [/f:
{on | off}] [/v:{on | off}] [<string>]
```

Parameters

Parameter	Description
/c	Carries out the command specified by `<string>` and then exits the command processor.
/k	Carries out the command specified by `<string>` and keeps the command processor running.
/s	When used with `/c` or `/k`, triggers special non-parsing rules that strip the first and last quotes (`"`) around the `<string>` but leaves the rest of the command unchanged.
/q	Turns echo off.
/d	Disables execution of AutoRun commands.
/a	Formats command output as American National Standards Institute (ANSI).
/u	Formats command output as Unicode.
/t:{`<b><f>` | `<f>`}	Sets the background (*b*) and foreground (*f*) colors.
/e:on	Enables command extensions.
/e:off	Disables commands extensions.
/f:on	Enables file and directory name completion.
/f:off	Disables file and directory name completion.

Parameter	Description
/v:on	Enables delayed environment variable expansion.
/v:off	Disables delayed environment variable expansion.
`<string>`	Specifies the command you want to carry out.
/?	Displays help at the command prompt.

The following table lists valid hexadecimal digits that you can use as the values for `<b>` and `<f>`:

Value	Color
0	Black
1	Blue
2	Green
3	Aqua
4	Red
5	Purple
6	Yellow
7	White
8	Gray
9	Light blue
a	Light green
b	Light aqua
c	Light red
d	Light purple
e	Light yellow
f	Bright white

Remarks

- To redirect command output to the input of another command, use the pipe (`|`) character. For example:

```
<command1> | <command2>
```

- To redirect command output to a file, use the greater-than angle bracket `>` character. For example:

```
<command1> > <file1.txt>
```

- To use multiple commands for `<string>`, separate them by the command separator `&&`. For example:

```
<command1>&&<command2>&&<command3>
```

- If the directory path, files, or any information you supply contains spaces, you must use double quotation marks (`"`) around the text, such as `"Computer Name"`. For example:

```
mkdir Test&&mkdir "Test 2"&&move "Test 2" Test
```

- You must use quotation marks around the following special characters: & < > [ ] | { } ^ = ; ! ' + , ` ~ [white space].

- If you specify `/c` or `/k`, the `cmd` processes, the remainder of `<string>`, and the quotation marks are preserved only if all of the following conditions are met:
  - You don't also use `/s`.
  - You use exactly one set of quotation marks.
  - You don't use any special characters within the quotation marks (for example: & < > ( ) @ ^ |).
  - You use one or more white-space characters within the quotation marks.
  - The `<string>` within quotation marks is the name of an executable file.

If the previous conditions aren't met, `<string>` is processed by examining the first character to verify whether it's an opening quotation mark. If the first character is an opening quotation mark, it's stripped along with the closing quotation mark. Any text following the closing quotation marks is preserved.

- If you don't specify `/d`, Cmd.exe looks for the following registry subkeys:

  - **HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun\REG_SZ**
  - **HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun\REG_EXPAND_SZ**

  If one or both registry subkeys are present, they're executed before all other variables.

  > ⊗ **Caution**
  >
  > Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

- You can disable command extensions for a particular process by using `/e:off`. You can enable or disable extensions for all `cmd` command-line options on a computer or user session by setting the following **REG_DWORD** values:

  - **HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions\REG_DWORD**
  - **HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions\REG_DWORD**

  Set the **REG_DWORD** value to either **0×1** (enabled) or **0×0** (disabled) in the registry by using Regedit.exe. User-specified settings take precedence over computer settings, and command-line options take precedence over registry settings.

  > ⊗ **Caution**
  >
  > Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

- When you enable command extensions, the following commands are affected:
  - `assoc`
  - `call`
  - `chdir` (`cd`)
  - `color`
  - `del` (`erase`)
  - `endlocal`
  - `for`
  - `ftype`
  - `goto`
  - `if`
  - `mkdir` (`md`)
  - `popd`
  - `prompt`
  - `pushd`
  - `set`
  - `setlocal`
  - `shift`
  - `start` (also includes changes to external command processes)
- If you enable delayed environment variable expansion, you can use the exclamation point character (`!`) to substitute the value of an environment variable at run time.
- File and directory name completion isn't enabled by default. You can enable or disable file name completion for a particular process of the `cmd` command with `/f:{on | off}`.
- You can enable or disable file and directory name completion for all processes of the `cmd` command on a computer or for a user logon session by setting the following **REG_DWORD** values:
  - **HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar\REG_DWORD**
  - **HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar\REG_DWORD**
  - **HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar\REG_DWORD**

- **HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar\REG_DWORD**

  To set the **REG_DWORD** value, run Regedit.exe and use the hexadecimal value of a control character for a particular function (for example, **0×9** is TAB and **0×08** is BACKSPACE). Use the [**0×20**] value for white space, because it isn't a valid control character. User-specified settings take precedence over computer settings, and command-line options take precedence over registry settings.

  > **⊗ Caution**
  >
  > Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

- If you enable file and directory name completion by using `/f:on`, use **CTRL+D** for directory name completion and **CTRL+F** for file name completion. The only difference between the key combinations **CTRL+D** and **CTRL+F** is that **CTRL+D** only matches directory names and **CTRL+F** matches both file and directory names. If you use file and directory name completion on the built-in directory commands `cd`, `md`, or `rd`, directory completion is assumed.

- Pressing **CTRL+D** or **CTRL+F** processes the file and directory name completion. These key combination functions append a wildcard character to `<string>` if one isn't present, build a list of paths that match, and then display the first matching path. If none of the paths match, the file and directory name completion function beeps and doesn't change the display.
  - To move through the list of matching paths, press **CTRL+D** or **CTRL+F** repeatedly.
  - To move through the list backwards, press the **SHIFT** key and **CTRL+D** or **CTRL+F** simultaneously.
  - To discard the saved list of matching paths and generate a new list, edit `<string>` and press **CTRL+D** or **CTRL+F**.
  - If you switch between **CTRL+D** and **CTRL+F**, the saved list of matching paths is discarded, and a new list is generated.

- File and directory name completion correctly processes file names that contain white space or special characters if you place quotation marks around the matching path.

- If you process file and directory name completion from within `<string>`, at the point in `<string>` where the completion was processed, any part of the *path* to the right of the cursor is discarded.

Related links

- Command-Line Syntax Key

cmdkey

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates, lists, and deletes stored user names and passwords or credentials.

Syntax

```
cmdkey [{/add:<targetname>|/generic:<targetname>}] {/smartcard | /user:
<username> [/pass:<password>]} [/delete{:<targetname> | /ras}] /list:
<targetname>
```

Parameters

Parameters	Description
/add:`<targetname>`	Adds a user name and password to the list. Requires the parameter of `<targetname>` which identifies the computer or domain name that this entry will be associated with.
/generic:`<targetname>`	Adds generic credentials to the list. Requires the parameter of `<targetname>` which identifies the computer or domain name that this entry will be associated with.
/smartcard	Retrieves the credential from a smart card. If more than one smart card is found on the system when this option is used, **cmdkey** displays information about all available smart cards, and then prompts the user to specify which one to use.
/user:`<username>`	Specifies the user or account name to store with this entry. If `<username>` isn't supplied, it will be requested.
/pass:`<password>`	Specifies the password to store with this entry. If `<password>` isn't supplied, it will be requested. Passwords are not displayed after they're stored.
/delete:`{<targetname> | /ras}`	Deletes a user name and password from the list. If `<targetname>` is specified, that entry is deleted. If `/ras` is specified, the stored remote access entry is deleted.

Parameters	Description
/list:`<targetname>`	Displays the list of stored user names and credentials. If `<targetname>` isn't specified, all stored user names and credentials are listed.
/?	Displays help at the command prompt.

Examples

To display a list of all user names and credentials that are stored, type:

```
cmdkey /list
```

To add a user name and password for user *Mikedan* to access computer *Server01* with the password *Kleo*, type:

```
cmdkey /add:server01 /user:mikedan /pass:Kleo
```

To add a user name and password for user *Mikedan* to access computer *Server01* and prompt for the password whenever Server01 is accessed, type:

```
cmdkey /add:server01 /user:mikedan
```

To delete a credential stored by remote access, type:

```
cmdkey /delete /ras
```

To delete a credential stored for *Server01*, type:

```
cmdkey /delete:server01
```

Related links

- Command-Line Syntax Key

cmstp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Installs or removes a Connection Manager service profile. Used without optional parameters, **cmstp** installs a service profile with default settings appropriate to the operating system and to the user's permissions.

Syntax

Syntax 1 - This is the typical syntax used in a custom installation application. To use this syntax, you must run **cmstp** from the directory that contains the `<serviceprofilefilename>.exe` file.

```
<serviceprofilefilename>.exe /q:a /c:cmstp.exe <serviceprofilefilename>.inf
[/nf] [/s] [/u]
```

Syntax 2

```
cmstp.exe [/nf] [/s] [/u] [drive:][path]serviceprofilefilename.inf
```

Parameters

Parameter	Description
`<serviceprofilefilename>.exe`	Specifies, by name, the installation package that contains the profile that you want to install. Required for Syntax 1, but not valid for Syntax 2.
/q:a	Specifies that the profile should be installed without prompting the user. The verification message that the installation has succeeded will still appear. Required for Syntax 1, but not valid for Syntax 2.

Parameter	Description
[drive:][path] `<serviceprofilefilename>.inf`	Required. Specifies, by name, the configuration file that determines how the profile should be installed. The [drive:][path] parameter isn't valid for Syntax 1.
/nf	Specifies that the support files should not be installed.
/s	Specifies that the service profile should be installed or uninstalled silently (without prompting for user response or displaying verification message). This is the only parameter that you can use in combination with **/u**.
/u	Specifies that the service profile should be uninstalled.
/?	Displays help at the command prompt.

Examples

To install the *fiction* service profile without any support files, type:

```
fiction.exe /c:cmstp.exe fiction.inf /nf
```

To silently install the *fiction* service profile for a single user, type:

```
fiction.exe /c:cmstp.exe fiction.inf /s /su
```

To silently uninstall the *fiction* service profile, type:

```
fiction.exe /c:cmstp.exe fiction.inf /s /u
```

Related links

- Command-Line Syntax Key

color

Article • 09/20/2023

Changes the foreground and background colors in the Command Prompt window for the current session. If used without parameters, **color** restores the default Command Prompt window foreground and background colors.

Syntax

Windows Command Prompt

```
color [attr]
```

Parameters

Parameter	Description
`attr`	Specifies color attribute of console output.
/?	Displays help at the command prompt.

The following table lists valid hexadecimal digits that you can use as the values for `attr`:

Value	Color
0	Black
1	Blue
2	Green
3	Aqua
4	Red
5	Purple
6	Yellow
7	White
8	Gray
9	Light blue

Value	Color
a	Light green
b	Light aqua
c	Light red
d	Light purple
e	Light yellow
f	Bright white

Remarks

- You can specify one or two hexadecimal digits. The first is used as the foreground color and the second is used as the background color. If you specify two hexadecimal digits, don't use space characters between them.
- If you specify only one hexadecimal digit, the corresponding color is used as the foreground color and the background color is set to the default color.
- To set the default Command Prompt window color, select the upper-left corner of the **Command Prompt** window, select **Defaults**, select the **Colors** tab, and then select the colors that you want to use for the **Screen Text** and **Screen Background**.
- If you specify the same value for two hexadecimal digits, the ERRORLEVEL is set to `1` and no change is made to either the foreground or the background color.

Examples

To change the Command Prompt window background color to gray and the foreground color to red, type:

Windows Command Prompt

```
color 84
```

To change the Command Prompt window foreground color to light yellow, type:

Windows Command Prompt

```
color e
```

> **Note**
>
> In this example, the background is set to the default color because only one hexadecimal digit is specified.

Related links

- Command-Line Syntax Key

comp

Article • 02/03/2023

Compares the contents of two files or sets of files byte-by-byte. These files can be stored on the same drive or on different drives, and in the same directory or in different directories. When this command compares files, it displays their location and file names. If used without parameters, **comp** prompts you to enter the files to compare.

Syntax

```
comp [<data1>] [<data2>] [/d] [/a] [/l] [/n=<number>] [/c]
```

Parameters

Parameter	Description
`<data1>`	Specifies the location and name of the first file or set of files that you want to compare. You can use wildcard characters (* and ?) to specify multiple files.
`<data2>`	Specifies the location and name of the second file or set of files that you want to compare. You can use wildcard characters (* and ?) to specify multiple files.
/d	Displays differences in decimal format. (The default format is hexadecimal.)
/a	Displays differences as characters.
/l	Displays the number of the line where a difference occurs, instead of displaying the byte offset.
/n=`<number>`	Compares only the number of lines that are specified for each file, even if the files are different sizes.
/c	Performs a comparison that is not case-sensitive.
/off[line]	Processes files with the offline attribute set.
/?	Displays Help at the command prompt.

Remarks

- During the comparison, **comp** displays messages that identify the locations of unequal information between the files. Each message indicates the offset memory address of the unequal bytes and the contents of the bytes (in hexadecimal notation unless the **/a** or **/d** command-line parameter is specified). Messages appear in the following format:

  ```
  Compare error at OFFSET xxxxxxxx
  file1 = xx
  file2 = xx
  ```

  After ten unequal comparisons, **comp** stops comparing the files and displays the following message:

  `10 Mismatches - ending compare`

- If you omit necessary components of either *data1* or *data2*, or if you omit *data2* entirely, this command prompts you for the missing information.

- If *data1* contains only a drive letter or a directory name with no file name, this command compares all of the files in the specified directory to the file specified in *data1*.

- If *data2* contains only a drive letter or a directory name, the default file name for *data2* becomes the same name as for *data1*.

- If the **comp** command can't find the specified files, it will prompt you with a message about whether you want to compare additional files.

- The files that you compare can have the same file name, provided they're in different directories or on different drives. You can use wildcard characters (***** and **?**) to specify file names.

- You must specify **/n** to compare files of different sizes. If the file sizes are different and **/n** isn't specified, the following message is displayed:

  ```
  Files are different sizes
  Compare more files (Y/N)?
  ```

  To compare these files anyway, press **N** to stop the command. Then, run the **comp** command again, using the **/n** option to compare only the first portion of each file.

- If you use wildcard characters (* and ?) to specify multiple files, **comp** finds the first file that matches *data1* and compares it with the corresponding file in *data2*, if it exists. The **comp** command reports the results of the comparison for each file matching *data1*. When finished, **comp** displays the following message:

  `Compare more files (Y/N)?`

  To compare more files, press **Y**. The **comp** command prompts you for the locations and names of the new files. To stop the comparisons, press **N**. When you press **Y**, you're prompted for which command-line options to use. If you don't specify any command-line options, **comp** uses the ones you specified before.

Examples

To compare the contents of the directory *c:\reports* with the backup directory `\\sales\backup\april`, type:

```
comp c:\reports \\sales\backup\april
```

To compare the first ten lines of the text files in the *\invoice* directory and display the result in decimal format, type:

```
comp \invoice\*.txt \invoice\backup\*.txt /n=10 /d
```

Related links

- Command-Line Syntax Key

compact

Article • 02/03/2023

Displays or alters the compression of files or directories on NTFS partitions. If used without parameters, **compact** displays the compression state of the current directory and any files it contains.

Syntax

```
compact [/C | /U] [/S[:dir]] [/A] [/I] [/F] [/Q] [/EXE[:algorithm]]
[/CompactOs[:option] [/windir:dir]] [filename [...]]
```

Parameters

Parameter	Description
/c	Compresses the specified directory or file. Directories are marked so any files added afterwards are compressed, unless the /EXE parameter is specified.
/u	Uncompresses the specified directory or file. Directories are marked so any files added afterwards aren't compressed. If the /EXE parameter is specified, only files compressed as executables are uncompressed; if you don't specify the /EXE parameter, only NTFS compressed files are uncompressed.
/s`[:<dir>]`	Performs the chosen operation on files in the specified directory and all subdirectories. By default, the current directory is used as the `<dir>` value.
/a	Displays hidden or system files. By default, these files aren't included.
/i	Continues performing the specified operation, ignoring errors. By default, this command stops when an error is encountered.
/f	Forces compression or uncompression of the specified directory or file. Already-compressed files are skipped by default. The **/f** parameter is used in the case of a file that was partly compressed when the operation was interrupted by a system crash. To force the file to be compressed in its entirety, use the **/c** and **/f** parameters and specify the partially compressed file.
/q	Reports only the most essential information.

Parameter	Description
/EXE	Uses compression optimized for executable files that are read frequently, but not modified. Supported algorithms are: • **XPRESS4K** (fastest and default value) • **XPRESS8K** • **XPRESS16K** • **LZX** (most compact)
/CompactOs	Sets or queries the system's compression state. Supported options are: • **query** - Queries the system's **Compact** state. • **always** - Compresses all operating system binaries and sets the system state to Compact, which remains unless administrator changes it. • **never** - Uncompresses all operating system binaries and sets the system state to non-Compact, which remains unless administrator changes it.
/windir	Used with the **/CompactOs:query** parameter, when querying the offline operating system. Specifies the directory where Windows is installed.
`<filename>`	Specifies a pattern, file, or directory. You can use multiple file names, and the * and **?** wildcard characters.
/?	Displays help at the command prompt.

Remarks

- This command is the command-line version of the NTFS file system compression feature. The compression state of a directory indicates whether files are automatically compressed when they are added to the directory. Setting the compression state of a directory does not necessarily change the compression state of files that are already in the directory.
- You can't use this command to read, write, or mount volumes compressed using DriveSpace or DoubleSpace. You also can't use this command to compress file allocation table (FAT) or FAT32 partitions.

Examples

To set the compression state of the current directory, its subdirectories, and existing files, type:

```
compact /c /s
```

To set the compression state of files and subdirectories within the current directory, without altering the compression state of the current directory itself, type:

```
compact /c /s *.*
```

To compress a volume, from the root directory of the volume, type:

```
compact /c /i /s:\
```

> **Note**
>
> This example sets the compression state of all directories (including the root directory on the volume) and compresses every file on the volume. The **/i** parameter prevents error messages from interrupting the compression process.

To compress all files with the .bmp file name extension in the \tmp directory and all subdirectories of \tmp, without modifying the compressed attribute of the directories, type:

```
compact /c /s:\tmp *.bmp
```

To force complete compression of the file *zebra.bmp*, which was partially compressed during a system crash, type:

```
compact /c /f zebra.bmp
```

To remove the compressed attribute from the directory c:\tmp, without changing the compression state of any files in that directory, type:

```
compact /u c:\tmp
```

Related links

- Command-Line Syntax Key

copy

Article • 02/03/2023

Copies one or more files from one location to another.

> **Note**
>
> You can also use the **copy** command, with different parameters, from the Recovery Console. For more information about the recovery console, see **Windows Recovery Environment (Windows RE)**.

Syntax

```
copy [/d] [/v] [/n] [/y | /-y] [/z] [/a | /b] <source> [/a | /b] [+<source> [/a | /b] [+ ...]] [<destination> [/a | /b]]
```

Parameters

Parameter	Description
/d	Allows the encrypted files being copied to be saved as decrypted files at the destination.
/v	Verifies that new files are written correctly.
/n	Uses a short file name, if available, when copying a file with a name longer than eight characters, or with a file name extension longer than three characters.
/y	Suppresses prompting to confirm that you want to overwrite an existing destination file.
/-y	Prompts you to confirm that you want to overwrite an existing destination file.
/z	Copies networked files in restartable mode.
/a	Indicates an ASCII text file.
/b	Indicates a binary file.

Parameter	Description
`<source>`	Required. Specifies the location from which you want to copy a file or set of files. *Source* can consist of a drive letter and colon, a directory name, a file name, or a combination of these.
`<destination>`	Required. Specifies the location to which you want to copy a file or set of files. *Destination* can consist of a drive letter and colon, a directory name, a file name, or a combination of these.
/?	Displays help at the command prompt.

Remarks

- You can copy an ASCII text file that uses an end-of-file character (CTRL+Z) to indicate the end of the file.
- If **/a** precedes or follows a list of files on the command line, it applies to all files listed until **copy** encounters **/b**. In this case, **/b** applies to the file preceding **/b**.

  The effect of **/a** depends on its position in the command-line string: - If **/a** follows *source*, the **copy** command treats the file as an ASCII file and copies data that precedes the first end-of-file character (CTRL+Z). - If **/a** follows *destination*, the **copy** command adds an end-of-file character (CTRL+Z) as the last character of the file.
- If **/b** directs the command interpreter to read the number of bytes specified by the file size in the directory. **/b** is the default value for **copy**, unless **copy** combines files.
- If **/b** precedes or follows a list of files on the command line, it applies to all listed files until **copy** encounters **/a**. In this case, **/a** applies to the file preceding **/a**.

  The effect of **/b** depends on its position in the command–line string: - If **/b** follows *source*, the **copy** command copies the entire file, including any end-of-file character (CTRL+Z). - If **/b** follows *destination*, the **copy** command doesn't add an end-of-file character (CTRL+Z).
- If a write operation cannot be verified, an error message appears. Although recording errors rarely occur with the **copy** command , you can use **/v** to verify that critical data has been correctly recorded. The **/v** command-line option also slows down the **copy** command, because each sector recorded on the disk must be checked.

- If **/y** is preset in the **COPYCMD** environment variable, you can override this setting by using **/-y** at the command line. By default, you are prompted when you replace this setting, unless the **copy** command is executed in a batch script.
- To append files, specify a single file for *destination*, but multiple files for *source* (use wildcard characters or *file1*+*file2*+*file3* format).
- If the connection is lost during the copy phase (for example, if the server going offline breaks the connection), you can use **copy /z** to resume after the connection is re-established. The **/z** option also displays the percentage of the copy operation that is completed for each file.
- You can substitute a device name for one or more occurrences of *source* or *destination*.
- If *destination* is a device (for example, Com1 or Lpt1), the **/b** option copies data to the device in binary mode. In binary mode, **copy /b** copies all characters (including special characters such as CTRL+C, CTRL+S, CTRL+Z, and ENTER) to the device, as data. However, if you omit **/b**, the data is copied to the device in ASCII mode. In ASCII mode, special characters might cause files to combine during the copying process.
- If you don't specify a destination file, a copy is created with the same name, modified date, and modified time as the original file. The new copy is stored in the current directory on the current drive. If the source file is on the current drive and in the current directory and you do not specify a different drive or directory for the destination file, the **copy** command stops and displays the following error message:

  ```
  File cannot be copied onto itself
  0 File(s) copied
  ```

- If you specify more than one file in *source*, the **copy** command combines them all into a single file using the file name specified in *destination*. The **copy** command assumes the combined files are ASCII files unless you use the **/b** option.
- To copy files that are 0 bytes long, or to copy all of a directory's files and subdirectories, use the xcopy command.
- To assign the current time and date to a file without modifying the file, use the following syntax:

  ```
  ```

```
copy /b <source> +,,
```

Where the commas indicate that the *destination* parameter has been intentionally left out.

Examples

To copy a file called *memo.doc* to *letter.doc* in the current drive and ensure that an end-of-file character (CTRL+Z) is at the end of the copied file, type:

```
copy memo.doc letter.doc /a
```

To copy a file named *robin.typ* from the current drive and directory to an existing directory named *Birds* that is located on drive C, type:

```
copy robin.typ c:\birds
```

> ⓘ **Note**
>
> If the *Birds* directory doesn't exist, the file *robin.typ* is copied into a file named *Birds* that is located in the root directory on the disk in drive C.

To combine *Mar89.rpt*, *Apr89.rpt*, and *May89.rpt*, which are located in the current directory, and place them in a file named *Report* (also in the current directory), type:

```
copy mar89.rpt + apr89.rpt + may89.rpt Report
```

> ⓘ **Note**
>
> If you combine files, the **copy** command marks the destination file with the current date and time. If you omit *destination*, the files are combined and stored under the name of the first file in the list.

To combine all files in *Report*, when a file named *Report* already exists, type:

```
copy report + mar89.rpt + apr89.rpt + may89.rpt
```

To combine all files in the current directory that have the .txt file name extension into a single file named *Combined.doc*, type:

```
copy *.txt Combined.doc
```

To combine several binary files into one file by using wildcard characters, include **/b**. This prevents Windows from treating CTRL+Z as an end-of-file character. For example, type:

```
copy /b *.exe Combined.exe
```

> **⊗ Caution**
>
> If you combine binary files, the resulting file might be unusable due to internal formatting.

- Combining each file that has a .txt extension with its corresponding .ref file creates a file with the same file name, but with a .doc extension. The **Copy** command combines *file1.txt* with *file1.ref* to form *file1.doc*, and then the command combines *file2.txt* with *file2.ref* to form *file2.doc*, and so on. For example, type:

```
copy *.txt + *.ref *.doc
```

To combine all files with the .txt extension, and then to combine all files with the .ref extension into one file named *Combined.doc*, type:

```
copy *.txt + *.ref Combined.doc
```

Related links

- Command-Line Syntax Key
- xcopy command

cscript

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Starts a script to run in a command-line environment.

> **ⓘ Important**
>
> Performing this task does not require you to have administrative credentials. Therefore, as a security best practice, consider performing this task as a user without administrative credentials.

Syntax

```
cscript <scriptname.extension> [/b] [/d] [/e:<engine>] [{/h:cscript | /h:wscript}] [/i] [/job:<identifier>] [{/logo | /nologo}] [/s] [/t:<seconds>] [x] [/u] [/?] [<scriptarguments>]
```

Parameters

Parameter	Description
scriptname.extension	Specifies the path and file name of the script file with optional file name extension.
/b	Specifies batch mode, which does not display alerts, scripting errors, or input prompts.
/d	Starts the debugger.
/e:`<engine>`	Specifies the engine that is used to run the script.
/h:cscript	Registers cscript.exe as the default script host for running scripts.
/h:wscript	Registers wscript.exe as the default script host for running scripts. The default.

Parameter	Description
/i	Specifies interactive mode, which displays alerts, scripting errors, and input prompts. The default, and the opposite of `/b`.
/job:`<identifier>`	Runs the job identified by *identifier* in a .wsf script file.
/logo	Specifies that the Windows Script Host banner is displayed in the console before the script runs. The default, and the opposite of `/nologo`.
/nologo	Specifies that the Windows Script Host banner is not displayed before the script runs.
/s	Saves the current command-prompt options for the current user.
/t:`<seconds>`	Specifies the maximum time the script can run (in seconds). You can specify up to 32,767 seconds. The default is no time limit.
/u	Specifies Unicode for input and output that is redirected from the console.
/x	Starts the script in the debugger.
/?	Displays available command parameters and provides help for using them. The same as typing **cscript.exe** with no parameters and no script.
scriptarguments	Specifies the arguments passed to the script. Each script argument must be preceded by a slash (**/**).

Remarks

- Each parameter is optional; however, you can't specify script arguments without specifying a script. If you don't specify a script or any script arguments, cscript.exe displays the cscript.exe syntax and the valid host options.
- The **/t** parameter prevents excessive running of scripts by setting a timer. When the run time exceeds the specified value, cscript interrupts the script engine and ends the process.
- Windows script files usually have one of the following file name extensions: .wsf, .vbs, .js. Windows Script Host can use .wsf script files. Each .wsf file can use multiple scripting engines and perform multiple jobs.
- if you double-click a script file with an extension that has no association, the **Open With** dialog box appears. Select wscript or cscript, and then select **Always use this program to open this file type**. This registers wscript.exe or cscript as the default script host for files of this file type.

Related links

- Command-Line Syntax Key

date

Article • 02/03/2023

Displays or sets the system date. If used without parameters, **date** displays the current system date setting and prompts you to enter a new date.

> **ⓘ Important**
>
> You must be an administrator to use this command.

Syntax

```
date [/t | <month-day-year>]
```

Parameters

Parameter	Description
`<month-day-year>`	Sets the date specified, where *month* is the month (one or two digits, including values 1 through 12), *day* is the day (one or two digits, including values 1 through 31), and *year* is the year (two or four digits, including the values 00 through 99 or 1980 through 2099). You must separate values for *month*, *day*, and *year* with periods (.), hyphens (-), or slash marks (/). **Note:** Be mindful if you use 2 digits to represent the year, the values 80-99 correspond to 1980 through 1999.
/t	Displays the current date without prompting you for a new date.
/?	Displays help at the command prompt.

Examples

If command extensions are enabled, to display the current system date, type:

```
date /t
```

To change the current system date to August 3, 2007, you can type any of the following:

```
date 08.03.2007
date 08-03-07
date 8/3/07
```

To display the current system date, followed by a prompt to enter a new date, type:

```
date
```

To keep the current date and return to the command prompt, press **ENTER**. To change the current date, type the new date based on your current date configuration, as seen in the second example above, and then press **ENTER**.

Related links

- Command-Line Syntax Key

DCDiag

Article • 11/15/2023

> Applies To: Windows Server 2022, Windows Server 2019, Windows Server 2016

`DCDiag.exe` analyzes the state of domain controllers (DC) in a forest or enterprise and reports any problems to help in troubleshooting. As an end-user reporting program, DCDiag is a command-line tool that encapsulates detailed knowledge of how to identify abnormal behavior in the system.

By default, DCDiag is readily available if logged into a DC. An alternative method to access DCDiag is to install the Remote Server Administration Tools (RSAT) on your device. DCDiag must be ran with administrative rights from an elevated command prompt (CMD) or PowerShell.

DCDiag consists of a framework for executing tests and a series of tests to verify different functional areas of the system. This framework selects which DC is tested according to scope directives from the user, such as enterprise, site, or single server. Testing the overall connectivity and responsiveness of the DC includes verifying:

- The DC can be located in DNS
- The DC responds to Internet Control Message Protocol (ICMP) pings
- The DC allows Lightweight Directory Access Protocol (LDAP) connectivity by binding to the instance
- The DC allows binding to the AD RPC interface using the DsBindWithCred function.

> **Note**
>
> Blocking ICMP prevents DCDiag from functioning as intended. While blocking ICMP is recommended at the Internet-edge of your network, internally blocking ICMP traffic leads to administrative issues that break legacy group policies, black hole router detection, or inefficient MTU sizes due to lack of a discovery option. Troubleshooting tools such as `ping.exe` or `tracert.exe` are also affected.

DCDiag syntax

```
dcdiag [/s:<DomainController>] [/n:<NamingContext>] [/u:<Domain>\<UserName> /p:{* |
<Password> | ""}] [{/a | /e}] [{/q | /v}] [/i] [/f:<LogFile>] [/c [/skip:<Test>]]
[/test:<Test>] [/fix] [{/h | /?}] [/ReplSource:<SourceDomainController>]
```

DCDiag uses the following parameters:

Parameter	Description
/s:`<DomainController>`	Specifies the name of the server to run the command against. If this parameter isn't specified, the tests are run against the local domain controller. This parameter is ignored for DcPromo and RegisterInDns tests, which can only be run locally.
/n:`<NamingContext>`	Uses NamingContext as the naming context to test. You can specify domains in NetBIOS, Domain Name System (DNS), or distinguished name format.
/u:`<Domain>`\`<UserName>` /p:{`<Password>` | ""}	Uses Domain\UserName. DCDiag uses the current credentials of the user (or process) that is logged on. If alternate credentials are needed, use the following options to provide those credentials for binding with Password as the password: Use quotation marks ("") for an empty or null password. Use the wildcard character (*) to prompt for the password.
/a	Tests all the servers on this AD DS site.
/e	Tests all the servers in the enterprise. This overrides `/a`.
/q	Quiet. Prints only error messages.
/v	Verbose. Prints extended information.
/fix	Affects the MachineAccount test only. This parameter causes the test to fix the Service Principal Names (SPNs) on the Machine Account object of the domain controller.
/f:`<LogFile>`	Redirects all output to a log file.
/c	Comprehensive. Runs all tests except DCPromo and RegisterInDNS, including non-default tests. Optionally, you can use this parameter with the `/skip` parameter to skip specified tests. The following tests aren't run by default: • Topology • CutoffServers • OutboundSecureChannels.
/h or /?	Displays help at the command prompt.
/test:`<Test>`	Runs this test only. The connectivity test can't be skipped with the `/skip` parameter.
/ReplSource:`<SourceDomainController>`	Tests the connection between the domain controller on which you run the command and the source domain controller. (This parameter is used for the CheckSecurityError test.) SourceDomainController is the DNS name, NetBIOS name, or distinguished name of a real or potential server that will be the source domain controller for replication, as represented by a real or potential connection object.

DCDiag known tests

The following table displays known tests that run by default unless specified otherwise.

Test	Description
Advertising	Checks whether each domain controller advertises itself in the roles that it should be capable of performing. This test validates that the public DsGetDcName function used by computers to locate domain controllers will correctly locate any DCs. This test fails if the Netlogon Service has stopped or failed to start. If the Key Distribution Key (KDC) service is stopped, the Advertising test fails since the flag returned from DsGetDcName won't include KDC. If port 88 over TCP and UDP is blocked on a firewall, the Advertising test will pass despite the KDC not being able to answer Kerberos tickets requests.
CheckSDRefDom	Checks that all application directory partitions have appropriate security descriptor reference domains. This test uses LDAP and validates cross reference objects located in **cn=partitions,cn=configuration,dc=<forest root domain>** contain the correct domain names in their msDS-SDReferenceDomain attributes.
CheckSecurityError	Test is **not** run by default. Performs various security checks for errors related to the security components of the DC, such as issues with the security policy or the security database using LDAP, RPC, RPC over SMB, and ICMP. It checks: • That at least one KDC is online for each domain and is reachable. • That DCs computer object has replicated to other DCs. • If packet fragmentation of Kerberos over UDP might be an issue based on current MTU size by sending non-fragmenting ICMP packets. • That there aren't any replication or Knowledge Consistency Checker (KCC) connection issues for connected partners by querying the function DsReplicaGetInfo to get any security-related errors. • If the DCs computer account exists in Active Directory (AD) as part of the default "Domain Controllers" OU along with the correct UserAccountControl flags for DCs, the correct ServerReference attributes are set, and has the minimum required Service Principal Names (SPN) configured. When the **/ReplSource** parameter is added, the partner also checks: • The time skew calculated between the servers to verify it's less than 300 seconds (5 minutes) for Kerberos. It **doesn't** check the Kerberos policy to see if the allowed skew has been modified. • Permissions on all the naming contexts (such as Schema, Configuration, etc.) on the source DC that validates replication and connectivity functions between DCs. • Connectivity to validate that the user running DCDiag can connect to and read the SYSVOL and NETLOGON shares without any security errors. • The **Access this computer from the network** privilege on the DC is checked to verify it's held by the *Administrators*, *Authenticated Users*, and *Everyone* groups. • The DC's computer object is checked to ensure it's the latest version on the DCs. This is done to prove replication convergence along with checking versions, USNs, originating servers, and timestamps.

Test	Description
Connectivity	Verifies that the DSA and DNS are registered and reachable using LDAP and RPC.
CrossRefValidation	Retrieves a list of naming contexts located in *cn=partitions,cn=configuration,dc=<forest root domain>* with their cross references and then validates them similar to the **CheckSDRefDom** test using LDAP. This test looks at the nCName, dnsRoot, nETBIOSName, and systemFlags attributes to: • Ensure DNs names aren't invalid or null. • Confirm DNs haven't been altered by CNF or 0ADEL. • Ensure systemFlags are correct for that object. • Call out empty (orphaned) replica sets.
CutoffServers	Tests AD replication to ensure there aren't DCs without working connection objects between partners. Any servers that can't replicate inbound or outbound from any DCs are considered "cut off" using the DsReplicaSyncAll function, which triggers replication on the DCs. Use the `/e` parameter with caution if there are poorly implemented WAN links that are kept clean using schedules. If a server can't be contacted or is unavailable to LDAP on the network, then it provides no error or test results, even if the `/v` parameter is specified. This test uses RPC.
DcPromo	Tests against the server specified in the client DNS settings if the infrastructure meets the necessary requirements to promote your device to a DC. This test uses DNS on the network and checks: • If at least one network adapter has a primary DNS server set. • If there's a disjointed namespace based on the DNS suffix. • That proposed authoritative DNS zone can be contacted. • If dynamic DNS updates are possible for the server's A record. It checks both the setting on the authoritative DNS zone and client registry configuration for DnsUpdateOnAllAdapters and DisableDynamicUpdate. • If an LDAP DClocator record, like **_ldap._tcp.dc._msdcs.<domain>**, is returned when querying for existing forests. The following arguments are required: • `/DnsDomain`:<Active_Directory_Domain_DNS_Name> ◦ Using this parameter requires one of the following arguments: `/ChildDomain`, `/NewForest`, `/NewTree`, or `/ReplicaDC` • If `/NewTree` is specified, the following argument is required: ◦ `/ForestRoot`:<Forest_Root_Domain_DNS_Name>
DFSREvent	This test validates the Distributed File System Replication (DFSR) service's health by checking the DFSR event log warning and error entries from the past 24 hours. This test uses RPC and EventLog Remoting Protocol.
DNS	Tests enterprise-wide DNS health checks using DNS, RPC, and WMI protocols. Not ran by default and must be explicitly requested. See DNS syntax.
FrsEvent	Checks to see if there are errors in the File Replication Service (FRS) event log from the past 24 hours as failing replication of the SysVol share can cause policy problems. This

Test	Description
	test uses RPC and EventLog Remoting Protocol.
Intersite	Checks for failures that would prevent or temporarily hold up intersite replication and predicts how long it would take for the KCC to recover. This test uses DRS functions to check for conditions that would prevent intersite AD replication within a specific site or all sites by: • Locating and connecting to the Intersite Topology Generators (ISTG). • Locating and connecting to the bridgehead servers. • Reporting back any replication failures after triggering a replication. • Validating all DCs within sites with inbound connections to this site are available. • Checking the KCC values for **IntersiteFailuresAllowed** and **MaxFailureTimeForIntersiteLink** overrides within the registry key: **KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters**. The `/a` or `/e` parameter must be used as not providing a site would allow the test to run but skips actual testing. This test uses RPC over the network to test the replication aspects and asks registry connections to check for NTDS override entries. LDAP is also used to locate connection info.
KccEvent	This test queries the KCC on the DC for errors and warnings generated in the Directory Services event log during the last 15 minutes. The 15-minute threshold is irrespective of the Repl topology update period (secs) registry value on the DC. If firewall rules are causing this test to fail, see KB2512643 that covers enabling those rules to allow the test to succeed. This test uses RPC along with the EventLog Remoting Protocol.
KnowsOfRoleHolders	This test returns the DCs knowledge of the five Flexible Single Master Operation (FSMO) roles but doesn't check all DCs knowledge for consistency. Using the `/e` parameter provides data for comparison. This test uses RPC to return DSListRoles within the Directory Replication Service (DRS) functions.
MachineAccount	Checks whether the machine account has properly registered and that the services are advertised using LDAP and RPC over SMB, including checking: • The DC's computer account exists in AD. • It's within the Domain Controllers OU. • It has the correct UserAccountControl flags for DCs. • The correct ServerReference attributes are set. • The minimum Service Principal Names (SPN) are set. This test is identical to **CheckSecurityError** as they use the same internal test. This test also has two repair options: • `/RecreateMachineAccount` - Recreates a missing DC computer object. This is **not** a recommended fix as it doesn't recreate any child objects of a DC, such as FRS and DFSR subscriptions. The best practice is to use a valid SystemState backup to authoritatively restore the DC's deleted object and child objects. If you use this option, the DC needs to be gracefully demoted and promoted to repair all the missing relationships.

Test	Description
	• `/FixMachineAccount` - Adds the UserAccountControl flags **TRUSTED_FOR_DELEGATION** and **SERVER_TRUST_ACCOUNT** to a DCs computer object. Using this repair option is preferred over trying to set these flags yourself through **ADSIEDIT** or other LDAP editors.
NCSecDesc	Checks permissions on all the naming contexts (such as Schema, Configuration, etc.) on the source DC to validate that replication and connectivity works between DCs. It makes sure that *Enterprise Domain Controllers* and *Administrators* groups have the correct minimum permissions, which is the same test performed within **CheckSecurityError**. This test uses LDAP.
NetLogons	Validates that the user running DCDiag can connect to and read the SYSVOL and NETLOGON shares without any security errors. It also verifies that the *Administrators*, *Authenticated Users*, and *Everyone* group have the **access this computer from the network** privilege on the DC.
ObjectsReplicated	Checks that the Machine Account and Directory System Agent (DSA) objects have replicated. Two objects are validated by default and that they exist in each DC and are up to date on all other DCs: • **CN=NTDS Settings** • **CN=<DC name>** You can use the `/objectdn:dn` parameter with the `/n:nc` parameter to specify an additional object to check. This test is done using RPC with DRS functions.
OutboundSecureChannels	This test doesn't run by default. It checks that secure channels exist from all of the domain controllers in the domain to the domains specified by the `/testdomain` parameter. The `/nositerestriction` parameter prevents DCDiag from limiting the test to the domain controllers in the site.
RegisterInDNS	Tests whether the directory server can register the directory Server Locator DNS records. These records must be present in DNS in order for other computers to locate this directory server for the **<Active_Directory_Domain_DNS_Name>** domain. This also reports if any modifications to the existing DNS infrastructure are required. The parameter `/DnsDomain`:<Active_Directory_Domain_DNS_Name> must be used. This test checks: • The authoritative DNS zone can be contacted. • If at least one network adapter has a primary DNS server set. • If you would have a disjoint namespace based on the DNS suffix. • The proposed authoritative DNS zone can be contacted. • If dynamic DNS updates are possible for the server's A record. It checks settings on the authoritative DNS zone and the client registry configuration of **DnsUpdateOnAllAdapters** and **DisableDynamicUpdate**. • If an LDAP DClocator record, like **_ldap._tcp.dc._msdcs.<domain>**, is returned when querying for existing forests.
Replications	This test checks all AD replication connection objects for all naming contexts on specified DC(s) if:

Test	Description
	• The last replication attempted was successful or returns an error. • That replication is disabled. • Replication latency is more than 12 hours.
RidManager	Checks whether the relative identifier (RID) master is accessible and if: • It contains the proper information. • Can be located and contacted through a DsBind. • Has valid RID pool values. The role holder must be online and accessible for DCs to be able to create security principals (users, computers, and groups) as well as for further DCs to be promoted within a domain. This test uses LDAP and RPC.
Services	This test validates that various AD-dependent services are running, accessible, and set to specific start types. These services start automatically and run in a shared process unless specified otherwise: • DFSR (runs in own process) • DNSCACHE • EVENTSYSTEM • IISADMIN (If using SMTP-based AD replication) • ISMSERV • KDC • NETLOGON • NTDS • NTFRS (runs in own process) • RPCSS • SAMSS • SERVER • SMTPSVC (If using SMTP-based AD replication) • W32TIME (starts automatically or manually) • WORKSTATION These service names are listed in the registry path **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services**. This test uses RPC and the Service Control Manager remote protocol.
SysVolCheck	This test reads the DCs Netlogon SysVolReady registry key to validate that SYSVOL is ready. The value name has to exist with a value of 1 to pass this test and works with either FRS or DFSR replicated SYSVOLs. It doesn't check if the SYSVOL and NELOGON shares are accessible as this is performed by **CheckSecurityError**. This test uses RPC over SMB.
SystemLog	Validates the System Event Log's health by reading and writing entries from the past 60 minutes for any errors and warnings. This test uses RPC and the Service Control Manager remote protocol.
Topology	Checks that the generated AD replication topology is fully connected for all DSAs. This test isn't performed by default and must be ran explicitly. It checks:

Test	Description
	• If automatic intra-site topology generation is disabled. • If automatic inter-site topology generation is disabled. • For disconnected topologies (missing connection objects), both upstream and downstream from each reference DC. This test uses RPC, LDAP, and DsReplicaSyncAll with the flag **DS_REPSYNCALL_DO_NOT_SYNC**, meaning that it analyzes and validates replication topology without actually replicating changes. This test doesn't validate the availability of replication partners. Having a partner offline won't cause failures in this test. It also doesn't test if the schedule is closed, preventing replication. To see those active replication results, use tests **Replications** or **CutoffServers**.
VerifyEnterpriseReferences	Checks that specified system references are intact for the FRS and replication infrastructure across all objects in the enterprise on each domain controller. This includes the following DC site attributes and objects: • **frsComputerReference**: cn=domain system volume (sysvol share),cn=ntfrs subscriptions,cn=<DC Name>,ou=domain controllers,DC=<domain> • **frsComputerReferenceBL**: cn=<DC Name>,cn=domain system volume (sysvol share),cn=file replication service,cn=system,dc=<domain> • **hasMasterNCs**: cn=ntds settings,cn=<DC Name>,cn=<site>,cn=sites,cn=configuration,dc=<domain> • **msDFSR-ComputerReference**: cn=<DC Name>,cn=topology,cn=domain system volume,cn=dfsr-blobalsettings,cn=system,dc=<domain> • **msDFSR-ComputerReferenceBL**: cn=<DC Name>,ou=domain controllers,dc=<domain> • **nCName**: cn=<partition name>,cn=partitions,cn=configuration,dc=<domain> • **ServerReference**: cn=<DC name>,cn=<site>,cn=sites,cn=configuration,dc=<domain> • **ServerReferenceBL**: cn=<DC Name>,ou=domain controllers,dc=<domain> The two **DFSR** tests are only performed if domain functional level is Windows Server 2008 or higher. This means there will be an expected failure if **DFSR** hasn't been migrated to SYSVOL. This test uses LDAP and only the specified DCs are contacted.
VerifyReferences	Checks that certain system references are intact for the FRS and replication infrastructure. This test verifies computer reference attributes for a single DC, including the following DC site attributes and objects: • **frsComputerReference**: cn=domain system volume (sysvol share),cn=ntfrs subscriptions,cn=<DC Name>,ou=domain controllers,DC=<domain> • **frsComputerReferenceBL**: cn=<DC Name>,cn=domain system volume (sysvol share),cn=file replication service,cn=system,dc=<domain> • **msDFSR-ComputerReference**: cn=<DC Name>,cn=topology,cn=domain system volume,cn=dfsr-blobalsettings,cn=system,dc=<domain> • **msDFSR-ComputerReferenceBL**: cn=<DC Name>,ou=domain controllers,dc=<domain> • **ServerReference**: cn=<DC name>,cn=<site>,cn=sites,cn=configuration,dc=<domain> • **ServerReferenceBL**: cn=<DC Name>,ou=domain controllers,dc=<domain>

Test	Description
	This test uses LDAP and is similar to the **VerifyEnterpriseRefrences** test except that it doesn't check partition cross references or all other DC objects.
VerifyReplicas	Checks that all application directory partitions are fully instantiated on all replica servers. It verifies that the specified server hosts the application partitions specified by its crossref attributes in the partitions container. It operates like **CheckSDRefDom** except that it doesn't show output data and validates hosting. This test uses LDAP.

> ⓘ Note
>
> Connectivity checks on domain controllers that are registered on the network and connect with other resources like DNS, LDAP, and RPC **can't** be skipped.

DNS syntax

```
dcdiag /test:DNS [/DnsBasic | /DnsForwarders | /DnsDelegation | /DnsDynamicUpdate |
/DnsRecordRegistration | /DnsResolveExtName [/DnsInternetName:<InternetName>] |
/DnsAll] [/f:<LogFile>] [/x:<XMLLog.xml>] [/xsl:<XSLFile.xsl> or <XSLTFile.xslt>]
[/s:<DomainController>] [/e] [/v]
```

DNS test uses the following parameters:

Parameter	Description
/test:DNS	Performs the specified DNS test. If no test is specified, defaults to `/DnsAll`.
/DnsBasic	Performs basic DNS tests, including network connectivity, DNS client configuration, service availability, and zone existence.
/DnsForwarders	Performs the `/DnsBasic` tests and also checks the configuration of forwarders.
/DnsDelegation	Performs the `/DnsBasic` tests and also checks for proper delegations.
/DnsDynamicUpdate	Performs `/DnsBasic` tests and also determines if dynamic update is enabled in the Active Directory zone.
/DnsRecordRegistration	Performs the `/DnsBasic` tests, and also checks if the address (A), canonical name (CNAME) and well-known service (SRV) resource records are registered. In addition, creates an inventory report based on the test results.
/DnsResolveExtName [/DnsInternetName:\ `<InternetName>`]	Performs the `/DnsBasic` tests, and also attempts to resolve InternetName. If `/DnsInternetName` isn't specified, attempts to resolve the name

Parameter	Description
	<www.microsoft.com>. If `/DnsInternetName` is specified, attempts to resolve the Internet name supplied by the user.
/DnsAll	Performs all tests, except for the `/DnsResolveExtName` test, and generates a report.
/f:`<LogFile>`	Redirects all output to a log file.
/s:`<DomainController>`	Runs the tests against the domain controller. If this parameter isn't specified, the tests are run against the local domain controller.
/e	Runs all tests specified by `/test:DNS` against all domain controllers in the Active Directory forest.
/v	Verbose. Presents extended information about successful test results in addition to information about errors and warnings. When the `/v` parameter isn't used, provides only error and warning information. Use the `/v` switch when errors or warnings are reported in the summary table.
/x:`<XMLLog.xml>`	Redirects all output to xmllog.xml. This parameter works only with the `/test:DNS` option.
/xsl:`<XSLFile.xsl>` or /xsl:`<XSLTFile.xslt>`	Adds the processing instructions that reference the specified sheet. This parameter only works with the `/test:DNS /x:<XMLLog.xml` option.

> **Note**
>
> Run times for DNS tests can be significant in large enterprises when the `/e` parameter is used. Domain controllers and DNS servers that are offline will increase run times due to long time-out periods for RPC and other protocols.

Examples

Connectivity test

To run a series of connectivity tests on the local domain, run the following command:

PowerShell

```
dcdiag
```

A successful connectivity test output:

Output

```
Directory Server Diagnosis
```

```
Performing initial setup:

   Trying to find home server...

   Home Server = MapleWaffle-WS22

   * Identified AD Forest.
   Done gathering initial info.


Doing initial required tests


   Testing server: Default-First-Site-Name\MAPLEWAFFLE-WS2

      Starting test: Connectivity

         ..... MAPLEWAFFLE-WS2 passed test Connectivity


Doing primary tests

      Testing server: Default-First-Site-Name\MAPLEWAFFLE-WS2

      Starting test: Advertising
         ..... MAPLEWAFFLE-WS2 passed test Advertising

      Starting test: FrsEvent
         ..... MAPLEWAFFLE-WS2 passed test FrsEvent

      Starting test: DFSREvent
         ..... MAPLEWAFFLE-WS2 passed test DFSREvent

      Starting test: SysVolCheck
         ..... MAPLEWAFFLE-WS2 passed test SysVolCheck

      Starting test: KccEvent
         ..... MAPLEWAFFLE-WS2 passed test KccEvent

      Starting test: KnowsOfRoleHolders
         ..... MAPLEWAFFLE-WS2 passed test KnowsOfRoleHolders

      Starting test: MachineAccount
         ..... MAPLEWAFFLE-WS2 passed test MachineAccount

      Starting test: NCSecDesc
         ..... MAPLEWAFFLE-WS2 passed test NCSecDesc

      Starting test: NetLogons
         ..... MAPLEWAFFLE-WS2 passed test NetLogons

      Starting test: ObjectsReplicated
         ..... MAPLEWAFFLE-WS2 passed test ObjectsReplicated

      Starting test: Replications
         ..... MAPLEWAFFLE-WS2 passed test Replications

      Starting test: RidManager
         ..... MAPLEWAFFLE-WS2 passed test RidManager
```

```
      Starting test: Services
         ..... MAPLEWAFFLE-WS2 passed test Services

      Starting test: SystemLog
         ..... MAPLEWAFFLE-WS2 passed test SystemLog

      Starting test: VerifyReferences
         ..... MAPLEWAFFLE-WS2 passed test VerifyReferences

   Running partition tests on : ForestDnsZones

      Starting test: CheckSDRefDom
         ..... ForestDnsZones passed test CheckSDRefDom

      Starting test: CrossRefValidation
         ..... ForestDnsZones passed test CrossRefValidation

   Running partition tests on : DomainDnsZones

      Starting test: CheckSDRefDom
         ..... DomainDnsZones passed test CheckSDRefDom

      Starting test: CrossRefValidation
         ..... DomainDnsZones passed test CrossRefValidation

   Running partition tests on : Schema

      Starting test: CheckSDRefDom
         ..... Schema passed test CheckSDRefDom

      Starting test: CrossRefValidation
         ..... Schema passed test CrossRefValidation

   Running partition tests on : Configuration

      Starting test: CheckSDRefDom
         ..... Configuration passed test
         CheckSDRefDom

      Starting test: CrossRefValidation
         ..... Configuration passed test
         CrossRefValidation

   Running partition tests on : corp

      Starting test: CheckSDRefDom
         ..... corp passed test CheckSDRefDom

      Starting test: CrossRefValidation
         ..... corp passed test CrossRefValidation

   Running enterprise tests on : corp.contoso.com

      Starting test: LocatorCheck
         ..... corp.contoso.com passed test
         LocatorCheck

      Starting test: Intersite
```

```
         ..... corp.contoso.com passed test
         Intersite
```

To run a series of connectivity tests on a specific domain controller, run the following command:

```PowerShell
dcdiag /s:<DomainControllerName>
```

It should generate similar results as the local test if no issues are encountered.

Output to a log file

DCDiag is able to save the output results to a text file by running:

```PowerShell
dcdiag /s:<DomainControllerName> /f:<FileName.txt>
```

If no `<FilePath>` is specified, results are saved to `C:\Users\<UserName>\<FileName.txt>` by default.

To save to a specific location, run:

```PowerShell
dcdiag /s:<DomainControllerName> /f:<DriveLetter>\<FilePath>\<FileName.txt>
```

See also

Command-Line Syntax Key

dcgpofix

Article • 04/22/2024

Recreates the default Group Policy Objects (GPOs) for a domain. To get to the Group Policy Management Console (GPMC), you must install Group Policy Management as a feature through Server Manager. `Dcgpofix.exe` is included with Windows Server and is located in the `C:\Windows\system32\` folder.

`Dcgpofix.exe` restores only the policy settings that are contained in the Default Domain Policy GPO and Default Domain Controller GPO. `Dcgpofix.exe` doesn't restore other GPOs that administrators create, it's only intended for disaster recovery of the default GPOs.

> **Important**
>
> As a best practice, you should configure the Default Domain Policy GPO only to manage the default **Account Policies** settings, Password Policy, Account Lockout Policy, and Kerberos Policy. Additionally, you should configure the Default Domain Controllers Policy GPO only to set user rights and audit policies.

Syntax

```
dcgpofix [/ignoreschema] [/target: {domain | dc | both}] [/?]
```

Parameters

Expand table

Parameter	Description
/ignoreschema	Ignores the version of the Active Directory schema when you run this command. Otherwise, the command only works on the same schema version as the Windows version in which the command was shipped.
`/target {domain | dc | both`	Specifies whether to target the Default Domain policy, the Default Domain Controllers policy, or both types of policies.
/?	Displays Help at the command prompt.

Examples

To manage the default **Account Policies** settings, Password Policy, Account Lockout Policy, and Kerberos Policy, while ignoring the Active Directory schema version, type:

```
dcgpofix /ignoreschema /target:domain
```

To configure the Default Domain Controllers Policy GPO only to set user rights and audit policies, while ignoring the Active Directory schema version, type:

```
dcgpofix /ignoreschema /target:dc
```

Related links

- Command-Line Syntax Key

dcpromo

Article • 04/22/2024

Applies To: Windows Server (All supported versions)

The dcpromo command installs, promotes, demotes, and removes Active Directory Domain Services (AD DS) from a Windows Server.

For examples of how to use **dcpromo**, see Examples.

Syntax

```
dcpromo [/answer[:\<filename>] | /unattend[:\<filename>] | /unattend | /adv] /uninstallBinaries [/CreateDCAccount | /UseExistingAccount:Attach] /? /?[:{Promotion | CreateDCAccount | UseExistingAccount | Demotion}]
```

Dcpromo.exe parameters

Expand table

Parameter	Description
/answer[:<filename>]	Specifies an answer file that contains installation parameters and values.
/unattend[:<filename>]	Specifies an answer file that contains installation parameters and values. This command provides the same function as /answer[:<filename>].
/unattend	Specifies an unattended installation in which you provide installation parameters and values at the command line.
/adv	Performs an install from media (IFM) operation.
/UninstallBinaries	Uninstalls AD DS binaries.
/CreateDCAccount	Creates a read-only domain controller (RODC) account. Only a member of the Domain Admins group or the Enterprise Admins group can run this command.
/UseExistingAccount:Attach	Attaches a server to an existing RODC account. A member of the Domain Admins group or a delegated user can run this command.

Parameter	Description
/?	Displays Help for Dcpromo parameters.
/?[:{Promotion | CreateDCAccount | UseExistingAccount | Demotion}]	Displays parameters that apply to the dcpromo operation. For example, `dcpromo /?:Promotion` displays all of the parameters that you can use for a promotion operation.

dcpromo promotion operation parameters

The following table shows the parameters available when running `dcpromo.exe` from a command prompt for the unattended installation of a domain controller that runs Windows Server.

For more information about creating a new forest, see Installing a New Windows Server 2008 Forest.

For more information about creating a new domain, see Installing a New Windows Server 2008 Child Domain.

For more information about creating a new domain tree, see Installing a New Windows Server 2008 Domain Tree.

For more information about creating another domain controller for a domain, see Installing an Additional Windows Server 2008 Domain Controller.

Expand table

Parameter and value pair	Description and default
AllowDomainControllerReinstall:{Yes | <No> | NoAndNoPromptEither}	Specifies whether to continue installing this domain controller, even when another domain controller account with the same name is detected. Use Yes only if you're sure that the account isn't currently used by another domain controller. The default is **No**.
AllowDomainReinstall:{Yes | <No> | NoAndNoPromptEither}	Specifies whether an existing domain is recreated. The default is **No**.

Parameter and value pair	Description and default
ApplicationPartitionsToReplicate:""	Specifies the application directory partitions that dcpromo will replicate. Use the following format: "**partition1**" "**partition2**" "**partitionN**" Use * to replicate all application directory partitions.
AutoConfigDNS:{Yes | No} This parameter has been renamed to **InstallDNS**.	Specifies whether the DNS Server service should be installed. The default is automatically computed based on the environment.
ChildName:"child_domain_name"	Specifies the single-label Domain Name System (DNS) name of the child domain.
ConfirmGc:{Yes | No}	Specifies whether you want the domain controller to be a global catalog server.
CreateDNSDelegation: { Yes | No}	Indicates whether to create a DNS delegation that references the new DNS server that you're installing along with the domain controller. Valid for Active Directory–integrated DNS only. The default is computed automatically based on the environment.
CriticalReplicationOnly:{Yes | <No>}	Specifies whether the AD DS installation operation performs only critical replication before reboot and then continues, skipping the noncritical (and potentially lengthy) portion of replication. The noncritical replication happens after the installation finishes and the computer reboots. The default is **No**.
DatabasePath:"path_to_database_files"	Specifies the fully qualified, non–Universal Naming Convention (UNC) path to a directory on a fixed disk of the local computer that contains the domain database, for example, **C:\Windows\NTDS**. The default is **%SYSTEMROOT%\NTDS**.
DelegatedAdmin:"name of user or group"	Specifies the name of the user or group that will install and administer the RODC.

Parameter and value pair	Description and default
DNSDelegationPassword:"password"	Specifies the password for the user name (account credentials) for creating DNS delegation.
DNSDelegationUserName:"user_name"	Specifies the user name (account credentials) for creating DNS delegation.
DNSOnNetwork:{<Yes> | No}	Specifies whether DNS service is available on the network. This parameter is used only when the IP setting of the network adapter for this computer isn't configured with the name of a DNS server for name resolution. No indicates that a DNS server will be installed on this computer for name resolution. Otherwise, the IP settings of the network adapter must be configured with a DNS server name first. The default is **Yes**.
DomainLevel:{0 | 2 | 3 | 4 | 5 | 6 | 7 | 10}	This entry specifies the domain functional level. This entry is based on the levels that exist in the forest when a new domain is created in an existing forest. Value descriptions are as follows: - 0 = Windows 2000 Server native mode - 2 = Windows Server 2003 - 3 = Windows Server 2008 - 4 = Windows Server 2008 R2 - 5 = Windows Server 2012 - 6 = Windows Server 2012 R2 - 7 = Windows Server 2016 - 10 = Windows Server 2025 The domain functional level can't be lower than the forest functional level, but it can be higher. The default is automatically computed and set to the existing forest functional level or the value that is set for **/ForestLevel**.
DomainNetBiosName:"domain_NetBIOS_name"	Assigns a NetBIOS name to the new domain.
ForestLevel:{ 0 | 2 | 3 | 4 | 5 | 6 | 7 | 10}	This entry specifies the forest functional level when a new domain is created in a new forest as follows: - 0 = Windows 2000 Server native mode - 2 = Windows Server 2003

Parameter and value pair	Description and default
	- 3 = Windows Server 2008 - 4 = Windows Server 2008 R2 - 5 = Windows Server 2012 - 6 = Windows Server 2012 R2 - 7 = Windows Server 2016 - 10 = Windows Server 2025 The default forest functional level in Windows Server 2008 when you create a new forest is Windows 2000 (0). Don't use this parameter when you install a domain controller in an existing forest.
InstallDNS:{Yes | No}	Specifies whether the DNS Server service should be installed. The default is automatically computed based on the environment. This parameter replaces **AutoConfigDNS**.
LogPath:"path_to_log_files"	Specifies the fully qualified, non-UNC path to a directory on a fixed disk of the local computer that contains the domain log files, for example, **C:\Windows\Logs**. The default is **%SYSTEMROOT%\NTDS**.
NewDomain:{Tree | Child | <Forest>}	Indicates the type of domain that you want to create: a new domain tree in an existing forest, a child of an existing domain, or a new forest. The default is new forest.
NewDomainDNSName:"DNS_name_of_domain"	Specifies the fully qualified domain name (FQDN) for the new domain.
ParentDomainDNSName:"DNS_name_of_domain"	Specifies the FQDN of an existing parent domain. You use this parameter when you install a child domain.
Password:"password"	Specifies the password that corresponds to the user name (account credentials) that is used to install the domain controller. Use this parameter with the **UserName** parameter. Use * to prompt the user to supply a password.

Parameter and value pair	Description and default
PasswordReplicationAllowed:{"security_principal" | None}	Specifies the names of user accounts, group accounts, and computer accounts whose passwords can be replicated to this RODC. Use None if you want to keep the value empty. By default, only the Allowed RODC Password Replication Group is allowed, and it's originally created empty.
PasswordReplicationDenied:{"security_principal" | None}	Specifies the names of user accounts, group accounts, and computer accounts whose passwords aren't to be replicated to this RODC. Use None if you don't want to deny the replication of credentials of any users or computers. By default, Administrators, Server Operators, Backup Operators, Account Operators, and the Denied RODC Password Replication Group are denied. By default, the Denied RODC Password Replication Group includes: • Cert Publishers • Domain Admins • Enterprise Admins • Enterprise Domain Controllers • Enterprise Read-Only Domain Controllers • Group Policy Creator Owners • The krbtgt account • Schema Admins
RebootOnCompletion:{<Yes> | No}	Specifies whether to restart the computer upon completion of the command, regardless of success. The default is **Yes**.
RebootOnSuccess:{<Yes> | No | NoAndNoPromptEither}	Specifies whether to restart the computer upon successful completion of the command. The default is **Yes**.
ReplicaDomainDNSName:"DNS_name_of_domain"	Specifies the FQDN of the domain in which you want to install another domain controller.
ReplicaOrNewDomain:{<Replica> | ReadOnlyReplica | Domain}	Specifies whether to install another domain controller (a writable domain controller or an RODC) or to create a new domain.

Parameter and value pair	Description and default
	The default is to install another writable domain controller.
ReplicationSourceDC:"DNS_name_of_DC"	Indicates the FQDN of the partner domain controller from which you replicate the domain information.
ReplicationSourcePath:"replication_source_path"	Indicates the location of the installation media that will be used to install a new domain controller.
SafeModeAdminPassword:"password"	Supplies the password for the administrator account when the computer is started in Safe Mode or a variant of Safe Mode, such as Directory Services Restore Mode. The default is an empty password. You must supply a password.
SiteName:"site_name"	Specifies the name of an existing site where you can place the new domain controller. The default value depends on the type of installation. For a new forest, the default is Default-First-Site-Name. For all other installations, the default is the site that is associated with the subnet that includes the IP address of this server. If no such site exists, the default is the site of the replication source domain controller.
SkipAutoConfigDns	Skips automatic configuration of DNS client settings, forwarders, and root hints. This parameter is in effect only if the DNS Server service is already installed.
Syskey:{<none> | system key}	Specifies the system key for the media from which you replicate the data. The default is **none**.
SysVolPath:"path_to_database_file"	Specifies the fully qualified, non-UNC path to a directory on a fixed disk of the local computer, for example, **C:\Windows\SYSVOL**. The default is **%SYSTEMROOT%\SYSVOL**.
TransferIMRoleIfNecessary:{Yes | <No>}	Specifies whether to transfer the infrastructure master operations master role

Parameter and value pair	Description and default
	(also known as flexible single master operations or FSMO) to the domain controller that you're creating. Perform the transfer in case it's currently hosted on a global catalog server—and you don't plan to make the domain controller that you're creating a global catalog server. Use **Yes** to transfer the infrastructure master role to the domain controller that you're creating in case the transfer is needed; in this case, make sure to use `/ConfirmGC:No`. Use **No** if you want the infrastructure master role to remain where it currently is. The default is **No**.
UserDomain:"domain_name"	Specifies the domain name for the user name (account credentials) for installing a domain controller. Use this parameter with the **UserName** parameter.
UserName:"user_name"	Specifies the user name (account credentials) for the operation. If no value is specified, the credentials of the current user are used for the operation.

dcpromo /CreateDCAccount operation parameters

The following table shows the parameters that you can use when you create an RODC account.

For more information about creating an RODC account, see Performing a Staged RODC Installation.

Expand table

Parameter and value pair	Description and default
PAutoConfigDNS:{Yes | No} This parameter has been renamed to InstallDNS.	Specifies whether the DNS Server service should be installed. The default is computed automatically based on the environment.

Parameter and value pair	Description and default
ConfirmGc:{Yes | No}	Specifies whether the domain controller will be a global catalog server.
DCAccountName:"name of the domain controller to create"	Specifies the name of the RODC account that you're creating.
DelegatedAdmin:"name of user or group"	Specifies the name of the user or group that will install and administer the RODC.
InstallDNS:{Yes | No}	Specifies whether the DNS Server service should be installed. The default is computed automatically based on the environment. This parameter replaces **/AutoConfigDNS**.
password:"password"	Specifies the password that corresponds to the user name (account credentials) that is used to install the domain controller. Use this parameter with the **UserName** parameter. Specify * to prompt the user to supply a password.
PasswordReplicationAllowed:{"security_principal" | None}	Specifies the names of user accounts, group accounts, and computer accounts whose passwords can be replicated to this RODC. Use None if you want to keep this value empty. By default, only the Allowed RODC Password Replication Group is allowed, and it's originally created empty.
PasswordReplicationDenied:{"security_principal" | None}	Specifies the names of user accounts, group accounts, and computer accounts whose passwords aren't to be replicated to this RODC. Use None if you don't want to deny the replication of credentials of any users or computers. By default, Administrators, Server Operators, Backup Operators, Account Operators, and the Denied RODC Password Replication Group are denied. By default, the Denied RODC Password Replication Group includes: • Cert Publishers • Domain Admins • Enterprise Admins • Enterprise Domain Controllers • Enterprise Read-Only Domain Controllers • Group Policy Creator Owners

Parameter and value pair	Description and default
	• The krbtgt account • Schema Admins
ReplicaDomainDNSName:"DNS_name_of_domain"	Specifies the FQDN of the domain in which you want to install another domain controller.
ReplicationSourceDC:"DNS_name_of_DC"	Indicates the FQDN of the partner domain controller from which you replicate the domain information.
SiteName:"site_name"	Specifies the name of an existing site where you can place the new domain controller. The default value depends on the type of installation. For a new forest, the default is Default-First-Site-Name. For all other installations, the default is the site that is associated with the subnet that includes the IP address of this server. If no such site exists, the default is the site of the replication source domain controller.
UserDomain:"domain_name"	Specifies the domain name for the user name (account credentials) for the operation. This parameter also helps to specify the forest where you plan to install the domain controller or create an RODC account. If no value is specified, the domain of the computer is used.
UserName:"user_name"	Specifies the user name (account credentials) for the operation. If no value is specified, the credentials of the current user are used for the operation.

dcpromo /UseExistingAccount operation parameters

You can use parameters in the following list when you attach a server to an RODC account.

For more information about attaching a server to an RODC account, see Performing a Staged RODC Installation.

Expand table

Parameter and value pair	Description and default
ApplicationPartitionsToReplicate:""	Specifies the application directory partitions that dcpromo will replicate. Use the following format: "**partition1**" "**partition2**" "**partitionN**" Use * to replicate all application directory partitions.
CriticalReplicationOnly:{Yes | <No>}	Specifies whether the installation performs only critical replication before reboot and then continues, skipping the noncritical (and potentially lengthy) portion of replication. The noncritical replication happens after the role installation finishes and the computer reboots. The default is No.
DatabasePath:"path_to_database_files"	Specifies the fully qualified, non-UNC path to a directory on a fixed disk of the local computer that contains the domain database, for example, **C:\Windows\NTDS**. The default is **%SYSTEMROOT%\NTDS**.
DNSOnNetwork:{<Yes> | No}	Specifies whether the DNS Server service is available on the network. This parameter is used only when the IP setting of the network adapter for this computer isn't configured with the name of a DNS server for name resolution. No indicates that DNS server will be installed on this computer for name resolution. Otherwise, the IP settings of network adapter must be configured with a DNS server name first. The default is **Yes**.
LogPath:"path_to_log_files"	Specifies the fully qualified, non-UNC path to a directory on a fixed disk of the local computer that contains the domain log files, for example, C:\Windows\Logs. The default is **%SYSTEMROOT%\NTDS**.
Password:"password"	Specifies the password that corresponds to the user name (account credentials) that is

Parameter and value pair	Description and default
	used to install the domain controller. Use this parameter with the **UserName** parameter. Use * to prompt the user to supply a password.
RebootOnCompletion:{<Yes> | No}	Specifies whether to restart the computer upon completion, regardless of success. The default is **Yes**.
RebootOnSuccess:{<Yes> | No | NoAndNoPromptEither}	Specifies whether to restart the computer upon successful completion. The default is **Yes**.
ReplicaDomainDNSName:"DNS_name_of_domain"	Specifies the FQDN of the domain in which you want to install another domain controller.
ReplicationSourceDC:"DNS_name_of_DC"	Indicates the FQDN of the partner domain controller from which you replicate the domain information.
ReplicationSourcePath:"replication_source_path"	Indicates the location of the installation media that will be used to install a new domain controller.
SafeModeAdminPassword:"password"	Supplies the password for the administrator account when the computer is started in Safe Mode or a variant of Safe Mode, such as Directory Service Restore Mode. The default is an empty password. You must supply a password.
SkipAutoConfigDns	Skips automatic configuration of DNS client settings, forwarders, and root hints. This parameter is in effect only if the DNS Server service is already installed.
Syskey:{<none> | system key}	Specifies the system key for the media from which you replicate the data. The default is **none**.
SysVolPath:"path_to_database_file"	Specifies the fully qualified, non-UNC path to a directory on a fixed disk of the local computer, for example, **C:\Windows\SYSVOL**.

Parameter and value pair	Description and default
	The default is **%SYSTEMROOT%\SYSVOL**.
UserDomain:"domain_name"	Specifies the domain name for the user name (account credentials) for the operation. This parameter also helps to specify the forest where you plan to install the domain controller or create an RODC account. If no value is specified, the domain of the computer will be used.
UserName:"user_name"	Specifies the user name (account credentials) for the operation. If no value is specified, the credentials of the current user are used for the operation.

dcpromo Demotion operation parameters

You can use parameters in the following list when you remove AD DS from a domain controller that runs Windows Server.

For more information about removing a domain controller from a domain, see Removing a Windows Server 2008 Domain Controller from a Domain.

For more information about removing the last domain controller in a domain, see Removing the Last Windows Server 2008 Domain Controller in a Domain.

For more information about removing the last domain controller in a forest, see Removing the Last Windows Server 2008 Domain Controller in a Forest.

For more information about forcing the removal of a domain controller, see Forcing the Removal of a Windows Server 2008 Domain Controller.

Expand table

Parameter and value pair	Description and default
AdministratorPassword:"administrator password"	Specifies a local administrator account password when AD DS is removed from a domain controller. The default is an empty password.
DemoteFSMO:{Yes | <No>}	Indicates that (forced) demotion should continue, even if an operations master role is discovered on domain controller from which AD DS is being removed.

Parameter and value pair	Description and default
	The default is **No**.
DNSDelegationPassword {Password | *}	Specifies the password to use for the user name (the account credentials) when you create or remove the DNS delegation. Specify `*` to prompt the user to enter credentials.
DNSDelegationUserName: "user_name"	Specifies the user name to use when you create or remove the DNS delegation. If you don't specify a value, then the account credentials that you specify for the AD DS installation or removal are used to for the DNS delegation.
IgnoreIsLastDcInDomainMismatch: {Yes | <No>}	Used with `/IsLastDCInDomain`. This parameter specifies whether Dcpromo.exe ignores any inconsistency that it detects with the value that you specify for `/IsLastDCInDomain`. For example, if you specify `/IsLastDCInDomain:Yes` but dcpromo detects that there's actually another active domain controller in the domain, you can specify `/IgnoreIsLastDcInDomainMismatch:Yes` to have dcpromo continue the removal of AD DS from the domain controller despite the inconsistency that it has detected. Similarly, if you specify `/IsLastDCInDomain:No` but dcpromo can't detect that another domain controller is in the domain, you can specify `/IgnoreIsLastDcInDomainMismatch:Yes` to have dcpromo continue to remove AD DS from the domain controller. The default is **No**. The default causes the wizard to prompt the user to continue and causes the command-line tool to exit with an error.
IgnoreIsLastDNSServerForZone:{Yes | <No>}	Specifies whether to continue the removal of AD DS, even when the domain controller is the last DNS server for one or more of the Active Directory–integrated DNS zones that it hosts. The default is **No**.
IsLastDCInDomain:{Yes | <No>}	Specifies whether the computer from which AD DS is being removed is the last domain controller in the domain. The default is **No**.
Password:"password"	Specifies the password that corresponds to the user name (account credentials) that is used to install the domain controller. Use this parameter with the **UserName** parameter.

Parameter and value pair	Description and default
	Specify `*` to prompt the user to supply a password.
RebootOnCompletion:{<Yes> | No}	Specifies whether to restart the computer upon completion, regardless of success. The default is **Yes**.
RebootOnSuccess:{<Yes> | No | NoAndNoPromptEither}	Specifies whether to restart the computer upon successful completion. The default is **Yes**.
RemoveApplicationPartitions:{Yes | <No>}	Specifies whether to remove application partitions during the removal of AD DS from a domain controller. The default is **No**.
RemoveDNSDelegation:{<Yes> | No}	Specifies whether to remove DNS delegations that point to this DNS server from the parent DNS zone. The default is **Yes**.
RetainDCMetadata:{Yes | <No>}	Retains domain controller metadata in the domain after AD DS removal to allow a delegated administrator to remove AD DS from an RODC. **The default is No**.
UserDomain:"domain_name"	Specifies the domain name for the user name (account credentials) for the operation. This parameter also helps to specify the forest where you plan to install the domain controller or create an RODC account. If no value is specified, the domain of the computer will be used.
UserName:"user_name"	Specifies the user name (account credentials) for the operation. If no value is specified, the credentials of the current user are used for the operation.

Examples

The following example supplies an answer file named **NewForestInstallation**:

cli

```
dcpromo /answer:NewForestInstallation
```

The following example creates the first domain controller in a new child domain where you expect to install at least some Windows Server 2025 domain controllers:

```cli
dcpromo /unattend /InstallDns:yes /ParentDomainDNSName:contoso.com
/replicaOrNewDomain:domain /newDomain:child
/newDomainDnsName:east.contoso.com /childName:east /DomainNetbiosName:east
/databasePath:"e:\ntds" /logPath:"e:\ntdslogs" /sysvolpath:"g:\sysvol"
/safeModeAdminPassword:FH#3573.cK /forestLevel:10 /domainLevel:10
/rebootOnCompletion:yes
```

The following example creates another domain controller with the global catalog, and it installs and configures the DNS Server service:

```cli
dcpromo /unattend /InstallDns:yes /confirmGC:yes /replicaOrNewDomain:replica
/databasePath:"e:\ntds" /logPath:"e:\ntdslogs" /sysvolpath:"g:\sysvol"
/safeModeAdminPassword:M6$,U8Gvx4 /rebootOnCompletion:yes
```

Change History

Expand table

Date	Revision
10/04/2010	Removed the DNSDelegation, DNSDelegationUserName, DNSDelegationPassword, and TransferIMRoleIfNecessary parameters from the /UseExistingAccount operation.

defrag

Article • 09/28/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 11, Windows 10, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Locates and consolidates fragmented files on local volumes to improve system performance.

Membership in the local **Administrators** group, or equivalent, is the minimum required to run this command.

Syntax

```
defrag <volumes> | /c | /e <volumes>    [/h] [/m [n]| [/u] [v]]
defrag <volumes> | /c | /e <volumes> /a [/h] [/m [n]| [/u] [v]]
defrag <volumes> | /c | /e <volumes> /x [/h] [/m [n]| [/u] [v]]
defrag <volume> [<parameters>]
```

Parameters

Parameter	Description
`<volume>`	Specifies the drive letter or mount point path of the volume to be defragmented or analyzed.
/a	Performs an analysis on the specified volumes.
/b	Performs boot optimization to increase boot performance.
/c	Performs the operation on all volumes.
/d	Performs traditional defrag (this is the default). On a tiered volume though, traditional defrag is performed only on the Capacity tier.
/e	Performs the operation on all volumes except those specified.
/g	Optimizes the storage tiers on the specified volumes.
/h	Runs the operation at normal priority (default is low).
/i [n]	Tier optimization would run for at most n seconds on each volume.

Parameter	Description
/k	Performs slab consolidation on the specified volumes.
/l	Performs retrim on the specified volumes.
/m [n]	Runs the operation on each volume in parallel in the background. At most, *n* threads optimize the storage tiers in parallel.
/o	Performs the proper optimization for each media type.
/t	Tracks an operation already in progress on the specified volume.
/u	Prints the progress of the operation on the screen.
/v	Prints verbose output containing the fragmentation statistics.
/x	Performs free space consolidation on the specified volumes.
/?	Displays the help information.

Remarks

- You can't defragment specific file system volumes or drives, including:
  - Volumes locked by the file system.
  - Volumes the file system marked as dirty, indicating possible corruption. You must run `chkdsk` before you can defragment this volume or drive. You can determine if a volume is dirty by using the `fsutil dirty` command.
  - Network drives.
  - CD-ROMs.
  - File system volumes that aren't **NTFS**, **ReFS**, **Fat** or **Fat32**.
- To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure. As a security best practice, consider using **Run As** to perform this procedure.
- A volume must have at least 15% free space for **defrag** to completely and adequately defragment it. **defrag** uses this space as a sorting area for file fragments. If a volume has less than 15% free space, **defrag** will only partially

defragment it. To increase the free space on a volume, delete unneeded files or move them to another disk.

- While **defrag** is analyzing and defragmenting a volume, it displays a blinking cursor. When **defrag** is finished analyzing and defragmenting the volume, it displays the analysis report, the defragmentation report, or both reports, and then exits to the command prompt.
- By default, **defrag** displays a summary of both the analysis and defragmentation reports if you don't specify the **/a** or **/v** parameters.
- You can send the reports to a text file by typing **>***FileName.txt*, where *FileName.txt* is a file name you specify. For example: `defrag volume /v > FileName.txt`
- To interrupt the defragmentation process, at the command line, press **CTRL+C**.
- Running the **defrag** command and Disk defragmenter are mutually exclusive. If you're using Disk defragmenter to defragment a volume and you run the **defrag** command at a command-line, the **defrag** command fails. Conversely, if you run the **defrag** command and open Disk defragmenter, the defragmentation options in Disk defragmenter are unavailable.

Examples

To defragment the volume on drive C while providing progress and verbose output, type:

```
defrag c: /u /v
```

To defragment the volumes on drives C and D in parallel in the background, type:

```
defrag c: d: /m
```

To perform a fragmentation analysis of a volume mounted on drive C and provide progress, type:

```
defrag c: mountpoint /a /u
```

To defragment all volumes with normal priority and provide verbose output, type:

```
defrag /c /h /v
```

Scheduled task

The defragmentation process runs scheduled task as a maintenance task, which typically runs every week. As an Administrator, you can change how often the task runs by using the **Optimize Drives** app.

- When run from the scheduled task, **defrag** uses the below policy guidelines for SSDs:
    - **Traditional optimization processes**. Includes **traditional defragmentation**, for example moving files to make them reasonably contiguous and **retrim**. This is done once per month. However, if both **traditional defragmentation** and **retrim** are skipped, then **analysis** isn't run. Changing the frequency of the scheduled task doesn't affect the once per month cadence for the SSDs.
    - If you manually run **traditional defragmentation** on an SSD, between your normally scheduled runs, the next scheduled task run performs **analysis** and **retrim**, but skips **traditional defragmentation** on that SSD.
    - If you skip **analysis**, you won't see an updated **Last run** time in the **Optimize Drives** app. Because of that, the **Last run** time can be up to a month old.
    - You might find that scheduled task hasn't defragmented all volumes. This is typically because:
        - The process won't wake the computer to run.
        - The computer isn't plugged in. The process won't run if the computer is running on battery power.
        - The computer is resumed from being idle.

Related links

- Command-Line Syntax Key
- chkdsk

- fsutil
- fsutil dirty
- Optimize-Volume PowerShell

del

Article • 02/03/2023

Deletes one or more files. This command performs the same actions as the **erase** command.

The **del** command can also run from the Windows Recovery Console, using different parameters. For more information, see Windows Recovery Environment (WinRE).

> ⚠ **Warning**
>
> If you use **del** to delete a file from your disk, you can't retrieve it.

Syntax

```
del [/p] [/f] [/s] [/q] [/a[:]<attributes>] <names>
erase [/p] [/f] [/s] [/q] [/a[:]<attributes>] <names>
```

Parameters

Parameter	Description
`<names>`	Specifies a list of one or more files or directories. Wildcards may be used to delete multiple files. If a directory is specified, all files within the directory will be deleted.
/p	Prompts for confirmation before deleting the specified file.
/f	Forces deletion of read-only files.
/s	Deletes specified files from the current directory and all subdirectories. Displays the names of the files as they are being deleted.
/q	Specifies quiet mode. You are not prompted for delete confirmation.

Parameter	Description
/a[:]`<attributes>`	Deletes files based on the following file attributes: • **r** Read-only files • **h** Hidden files • **i** Not content indexed files • **s** System files • **a** Files ready for archiving • **l** Reparse points • **-** Used as a prefix meaning 'not' .
/?	Displays help at the command prompt.

Remarks

- If you use the `del /p` command, you'll see the following message:

  `FileName, Delete (Y/N)?`

  To confirm the deletion, press **Y**. To cancel the deletion and to display the next file name (if you specified a group of files), press **N**. To stop the **del** command, press CTRL+C.

- If you disable command extension, the **/s** parameter will display the names of any files that weren't found ,instead of displaying the names of files that are being deleted.

- If you specify specific folders in the `<names>` parameter, all of the included files will also be deleted. For example, if you want to delete all of the files in the *\work* folder, type:

  ```
  del \work
  ```

- You can use wildcards (***** and **?**) to delete more than one file at a time. However, to avoid deleting files unintentionally, you should use wildcards cautiously. For example, if you type the following command:

  ```
  del *.*
  ```

The **del** command displays the following prompt:

```
Are you sure (Y/N)?
```

To delete all of the files in the current directory, press **Y** and then press ENTER. To cancel the deletion, press **N** and then press ENTER.

> **Note**
>
> Before you use wildcard characters with the **del** command, use the same wildcard characters with the **dir** command to list all the files that will be deleted.

Examples

To delete all the files in a folder named Test on drive C, type either of the following:

```
del c:\test
del c:\test\*.*
```

To delete all the files in a folder where the folder has a space in its name, the full path needs to be wrapped in double quotes. Type either of the following:

```
del "c:\test folder\"
del "c:\test folder\*.*"
```

To delete all files with the .bat file name extension from the current directory, type:

```
del *.bat
```

To delete all read-only files in the current directory, type:

```
del /a:r *.*
```

Related links

- Command-Line Syntax Key
- Windows Recovery Environment (WinRE)

dfsdiag

Article • 02/03/2023

Provides diagnostic information for DFS Namespaces.

Syntax

```
dfsdiag /testdcs [/domain:<domain name>]
dfsdiag /testsites </machine:<server name>| /DFSPath:<namespace root or DFS
folder> [/recurse]> [/full]
dfsdiag /testdfsconfig /DFSRoot:<namespace>
dfsdiag /testdfsintegrity /DFSRoot:<DFS root path> [/recurse] [/full]
dfsdiag /testreferral /DFSpath:<DFS path to get referrals> [/full]
```

Parameters

Parameter	Description
dfsdiag testdcs	Checks domain controller configuration.
dfsdiag testsites	Checks site associations.
dfsdiag testdfsconfig	Checks DFS Namespace configuration.
dfsdiag testdfsintegrity	Checks DFS Namespace integrity.
dfsdiag testreferral	Checks referral responses.
/?	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

dfsdiag testdcs

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Checks the configuration of domain controllers by performing the following tests on each domain controller in the specified domain:

- Verifies that the Distributed File System (DFS) Namespace service is running and that its startup type is set to **Automatic**.
- Checks for the support of site-costed referrals for NETLOGON and SYSvol.
- Verifies the consistency of the site association by hostname and IP address.

Syntax

```
dfsdiag /testdcs [/domain:<domain_name>]
```

Parameters

Parameter	Description
/domain:`<domain_name>`	Name of the domain to check. This parameter is optional. The default value is the local domain to which the local host is joined.

Examples

To verify the configuration of domain controllers in the *contoso.com* domain, type:

```
dfsdiag /testdcs /domain:contoso.com
```

Related links

- Command-Line Syntax Key
- dfsdiag command

dfsdiag testdfsconfig

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Checks the configuration of a Distributed File System (DFS) namespace by performing the following actions:

- Verifies that the DFS Namespace service is running and that its startup type is set to **Automatic** on all namespace servers.
- Verifies that the DFS registry configuration is consistent among namespace servers.
- Validates the following dependencies on clustered namespace servers:
  - Namespace root resource dependency on network name resource.
  - Network name resource dependency on IP address resource.
  - Namespace root resource dependency on physical disk resource.

Syntax

```
dfsdiag /testdfsconfig /DFSroot:<namespace>
```

Parameters

Parameter	Description
/DFSroot:`<namespace>`	The namespace (DFS root) to diagnose.

Examples

To verify the configuration of Distributed File System (DFS) namespaces in *contoso.com\MyNamespace*, type:

```
```

```
dfsdiag /testdfsconfig /DFSroot:\\contoso.com\MyNamespace
```

Related links

- Command-Line Syntax Key
- dfsdiag command

dfsdiag testdfsintegrity

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Checks the integrity of the Distributed File System (DFS) namespace by performing the following tests:

- Checks for DFS metadata corruption or inconsistencies between domain controllers.
- Validates the configuration of access-based enumeration to ensure that it is consistent between DFS metadata and the namespace server share.
- Detects overlapping DFS folders (links), duplicate folders, and folders with overlapping folder targets.

Syntax

```
dfsdiag /testdfsintegrity /DFSroot: <DFS root path> [/recurse] [/full]
```

Parameters

Parameter	Description
/DFSroot: `<DFS root path>`	The DFS namespace to diagnose.
/recurse	Performs the testing, including any namespace interlinks.
/full	Verifies the consistency of the share and NTFS ACLs, along with the client side configuration on all folder targets. It also verifies that the online property is set.

Examples

To verify the integrity and consistency of the Distributed File System (DFS) namespaces in *contoso.com\MyNamespace*, including any interlinks, type:

```
dfsdiag /testdfsintegrity /DFSRoot:\contoso.com\MyNamespace /recurse /full
```

Related links

- Command-Line Syntax Key
- dfsdiag command

dfsdiag testreferral

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Checks Distributed File System (DFS) referrals by performing the following tests:

- If you use the **DFSpath*** parameter without arguments, the command validates that the referral list includes all trusted domains.
- If you specify a domain, the command performs a health check of domain controllers (`dfsdiag /testdcs`) and tests the site associations and domain cache of the local host.
- If you specify a domain and \SYSvol or \NETLOGON, the command performs the same domain controller health checks, along with checking that the time **To Live (TTL)** of SYSvol or NETLOGON referrals matches the default value of 900 seconds.
- If you specify a namespace root, the command performs the same domain controller health checks, along with performing a DFS configuration check (`dfsdiag /testdfsconfig`) and a namespace integrity check (`dfsdiag /testdfsintegrity`).
- If you specify a DFS folder (link), the command performs the same namespace root health checks, along with validating the site configuration for folder targets (dfsdiag /testsites) and validating the site association of the local host.

Syntax

```
dfsdiag /testreferral /DFSpath:<DFS path to get referrals> [/full]
```

Parameters

Parameter	Description

Parameter	Description
/DFSpath:`<path to get referrals>`	Can be one of the following: • **Blank:** Tests only trusted domains. • `\\Domain:` Tests only domain controller referrals. • `\\Domain\SYSvol:` Tests only SYSvol referrals. • `\\Domain\NETLOGON:` Tests only NETLOGON referrals. • `\\<domain or server>\<namespace root>:` Tests only namespace root referrals. • `\\<domain or server>\<namespace root>\<DFS folder>:` Tests only the DFS folder (link) referrals.
/full	Applies only to Domain and Root referrals. Verifies the consistency of site association information between the registry and active directory Domain Services (AD DS).

Examples

To check the Distributed File System (DFS) referrals in *contoso.com\MyNamespace*, type:

```
dfsdiag /testreferral /DFSpath:\\contoso.com\MyNamespace
```

To check the Distributed File System (DFS) referrals in all trusted domains, type:

```
dfsdiag /testreferral /DFSpath:
```

Related links

- Command-Line Syntax Key
- dfsdiag command

dfsdiag testsites

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Checks the configuration of active directory Domain Services (AD DS) sites by verifying that servers that act as namespace servers or folder (link) targets have the same site associations on all domain controllers.

Syntax

```
dfsdiag /testsites </machine:<server name>| /DFSpath:<namespace root or DFS folder> [/recurse]> [/full]
```

Parameters

Parameter	Description
`/machine:<server name>`	The name of the server on which to verify the site association.
`/DFSpath:<namespace root or DFS folder>`	The namespace root or Distributed File System (DFS) folder (link) with targets for which to verify the site association.
/recurse	Enumerates and verifies the site associations for all folder targets under the specified namespace root.
/full	Verifies that AD DS and the registry of the server contain the same site association information.

Examples

To check the site associations on *machine\MyServer*, type:

```
dfsdiag /testsites /machine:MyServer
```

To check a Distributed File System (DFS) folder to verify the site association, along with verifying that AD DS and the registry of the server contain the same site association information, type:

```
dfsdiag /TestSites /DFSpath:\\contoso.com\namespace1\folder1 /full
```

To check a namespace root to verify the site association, along with enumerating and verifying the site associations for all folder targets under the specified namespace root, and verifying that AD DS and the registry of the server contain the same site association information, type:

```
dfsdiag /testsites /DFSpath:\\contoso.com\namespace2 /recurse /full
```

Related links

- Command-Line Syntax Key
- dfsdiag command

dfsrmig

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

The migration tool for the DFS Replication service, dfsrmig.exe, is installed with the DFS Replication service. This tool migrates SYSvol replication from File Replication Service (FRS) to Distributed File System (DFS) Replication. It also provides information about the progress of the migration and modifies Active Directory Domain Services (AD DS) objects to support the migration.

Syntax

```
dfsrmig [/setglobalstate <state> | /getglobalstate | /getmigrationstate |
/createglobalobjects |
/deleterontfrsmember [<read_only_domain_controller_name>] |
/deleterodfsrmember [<read_only_domain_controller_name>] | /?]
```

Parameters

Parameter	Description
`/setglobalstate <state>`	Sets the domain's global migration state to one that corresponds to the value specified by *state*. You can only set the global migration state to a stable state. The *state* values include: • **0** - Start state • **1** - Prepared state • **2** - Redirected state • **3** - Eliminated state
/getglobalstate	Retrieves the current global migration state for the domain from the local copy of the AD DS database, when run on the PDC emulator. Use this option to confirm that you set the correct global migration state. **Important:** You should only run this command on the PDC emulator.

Parameter	Description
/getmigrationstate	Retrieves the current local migration state for all domain controllers in the domain and determines whether those local states match the current global migration state. Use this option to determine if all domain controllers have reached the global migration state.
/createglobalobjects	Creates the global objects and settings in AD DS used by DFS Replication uses. The only situations where you should use this option to manually create objects and settings, are: • **A new read-only domain controller is promoted during migration**. If a new read-only domain controller is promoted in the domain after moving into the **Prepared** state, but before migration to the **Eliminated** state, then the objects that correspond to the new domain controller aren't created, causing replication and the migration to fail. • **Global settings for the DFS Replication service are missing or were deleted**. If these settings are missing for a domain controller, migration from the **Start** state to the **Prepared** state will stall at the **Preparing** transition state. **Note:** Because the global AD DS settings for the DFS Replication service for a read-only domain controller are created on the PDC emulator, these settings need to replicate to the read-only domain controller from the PDC emulator before the DFS Replication service on the read-only domain controller can use these settings. Because of Active Directory replication latencies, this replication can take some time to occur.

Parameter	Description
`/deleterontfrsmember [<read_only_domain_controller_name>]`	Deletes the global AD DS settings for FRS replication that correspond to the specified read-only domain controller, or deletes the global AD DS settings for FRS replication for all read-only domain controllers if no value is specified for `<read_only_domain_controller_name>`. You shouldn't need to use this option during a normal migration process, because the DFS Replication service automatically deletes these AD DS settings during the migration from the **Redirected** state to the **Eliminated** state. Use this option to manually delete the AD DS settings only when the automatic deletion fails on a read-only domain controller and stalls the read-only domain controller for a long time during the migration from the **Redirected** state to the **Eliminated** state.
`/deleterodfsrmember [<read_only_domain_controller_name>]`	Deletes the global AD DS settings for DFS Replication that correspond to the specified read-only domain controller, or deletes the global AD DS settings for DFS Replication for all read-only domain controllers if no value is specified for `<read_only_domain_controller_name>`. Use this option to manually delete the AD DS settings only when the automatic deletion fails on a read-only domain controller and stalls the read-only domain controller for a long time when rolling back the migration from the Prepared state to the start state.
/?	Displays help at the command prompt.

Remarks

- Use the `/setglobalstate <state>` command to set the global migration state in AD DS on the PDC emulator to initiate and control the migration process. If the PDC emulator isn't available, this command fails.
- Migration to the **Eliminated** state is irreversible and rollback isn't possible, so use a value of **3** for *state* only when you are fully committed to using DFS Replication for SYSvol replication.
- Global migration states must be a stable migration state.

- Active Directory replication replicates the global state to other domain controllers in the domain, but because of replication latencies, you can get inconsistencies if you run `dfsrmig /getglobalstate` on a domain controller other than the PDC emulator.
- The output of `dfsrmig /getmigrationstate` indicates whether migration to the current global state is complete, listing the local migration state for any domain controllers that haven't yet reached the current global migration state. The local migration state for domain controllers can also include transition states for domain controllers that have not reached the current global migration state.
- Read-only domain controllers can't delete settings from AD DS, the PDC emulator performs this operation, and the changes eventually replicate to the read-only domain controllers after the applicable latencies for active directory replication.
- The **dfsrmig** command is supported only on domain controllers that run at the Windows Server domain functional level, because SYSvol migration from FRS to DFS Replication is only possible on domain controllers that operate at that level.
- You can run the **dfsrmig** command on any domain controller, but operations that create or manipulate AD DS objects are only allowed on read-write capable domain controllers (not on read-only domain controllers).

Examples

To set the global migration state to Prepared (**1**) and to initiate migration or to rollback from the Prepared state, type:

```
dfsrmig /setglobalstate 1
```

To set the global migration state to Start (**0**) and to initiate rollback to the Start state, type:

```
dfsrmig /setglobalstate 0
```

To display the global migration state, type:

```
```

```
dfsrmig /getglobalstate
```

Output from the `dfsrmig /getglobalstate` command:

```
Current DFSR global state: Prepared
Succeeded.
```

To display information about whether the local migration states on all the domain controllers match the global migration state and if there are any local migration states where the local state doesn't match the global state, type:

```
dfsrmig /GetMigrationState
```

Output from the `dfsrmig /getmigrationstate` command when the local migration states on all of the domain controllers match the global migration state:

```
All Domain Controllers have migrated successfully to Global state
(Prepared).
Migration has reached a consistent state on all Domain Controllers.
Succeeded.
```

Output from the `dfsrmig /getmigrationstate` command when the local migration states on some domain controllers don't match the global migration state.

```
The following Domain Controllers are not in sync with Global state
(Prepared):
Domain Controller (Local Migration State) DC type
=========
CONTOSO-DC2 (start) ReadOnly DC
CONTOSO-DC3 (Preparing) Writable DC
Migration has not yet reached a consistent state on all domain controllers
State information might be stale due to AD latency.
```

To create the global objects and settings that DFS Replication uses in AD DS on domain controllers where those settings were not created automatically during migration or where those settings are missing, type:

```
dfsrmig /createglobalobjects
```

To delete the global AD DS settings for FRS replication for a read-only domain controller named contoso-dc2 if those settings were not deleted automatically by the migration process, type:

```
dfsrmig /deleterontfrsmember contoso-dc2
```

To delete the global AD DS settings for FRS replication for all read-only domain controllers if those settings were not deleted automatically by the migration process, type:

```
dfsrmig /deleterontfrsmember
```

To delete the global AD DS settings for DFS Replication for a read-only domain controller named contoso-dc2 if those settings were not deleted automatically by the migration process, type:

```
dfsrmig /deleterodfsrmember contoso-dc2
```

To delete the global AD DS settings for DFS Replication for all read-only domain controllers if those settings were not deleted automatically by the migration process, type:

```
dfsrmig /deleterodfsrmember
```

To display help at the command prompt:

```
dfsrmig
```

```
dfsrmig /?
```

Related links

- Command-Line Syntax Key
- SYSvol Migration Series: Part 2 dfsrmig.exe: The SYSvol Migration Tool
- Active Directory Domain Services

dfsutil

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

The dfsutil command manages DFS Namespaces, servers, and clients.

Functionality available in PowerShell

The DFSN PowerShell module provides equivalent functionality to the following dfsutil parameters.

Expand table

Parameter	Description
root	Displays, creates, removes, imports, exports namespace roots.
link	Displays, creates, removes, or moves folders (links).
target	Displays, create, remove folder target or namespace server.
property	Displays or modifies a folder target or namespace server.
server	Displays or modifies namespace configuration.
domain	Displays all domain-based namespaces in a domain.

Functionality available only in dfsutil

The following functionality is available only as dfsutil parameters:

Expand table

Parameter	Description
client	Displays or modifies client information or registry keys.
diag	Perform diagnostics or view dfsdirs/dfspath.
cache	Displays or flushes the client cache.

For more info about each of these commands, open a command prompt on a server with the DFS Namespaces management tools installed, and then type `dfsutil client /?`, `dfsutil diag /?`, or `dfsutil cache /?`.

Related links

- Command-Line Syntax Key

Feedback

Was this page helpful? Yes No

diantz

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Package existing files into a cabinet (.cab) file. This command performs the same actions as the updated makecab command.

Syntax

```
diantz [/v[n]] [/d var=<value> ...] [/l <dir>] <source> [<destination>]
diantz [/v[<n>]] [/d var=<value> ...] /f <directives_file> [...]
```

Parameters

Parameter	Description
`<source>`	File to compress.
`<destination>`	File name to give compressed file. If omitted, the last character of the source file name is replaced with an underscore (_) and used as the destination.
/f `<directives_file>`	A file with **diantz** directives (may be repeated).
/d var=`<value>`	Defines variable with specified value.
/l `<dir>`	Location to place destination (default is current directory).
/v[`<n>`]	Set debugging verbosity level (0=none,...,3=full).
/?	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- Microsoft Cabinet format

dir

Article • 02/03/2023

Displays a list of a directory's files and subdirectories. If used without parameters, this command displays the disk's volume label and serial number, followed by a list of directories and files on the disk (including their names and the date and time each was last modified). For files, this command displays the name extension and the size in bytes. This command also displays the total number of files and directories listed, their cumulative size, and the free space (in bytes) remaining on the disk.

The **dir** command can also run from the Windows Recovery Console, using different parameters. For more information, see Windows Recovery Environment (WinRE).

Syntax

```
dir [<drive>:][<path>][<filename>] [...] [/p] [/q] [/w] [/d] [/a[[:]
<attributes>]][/o[[:]<sortorder>]] [/t[[:]<timefield>]] [/s] [/b] [/l] [/n]
[/x] [/c] [/4] [/r]
```

Parameters

Parameter	Description
`[<drive>:]` `[<path>]`	Specifies the drive and directory for which you want to see a listing.
`[<filename>]`	Specifies a particular file or group of files for which you want to see a listing.
/p	Displays one screen of the listing at a time. To see the next screen, press any key.
/q	Displays file ownership information.
/w	Displays the listing in wide format, with as many as five file names or directory names on each line.
/d	Displays the listing in the same format as **/w**, but the files are sorted by column.

Parameter	Description
/a[[:]`<attributes>`]	Displays only the names of those directories and files with your specified attributes. If you don't use this parameter, the command displays the names of all files except hidden and system files. If you use this parameter without specifying any *attributes*, the command displays the names of all files, including hidden and system files. The list of possible *attributes* values are: • **d** - Directories • **h** - Hidden files • **s** - System files • **l** - Reparse points • **r** - Read-only files • **a** - Files ready for archiving • **i** - Not content indexed files You can use any combination of these values, but don't separate your values using spaces. Optionally you can use a colon (:) separator, or you can use a hyphen (-) as a prefix to mean, "not". For example, using the **-s** attribute won't show the system files.
/o[[:]`<sortorder>`]	Sorts the output according to *sortorder*, which can be any combination of the following values: • **n** - Alphabetically by name • **e** - Alphabetically by extension • **g** - Group directories first • **s** - By size, smallest first • **d** - By date/time, oldest first • Use the **-** prefix to reverse the sort order Multiple values are processed in the order in which you list them. Don't separate multiple values with spaces, but you can optionally use a colon (:). If *sortorder* isn't specified, **dir /o** lists the directories alphabetically, followed by the files, which are also sorted alphabetically.
/t[[:]`<timefield>`]	Specifies which time field to display or to use for sorting. The available *timefield* values are: • **c** - Creation • **a** - Last accessed • **w** - Last written
/s	Lists every occurrence of the specified file name within the specified directory and all subdirectories.
/b	Displays a bare list of directories and files, with no additional information. The **/b** parameter overrides **/w**.

Parameter	Description
/l	Displays unsorted directory names and file names, using lowercase.
/n	Displays a long list format with file names on the far right of the screen.
/x	Displays the short names generated for non-8dot3 file names. The display is the same as the display for **/n**, but the short name is inserted before the long name.
/c	Displays the thousand separator in file sizes. This is the default behavior. Use **/-c** to hide separators.
/4	Displays years in four-digit format.
/r	Display alternate data streams of the file.
/?	Displays help at the command prompt.

Remarks

- To use multiple *filename* parameters, separate each file name with a space, comma, or semicolon.
- You can use wildcard characters (***** or **?**), to represent one or more characters of a file name and to display a subset of files or subdirectories.
- You can use the wildcard character, *, to substitute for any string of characters, for example:
  - `dir *.txt` lists all files in the current directory with extensions that begin with .txt, such as .txt, .txt1, .txt_old.
  - `dir read *.txt` lists all files in the current directory that begin with read and with extensions that begin with .txt, such as .txt, .txt1, or .txt_old.
  - `dir read *.*` lists all files in the current directory that begin with read with any extension.

  The asterisk wildcard always uses short file name mapping, so you might get unexpected results. For example, the following directory contains two files (t.txt2 and t97.txt):

```
C:\test>dir /x
Volume in drive C has no label.
```

```
 Volume Serial Number is B86A-EF32

 Directory of C:\test

 11/30/2004  01:40 PM <DIR>  .
 11/30/2004  01:40 PM <DIR> ..
 11/30/2004  11:05 AM 0 T97B4~1.TXT t.txt2
 11/30/2004  01:16 PM 0 t97.txt
```

You might expect that typing `dir t97\*` would return the file t97.txt. However, typing `dir t97\*` returns both files, because the asterisk wildcard matches the file t.txt2 to t97.txt by using its short name map *T97B4~1.TXT*. Similarly, typing `del t97\*` would delete both files.

- You can use the question mark (?) as a substitute for a single character in a name. For example, typing `dir read???.txt` lists any files in the current directory with the .txt extension that begin with read and are followed by up to three characters. This includes Read.txt, Read1.txt, Read12.txt, Read123.txt, and Readme1.txt, but not Readme12.txt.

- If you use **/a** with more than one value in *attributes*, this command displays the names of only those files with all the specified attributes. For example, if you use **/a** with **r** and **-h** as attributes (by using either `/a:r-h` or `/ar-h`), this command will only display the names of the read-only files that aren't hidden.

- If you specify more than one *sortorder* value, this command sorts the file names by the first criterion, then by the second criterion, and so on. For example, if you use **/o** with the **e** and **-s** parameters for *sortorder* (by using either `/o:e-s` or `/oe-s`), this command sorts the names of directories and files by extension, with the largest first, and then displays the final result. The alphabetic sorting by extension causes file names with no extensions to appear first, then directory names, and then file names with extensions.

- If you use the redirection symbol (`>`) to send this command's output to a file, or if you use a pipe (`|`) to send this command's output to another command, you must use `/a:-d` and **/b** to only list the file names. You can use *filename* with **/b** and **/s** to specify that this command is to search the current directory and its subdirectories for all file names that match *filename*. This command lists only the drive letter, directory name, file name, and file name extension (one path per line), for each file name it finds. Before you use a pipe to send this command's output to another command, you should set the *TEMP* environment variable in your Autoexec.nt file.

Examples

To display all directories one after the other, in alphabetical order, in wide format, and pausing after each screen, make sure that the root directory is the current directory, and then type:

```
dir /s/w/o/p
```

The output lists the root directory, the subdirectories, and the files in the root directory, including extensions. This command also lists the subdirectory names and the file names in each subdirectory in the tree.

To alter the preceding example so that **dir** displays the file names and extensions, but omits the directory names, type:

```
dir /s/w/o/p/a:-d
```

To print a directory listing, type:

```
dir > prn
```

When you specify **prn**, the directory list is sent to the printer that is attached to the LPT1 port. If your printer is attached to a different port, you must replace **prn** with the name of the correct port.

You can also redirect output of the **dir** command to a file by replacing **prn** with a file name. You can also type a path. For example, to direct **dir** output to the file dir.doc in the Records directory, type:

```
dir > \records\dir.doc
```

If dir.doc does not exist, **dir** creates it, unless the **Records** directory does not exist. In that case, the following message appears:

```
File creation error
```

To display a list of all the file names with the .txt extension in all directories on drive C, type:

```

dir c:\*.txt /w/o/s/p
```

The **dir** command displays, in wide format, an alphabetized list of the matching file names in each directory, and it pauses each time the screen fills until you press any key to continue.

Related links

- Command-Line Syntax Key

diskcomp

Article • 02/03/2023

Compares the contents of two floppy disks. If used without parameters, **diskcomp** uses the current drive to compare both disks.

Syntax

```
diskcomp [<drive1>: [<drive2>:]]
```

Parameters

Parameter	Description
`<drive1>`	Specifies the drive containing one of the floppy disks.
/?	Displays help at the command prompt.

Remarks

- The **diskcomp** command works only with floppy disks. You cannot use **diskcomp** with a hard disk. If you specify a hard disk drive for *drive1* or *drive2*, **diskcomp** displays the following error message:

  ```
  Invalid drive specification
  Specified drive does not exist
  or is nonremovable
  ```

- If all tracks on the two disks being compared are the same (it ignores a disk's volume number), **diskcomp** displays the following message:

  ```
  Compare OK
  ```

  If the tracks aren't the same, **diskcomp** displays a message similar to the following:

```
Compare error on
side 1, track 2
```

When **diskcomp** completes the comparison, it displays the following message:

```
Compare another diskette (Y/N)?
```

If you press **Y**, **diskcomp** prompts you to insert the disk for the next comparison. If you press **N**, **diskcomp** stops the comparison.

- If you omit the *drive2* parameter, **diskcomp** uses the current drive for *drive2*. If you omit both drive parameters, **diskcomp** uses the current drive for both. If the current drive is the same as *drive1*, **diskcomp** prompts you to swap disks as necessary.

- If you specify the same floppy disk drive for *drive1* and *drive2*, **diskcomp** compares them by using one drive and prompts you to insert the disks as necessary. You might have to swap the disks more than once, depending on the capacity of the disks and the amount of available memory.

- **Diskcomp** can't compare a single-sided disk with a double-sided disk, nor a high-density disk with a double-density disk. If the disk in *drive1* isn't of the same type as the disk in *drive2*, **diskcomp** displays the following message:

  ```
  Drive types or diskette types not compatible
  ```

- **Diskcomp** doesn't work on a network drive or on a drive created by the **subst** command. If you attempt to use **diskcomp** with a drive of any of these types, **diskcomp** displays the following error message:

  ```
  Invalid drive specification
  ```

- If you use **diskcomp** with a disk that you made by using **copy**, **diskcomp** might display a message similar to the following:

```
Compare error on
side 0, track 0
```

This type of error can occur even if the files on the disks are identical. Although **copy** duplicates information, it doesn't necessarily place it in the same location on the destination disk.

- **diskcomp** exit codes:

Exit code	Description
0	Disks are the same
1	Differences were found
3	Hard error occurred
4	Initialization error occurred

To process exit codes that are returned by **diskcomp**, you can use the *ERRORLEVEL* environment variable on the **if** command line in a batch program.

Examples

If your computer has only one floppy disk drive (for example, drive A), and you want to compare two disks, type:

```
diskcomp a: a:
```

Diskcomp prompts you to insert each disk, as needed.

To illustrates how to process a **diskcomp** exit code in a batch program that uses the *ERRORLEVEL* environment variable on the **if** command line:

```
rem Checkout.bat compares the disks in drive A and B
echo off
diskcomp a: b:
if errorlevel 4 goto ini_error
if errorlevel 3 goto hard_error
if errorlevel 1 goto no_compare
if errorlevel 0 goto compare_ok
:ini_error
```

```
echo ERROR: Insufficient memory or command invalid
goto exit
:hard_error
echo ERROR: An irrecoverable error occurred
goto exit
:break
echo You just pressed CTRL+C to stop the comparison
goto exit
:no_compare
echo Disks are not the same
goto exit
:compare_ok
echo The comparison was successful; the disks are the same
goto exit
:exit
```

Related links

- Command-Line Syntax Key

diskcopy

Article • 02/03/2023

Copies the contents of the floppy disk in the source drive to a formatted or unformatted floppy disk in the destination drive. If used without parameters, **diskcopy** uses the current drive for the source disk and the destination disk.

Syntax

```
diskcopy [<drive1>: [<drive2>:]] [/v]
```

Parameters

Parameter	Description
`<drive1>`	Specifies the drive that contains the source disk.
/v	Verifies that the information is copied correctly. This option slows down the copying process.
/?	Displays help at the command prompt.

Remarks

- **Diskcopy** works only with removable disks such as floppy disks, which must be the same type. You cannot use **diskcopy** with a hard disk. If you specify a hard disk drive for *drive1* or *drive2*, **diskcopy** displays the following error message:

  ```
  Invalid drive specification
  Specified drive does not exist or is nonremovable
  ```

  The **diskcopy** command prompts you to insert the source and destination disks and waits for you to press any key on the keyboard before continuing.

  After it copies the disk, **diskcopy** displays the following message:

  ```
  ```

```
Copy another diskette (Y/N)?
```

If you press **Y**, **diskcopy** prompts you to insert source and destination disks for the next copy operation. To stop the **diskcopy** process, press **N**.

If you're copying to an unformatted floppy disk in *drive2*, **diskcopy** formats the disk with the same number of sides and sectors per track as are on the disk in *drive1*. **Diskcopy** displays the following message while it formats the disk and copies the files:

```

Formatting while copying
```

- If the source disk has a volume serial number, **diskcopy** creates a new volume serial number for the destination disk and displays the number when the copy operation is complete.
- If you omit the *drive2* parameter, **diskcopy** uses the current drive as the destination drive. If you omit both drive parameters, **diskcopy** uses the current drive for both. If the current drive is the same as *drive1*, **diskcopy** prompts you to swap disks as necessary.
- Run **diskcopy** from a drive other than the floppy disk drive, for example the C drive. If floppy disk *drive1* and floppy disk *drive2* are the same, **diskcopy** prompts you to switch disks. If the disks contain more information than the available memory can hold, **diskcopy** cannot read all of the information at once. **Diskcopy** reads from the source disk, writes to the destination disk, and prompts you to insert the source disk again. This process continues until you have copied the entire disk.
- Fragmentation is the presence of small areas of unused disk space between existing files on a disk. A fragmented source disk can slow down the process of finding, reading, or writing files.

  Because **diskcopy** makes an exact copy of the source disk on the destination disk, any fragmentation on the source disk is transferred to the destination disk. To avoid transferring fragmentation from one disk to another, use the copy command or the xcopy command to copy your disk. Because **copy** and **xcopy** copy files sequentially, the new disk is not fragmented.

  ⓘ **Note**

You cannot use **xcopy** to copy a startup disk.

- **diskcopy** exit codes:

Exit code	Description
0	Copy operation was successful
1	Nonfatal Read/Write error occurred
3	Fatal hard error occurred
4	Initialization error occurred

To process the exit codes that are returned by **diskcomp**, you can use the *ERRORLEVEL* environment variable on the **if** command line in a batch program.

Examples

To copy the disk in drive B to the disk in drive A, type:

```
diskcopy b: a:
```

To use floppy disk drive A to copy one floppy disk to another, first switch to the C drive and then type:

```
diskcopy a: a:
```

Related links

- Command-Line Syntax Key
- xcopy command
- copy command

diskpart

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2, Windows Server 2008

The diskpart command interpreter helps you manage your computer's drives (disks, partitions, volumes, or virtual hard disks).

Before you can use **diskpart** commands, you must first list, and then select an object to give it focus. After an object has focus, any diskpart commands that you type will act on that object.

Determine focus

When you select an object, the focus remains on that object until you select a different object. For example, if the focus is set on disk 0 and you select volume 8 on disk 2, the focus shifts from disk 0 to disk 2, volume 8.

Some commands automatically change the focus. For example, when you create a new partition, the focus automatically switches to the new partition.

You can only give focus to a partition on the selected disk. After a partition has focus, the related volume (if any) also has focus. After a volume has focus, the related disk and partition also have focus if the volume maps to a single specific partition. If this isn't the case, focus on the disk and partition are lost.

Syntax

To start the diskpart command interpreter, at the command prompt type:

Windows Command Prompt

```
diskpart <parameter>
```

> **ⓘ Important**
>
> You must be in your local **Administrators** group, or a group with similar permissions, to run diskpart.

Parameters

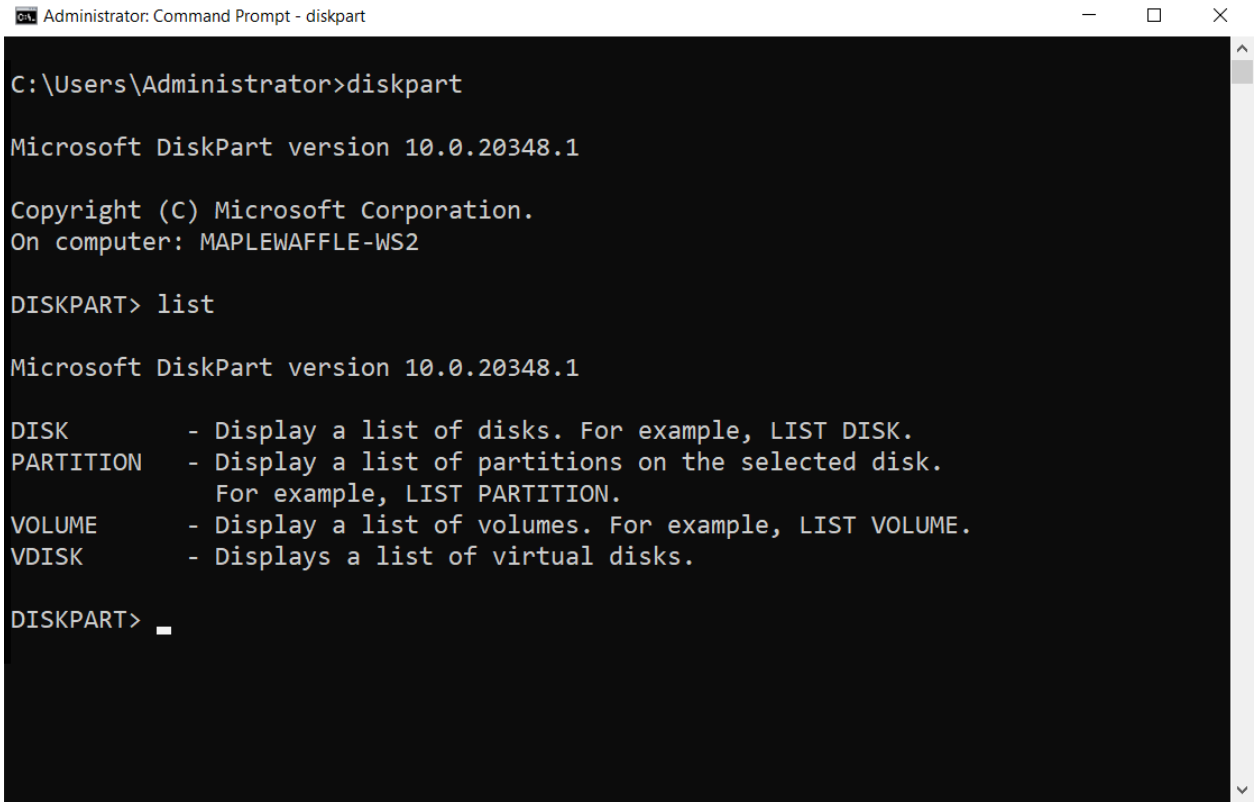
You can run the following commands from the Diskpart command interpreter:

Command	Description
active	Marks the disk's partition with focus, as active.
add	Mirrors the simple volume with focus to the specified disk.
assign	Assigns a drive letter or mount point to the volume with focus.
attach vdisk	Attaches (sometimes called mounts or surfaces) a virtual hard disk (VHD) so that it appears on the host computer as a local hard disk drive.
attributes	Displays, sets, or clears the attributes of a disk or volume.
automount	Enables or disables the automount feature.
break	Breaks the mirrored volume with focus into two simple volumes.
clean	Removes any and all partition or volume formatting from the disk with focus.
compact vdisk	Reduces the physical size of a dynamically expanding virtual hard disk (VHD) file.
convert	Converts file allocation table (FAT) and FAT32 volumes to the NTFS file system, leaving existing files and directories intact.
create	Creates a partition on a disk, a volume on one or more disks, or a virtual hard disk (VHD).
delete	Deletes a partition or a volume.
detach vdisk	Stops the selected virtual hard disk (VHD) from appearing as a local hard disk drive on the host computer.
detail	Displays information about the selected disk, partition, volume, or virtual hard disk (VHD).
exit	Exits the diskpart command interpreter.
expand vdisk	Expands a virtual hard disk (VHD) to the size that you specify.
extend	Extends the volume or partition with focus, along with its file system, into free (unallocated) space on a disk.
filesystems	Displays information about the current file system of the volume with focus and lists the file systems that are supported for formatting the volume.

Command	Description
format	Formats a disk to accept files.
gpt	Assigns the gpt attribute(s) to the partition with focus on basic GUID partition table (gpt) disks.
help	Displays a list of the available commands or detailed help information on a specified command.
import	Imports a foreign disk group into the disk group of the local computer.
inactive	Marks the system partition or boot partition with focus as inactive on basic master boot record (MBR) disks.
list	Displays a list of disks, of partitions in a disk, of volumes in a disk, or of virtual hard disks (VHDs).
merge vdisk	Merges a differencing virtual hard disk (VHD) with its corresponding parent VHD.
offline	Takes an online disk or volume to the offline state.
online	Takes an offline disk or volume to the online state.
recover	Refreshes the state of all disks in a disk group, attempt to recover disks in an invalid disk group, and resynchronizes mirrored volumes and RAID-5 volumes that have stale data.
rem	Provides a way to add comments to a script.
remove	Removes a drive letter or mount point from a volume.
repair	Repairs the RAID-5 volume with focus by replacing the failed disk region with the specified dynamic disk.
rescan	Locates new disks that may have been added to the computer.
retain	Prepares an existing dynamic simple volume to be used as a boot or system volume.
san	Displays or sets the storage area network (san) policy for the operating system.
select	Shifts the focus to a disk, partition, volume, or virtual hard disk (VHD).
set id	Changes the partition type field for the partition with focus.
shrink	Reduces the size of the selected volume by the amount you specify.
uniqueid	Displays or sets the GUID partition table (GPT) identifier or master boot record (MBR) signature for the disk with focus.

Listing available objects

You can view a list of options associated to each command by running the main command followed by what is available to that specific command. Running **list** by itself will display the four parameters below:



> ⓘ Note
>
> After you run the **list** command, an asterisk (*) appears next to the object of focus.

Examples

To see available disk(s), run **list disk**:

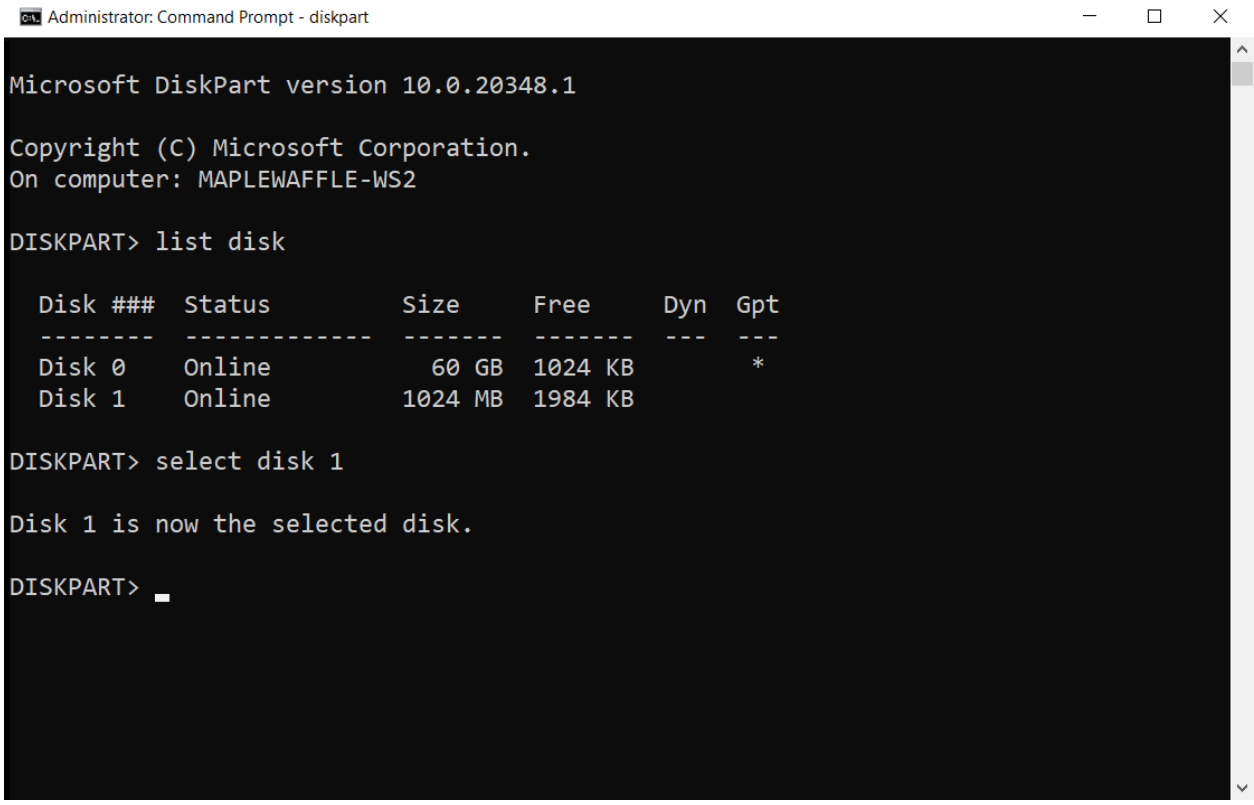
Windows Command Prompt

```
list disk
```

To select a disk, run **select disk** followed by the disk number. For example:

Windows Command Prompt

```
select disk 1
```



Before disk 1 can be utilized, a partition will need to be created by running **create partition primary**:

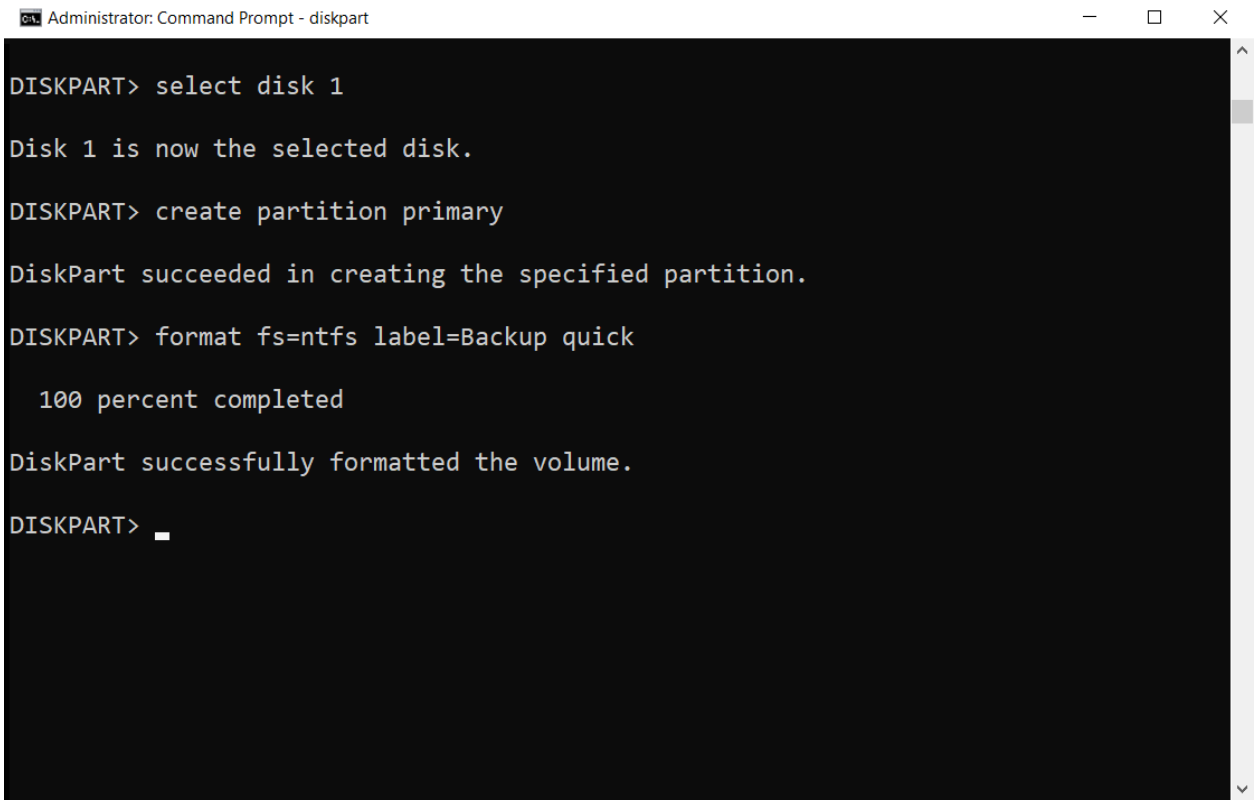
Windows Command Prompt

```
create partition primary
```

Lastly, we can perform a quick format of disk 1 to NTFS with the label "Backup" by running **format fs=ntfs label=Backup quick** as seen below:

Windows Command Prompt

```
format fs=ntfs label=Backup quick
```



Related links

- Command-Line Syntax Key
- Disk management overview
- Storage Cmdlets in Windows PowerShell

diskpart scripts and examples

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Use `diskpart /s` to run scripts that automate disk-related tasks, such as creating volumes or converting disks to dynamic disks. Scripting these tasks is useful if you deploy Windows by using unattended Setup or the Sysprep tool, which do not support creating volumes other than the boot volume.

To create a diskpart script, create a text file that contains the Diskpart commands that you want to run, with one command per line, and no empty lines. You can start a line with `rem` to make the line a comment. For example, here's a script that wipes a disk and then creates a 300 MB partition for the Windows Recovery Environment:

```
select disk 0
clean
convert gpt
create partition primary size=300
format quick fs=ntfs label=Windows RE tools
assign letter=T
```

Examples

- To run a diskpart script, at the command prompt, type the following command, where *scriptname* is the name of the text file that contains your script:

```
diskpart /s scriptname.txt
```

- To redirect diskpart's scripting output to a file, type the following command, where *logfile* is the name of the text file where diskpart writes its output:

```
diskpart /s scriptname.txt > logfile.txt
```

Remarks

- When using the **diskpart** command as a part of a script, we recommend that you complete all of the diskpart operations together as part of a single diskpart script. You can run consecutive diskpart scripts, but you must allow at least 15 seconds between each script for a complete shutdown of the previous execution before running the **diskpart** command again in successive scripts. Otherwise, the successive scripts might fail. You can add a pause between consecutive diskpart scripts by adding the `timeout /t 15` command to your batch file along with your diskpart scripts.
- When diskpart starts, the diskpart version and computer name display at the command prompt. By default, if diskpart encounters an error while attempting to perform a scripted task, diskpart stops processing the script and displays an error code (unless you specified the **noerr** parameter). However, diskpart always returns errors when it encounters syntax errors, regardless of whether you used the **noerr** parameter. The **noerr** parameter enables you to perform useful tasks such as using a single script to delete all partitions on all disks regardless of the total number of disks.

Related links

- Command-Line Syntax Key
- Sample: Configure UEFI/GPT-Based Hard Drive Partitions by Using Windows PE and DiskPart
- Sample: Configure BIOS/MBR-Based Hard Disk Partitions by Using Windows PE and DiskPart
- Storage Cmdlets in Windows PowerShell

Feedback

Was this page helpful? Yes No

active

Article • 02/03/2023

On basic disks, marks the partition with focus as active. Only partitions can be marked as active. A partition must be selected for this operation to succeed. Use the **select partition** command to select a partition and shift the focus to it.

> **⊗ Caution**
>
> DiskPart only informs the basic input/output system (BIOS) or Extensible Firmware Interface (EFI) that the partition or volume is a valid system partition or system volume, and is capable of containing the operating system startup files. DiskPart does not check the contents of the partition. If you mistakenly mark a partition as active and it does not contain the operating system startup files, your computer might not start.

Syntax

```
active
```

Examples

To mark the partition with focus as the active partition, type:

```
active
```

Related links

- Command-Line Syntax Key
- select partition command

add

Article • 10/16/2023

Mirrors the simple volume with focus to the specified active disk.

> **Note**
>
> This DiskPart command isn't available in any edition of Windows Vista.

Syntax

```
add disk=<n> [align=<n>] [wait] [noerr]
```

Parameters

Parameter	Description
disk=`<n>`	Specifies a disk, other than the one containing the existing simple volume, to contain the mirror. You can mirror only simple volumes. The specified disk must have unallocated space at least as large as the size of the simple volume you want to mirror.
align=`<n>`	Typically used with hardware RAID Logical Unit Number (LUN) arrays to improve performance. Aligns all volume or partition extents to the closest alignment boundary. `n` is the number of kilobytes (KB) from the beginning of the disk to the closest alignment boundary.
wait	Waits for the volume to finish synchronizing with the added disk before returning. Without this parameter, DiskPart returns after the mirrored volume is created and doesn't wait for the synchronization to complete.
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error didn't occur. Without this parameter, an error causes DiskPart to exit with an error code.

Remarks

- A volume must be selected for this operation to succeed. Use the select volume command to select a volume and shift the focus to it.

Examples

To create a mirror of the volume with focus on disk 2, type:

```
add disk=2
```

Related links

- Command-Line Syntax Key

assign

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Assigns a drive letter or mount point to the volume with focus. You can also use this command to change the drive letter associated with a removable drive. If no drive letter or mount point is specified, the next available drive letter is assigned. If the drive letter or mount point is already in use, an error is generated.

A volume must be selected for this operation to succeed. Use the **select volume** command to select a volume and shift the focus to it.

> **Important**
>
> You can't assign drive letters to system volumes, boot volumes, or volumes that contain the paging file. In addition, you cannot assign a drive letter to an Original Equipment Manufacturer (OEM) partition or any GUID Partition Table (gpt) partition other than a basic data partition.

Syntax

```
assign [{letter=<d> | mount=<path>}] [noerr]
```

Parameters

Parameter	Description
`letter=<d>`	The drive letter you want to assign to the volume.
`mount=<path>`	The mount point path you want to assign to the volume. For instructions about how to use this command, see Assign a mount point folder path to a drive.
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To assign the letter E to the volume in focus, type:

```
assign letter=e
```

Related links

- Command-Line Syntax Key
- select volume command

attach vdisk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Attaches (sometimes called mounts or surfaces) a virtual hard disk (VHD) so that it appears on the host computer as a local hard disk drive. If the VHD already has a disk partition and file system volume when you attach it, the volume inside the VHD is assigned a drive letter.

> **ⓘ Important**
>
> You must choose and detach a VHD for this operation to succeed. Use the **select vdisk** command to select a VHD and shift the focus to it.

Syntax

```
attach vdisk [readonly] { [sd=<SDDL>] | [usefilesd] } [noerr]
```

Parameters

Parameter	Description
readonly	Attaches the VHD as read-only. Any write operation returns an error.

Parameter	Description
`sd=<SDDL string>`	Sets the user filter on the VHD. The filter string must be in the Security Descriptor Definition Language (SDDL) format. By default the user filter allows access like on a physical disk. SDDL strings can be complex, but in its simplest form, a security descriptor that protects access is known as a discretionary access control list (DACL). It uses the form: `D:<dacl_flags><string_ace1><string_ace2>`... `<string_acen>` Common DACL flags are: • **A**. Allow access • **D**. Deny access Common rights are: • **GA**. All access • **GR**. Read access • **GW**. Write access Common user accounts are: • **BA**. Built in administrators • **AU**. Authenticated users • **CO**. Creator owner • **WD**. Everyone Examples: • **D:P:(A;;GR;;;AU**. Gives read-access to all authenticated users. • **D:P:(A;;GA;;;WD**. Gives everyone full access.
usefilesd	Specifies that the security descriptor on the .vhd file should be used on the VHD. If the **Usefilesd** parameter is not specified, the VHD will not have an explicit security descriptor unless it is specified with the **Sd** parameter.
noerr	Used for scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To attach the selected VHD as read-only, type:

```
attach vdisk readonly
```

Related links

- Command-Line Syntax Key
- select vdisk
- compact vdisk
- detail vdisk
- detach vdisk
- expand vdisk
- merge vdisk
- list

attributes

Article • 02/03/2023

Displays, sets, or clears the attributes of a disk or volume.

Syntax

```
attributes disk
attributes volume
```

Parameters

Parameter	Description
attributes disk	Displays, sets, or clears the attributes of a disk.
attributes volume	Displays, sets, or clears the attributes of a volume.

Related links

- Command-Line Syntax Key

attributes disk

Article • 02/03/2023

Displays, sets, or clears the attributes of a disk. When this command is used to display the current attributes of a disk, the startup disk attribute denotes the disk used to start the computer. For a dynamic mirror, it displays the disk that contains the boot plex of the boot volume.

> **ⓘ Important**
>
> A disk must be selected for the **attributes disk** command to succeed. Use the **select disk** command to select a disk and shift the focus to it.

Syntax

```
attributes disk [{set | clear}] [readonly] [noerr]
```

Parameters

Parameter	Description
set	Sets the specified attribute of the disk with focus.
clear	Clears the specified attribute of the disk with focus.
readonly	Specifies that the disk is read-only.
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To view the attributes of the selected disk, type:

```
attributes disk
```

To set the selected disk as read-only, type:

```
attributes disk set readonly
```

Related links

- Command-Line Syntax Key
- select disk command

attributes volume

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays, sets, or clears the attributes of a volume.

Syntax

```
attributes volume [{set | clear}] [{hidden | readonly | nodefaultdriveletter | shadowcopy}] [noerr]
```

Parameters

Parameter	Description
set	Sets the specified attribute of the volume with focus.
clear	Clears the specified attribute of the volume with focus.
readonly	Specifies that the volume is read-only.
hidden	Specifies that the volume is hidden.
nodefaultdriveletter	Specifies that the volume does not receive a drive letter by default.
shadowcopy	Specifies that the volume is a shadow copy volume.
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Remarks

- On basic master boot record (MBR) disks, the **hidden**, **readonly**, and **nodefaultdriveletter** parameters apply to all volumes on the disk.
- On basic GUID partition table (GPT) disks, and on dynamic MBR and gpt disks, the **hidden**, **readonly**, and **nodefaultdriveletter** parameters apply only to the selected

volume.

- A volume must be selected for the **attributes volume** command to succeed. Use the **select volume** command to select a volume and shift the focus to it.

Examples

To display the current attributes on the selected volume, type:

```
attributes volume
```

To set the selected volume as hidden and read-only, type:

```
attributes volume set hidden readonly
```

To remove the hidden and read-only attributes on the selected volume, type:

```
attributes volume clear hidden readonly
```

Related links

- Command-Line Syntax Key
- select volume command

automount

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

- Command-Line Syntax Key

> **ⓘ Important**
>
> In storage area network (SAN) configurations, disabling automount prevents Windows from automatically mounting or assigning drive letters to any new basic volumes that are visible to the system.

Syntax

automount [{ enable | disable | scrub }] [noerr]

Parameters

Parameter	Description
enable	Enables Windows to automatically mount new basic and dynamic volumes that are added to the system and to assign them drive letters.
disable	Prevents Windows from automatically mounting any new basic and dynamic volumes that are added to the system. **Note**: Disabling automount can cause failover clusters to fail the storage portion of the Validate a Configuration Wizard.
scrub	Removes volume mount point directories and registry settings for volumes that are no longer in the system. This prevents volumes that were previously in the system from being automatically mounted and given their former volume mount point(s) when they are added back to the system.
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To see if the automount feature is enabled, type the following commands from within the diskpart command:

```
automount
```

To enable the automount feature, type:

```
automount enable
```

To disable the automount feature, type:

```
automount disable
```

Related links

- Command-Line Syntax Key
- diskpart commands

break

Article • 02/03/2023

> **Important**
>
> This command is no longer in use. It is included only to preserve compatibility with existing MS-DOS files, but it has no effect at the command line because the functionality is automatic.

Sets or clears extended CTRL+C checking on MS-DOS systems. If used without parameters, **break** displays the existing setting value.

If command extensions are enabled and running on the Windows platform, inserting the **break** command into a batch file enters a hard-coded breakpoint if being debugged by a debugger.

Syntax

```
break=[on|off]
```

> **Note**
>
> Because the break command has no effect, it is often used to create empty files or delete the content of an existing file. For example:

```
rem -- cleans the content of the file --
break>log
```

Related links

- Command-Line Syntax Key
- break command

clean

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes all partitions or volume formatting from the disk with focus.

> **Note**
>
> For a PowerShell version of this command, see **clear-disk command**.

Syntax

```
clean [all]
```

Parameters

Parameter	Description
all	Specifies that each and every sector on the disk is set to zero, which completely deletes all data contained on the disk.

Remarks

- On master boot record (MBR) disks, only the MBR partitioning information and hidden sector information is overwritten.
- On GUID Partition Table (gpt) disks, the gpt partitioning information, including the Protective MBR, is overwritten. There is no hidden sector information.
- A disk must be selected for this operation to succeed. Use the **select disk** command to select a disk and shift the focus to it.

Examples

To remove all formatting from the selected disk, type:

```
clean
```

Related links

- clear-disk command
- Command-Line Syntax Key

compact vdisk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Reduces the physical size of a dynamically expanding virtual hard disk (VHD) file. This parameter is useful because dynamically expanding VHDs increase in size as you add files, but they do not automatically reduce in size when you delete files.

Syntax

```
compact vdisk
```

Remarks

- A dynamically expanding VHD must be selected for this operation to succeed. Use the select vdisk command to select a VHD and shift the focus to it.
- You can only use compact dynamically expanding VHDs that are detached or attached as read-only.

Related links

- Command-Line Syntax Key
- attach vdisk command
- detail vdisk command
- Detach vdisk command
- expand vdisk command
- Merge vdisk command
- select vdisk command
- list command

convert

Article • 02/03/2023

Converts a disk from one disk type to another.

Syntax

```
convert basic
convert dynamic
convert gpt
convert mbr
```

Parameters

Parameter	Description
convert basic command	Converts an empty dynamic disk into a basic disk.
convert dynamic command	Converts a basic disk into a dynamic disk.
convert gpt command	Converts an empty basic disk with the master boot record (MBR) partition style into a basic disk with the GUID partition table (GPT) partition style.
convert mbr command	Converts an empty basic disk with the GUID Partition Table (GPT) partition style into a basic disk with the master boot record (MBR) partition style.

Related links

- Command-Line Syntax Key

convert basic

Article • 02/03/2023

Converts an empty dynamic disk to a basic disk. A dynamic disk must be selected for this operation to succeed. Use the select disk command to select a dynamic disk and shift the focus to it.

> **Important**
>
> The disk must be empty to convert it to a basic disk. Back up your data, and then delete all partitions or volumes before converting the disk.

> **Note**
>
> For instructions regarding how to use this command, see **Change a Dynamic Disk Back to a Basic Disk**).

Syntax

```
convert basic [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To convert the selected dynamic disk to basic, type:

```
convert basic
```

Related links

- Command-Line Syntax Key
- convert command

convert dynamic

Article • 02/03/2023

Converts a basic disk into a dynamic disk. A basic disk must be selected for this operation to succeed. Use the select disk command to select a basic disk and shift the focus to it.

> **Note**
>
> For instructions regarding how to use this command, see **Change a Dynamic Disk Back to a Basic Disk**).

Syntax

```
convert dynamic [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Remarks

- Any existing partitions on the basic disk become simple volumes.

Examples

To convert a basic disk into a dynamic disk, type:

```
convert dynamic
```

Related links

- Command-Line Syntax Key
- convert command

convert gpt

Article • 02/03/2023

Converts an empty basic disk with the master boot record (MBR) partition style into a basic disk with the GUID partition table (GPT) partition style. A basic MBR disk must be selected for this operation to succeed. Use the select disk command to select a basic disk and shift the focus to it.

> **ⓘ Important**
>
> The disk must be empty to convert it to a basic disk. Back up your data, and then delete all partitions or volumes before converting the disk. The required minimum disk size for conversion to GPT is 128 megabytes.

> **ⓘ Note**
>
> For instructions regarding how to use this command, see **Change a Master Boot Record Disk into a GUID Partition Table Disk**.

Syntax

```
convert gpt [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To convert a basic disc from MBR partition style to GPT partition style, type:

```
convert gpt
```

Related links

- Command-Line Syntax Key
- convert command

convert mbr

Article • 02/03/2023

Converts an empty basic disk with the GUID Partition Table (GPT) partition style into a basic disk with the master boot record (MBR) partition style. A basic disk must be selected for this operation to succeed. Use the select disk command to select a basic disk and shift the focus to it.

> **Important**
>
> The disk must be empty to convert it to a basic disk. Back up your data, and then delete all partitions or volumes before converting the disk.

> **Note**
>
> For instructions regarding how to use this command, see **Change a GUID Partition Table Disk into a Master Boot Record Disk**.

Syntax

```
convert mbr [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To convert a basic disc from GPT partition style to MBR partition style, type>:

```
convert mbr
```

Related links

- Command-Line Syntax Key
- convert command

create

Article • 02/03/2023

Creates a partition or shadow on a disk, a volume on one or more disks, or a virtual hard disk (VHD). If you're using this command to create a volume on the shadow disk, you must already have at least one volume in the shadow copy set.

Syntax

```
create partition
create volume
```

Parameters

Parameter	Description
create partition primary command	Creates a primary partition on the basic disk with focus.
create partition efi command	Creates an Extensible Firmware Interface (EFI) system partition on a GUID Partition Table (gpt) disk on Itanium-based computers.
create partition extended command	Creates an extended partition on the disk with focus.
create partition logical command	Creates a logical partition in an existing extended partition.
create partition msr command	Creates a Microsoft Reserved (MSR) partition on a GUID partition table (gpt) disk.
create volume simple command	Creates a simple volume on the specified dynamic disk.
create volume mirror command	Creates a volume mirror by using the two specified dynamic disks.
create volume raid command	Creates a RAID-5 volume using three or more specified dynamic disks.
create volume stripe command	Creates a striped volume using two or more specified dynamic disks.

Related links

- Command-Line Syntax Key

delete

Article • 10/16/2023

Deletes a partition or a volume. It also deletes a dynamic disk from the list of disks.

Syntax

```
delete disk
delete partition
delete volume
```

Parameters

Parameter	Description
Delete disk	Deletes a missing dynamic disk from the list of disks.
Delete partition	Deletes a partition.
Delete volume	Deletes a volume.

Related links

- Command-Line Syntax Key

delete disk

Article • 02/03/2023

Deletes a missing dynamic disk from the list of disks.

> ⓘ Note
>
> For detailed instructions about how to use this command, see **Remove a Missing Dynamic Disk**.

Syntax

```
delete disk [noerr] [override]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.
override	Enables DiskPart to delete all simple volumes on the disk. If the disk contains half of a mirrored volume, the half of the mirror on the disk is deleted. The delete disk override command fails if the disk is a member of a RAID-5 volume.

Examples

To delete a missing dynamic disk from the list of disks, type:

```
delete disk
```

Related links

- Command-Line Syntax Key

- delete command

delete partition

Article • 02/03/2023

Deletes the partition with focus. Before you begin, you must select a partition for this operation to succeed. Use the select partition command to select a partition and shift the focus to it.

> ⚠ **Warning**
>
> Deleting a partition on a dynamic disk can delete all dynamic volumes on the disk, destroying any data and leaving the disk in a corrupt state.
>
> You can't delete the system partition, boot partition, or any partition that contains the active paging file or crash dump information.

Syntax

```
delete partition [noerr] [override]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.
override	Enables DiskPart to delete any partition regardless of type. Typically, DiskPart only permits you to delete known data partitions.

Remarks

- To delete a dynamic volume, always use the delete volume command instead.
- Partitions can be deleted from dynamic disks, but they shouldn't be created. For example, it's possible to delete an unrecognized GUID Partition Table (GPT) partition on a dynamic GPT disk. Deleting such a partition doesn't cause the resulting free space to become available. Instead, This command is intended to

allow you to reclaim space on a corrupted offline dynamic disk in an emergency situation where the clean command in DiskPart can't be used.

Examples

To delete the partition with focus, type:

```
delete partition
```

Related links

- Command-Line Syntax Key
- select partition
- delete command
- delete volume command
- clean command

delete volume

Article • 02/03/2023

Deletes the selected volume. Before you begin, you must select a volume for this operation to succeed. Use the select volume command to select a volume and shift the focus to it.

> **Important**
>
> You can't delete the system volume, boot volume, or any volume that contains the active paging file or crash dump (memory dump).

Syntax

```
delete volume [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To delete the volume with focus, type:

```
delete volume
```

Related links

- Command-Line Syntax Key

- select volume
- delete command

detach vdisk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Stops the selected virtual hard disk (VHD) from appearing as a local hard disk drive on the host computer. When a VHD is detached, you can copy it to other locations. Before you begin, you must select a VHD for this operation to succeed. Use the select vdisk command to select a VHD and shift the focus to it.

Syntax

```
detach vdisk [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To detach the selected VHD, type:

```
detach vdisk
```

Related links

- Command-Line Syntax Key
- attach vdisk command

- compact vdisk command
- detail vdisk command
- expand vdisk command
- Merge vdisk command
- select vdisk command
- list command

detail

Article • 02/03/2023

Displays information about the selected disk, partition, volume, or virtual hard disk (VHD).

Syntax

```
detail disk
detail partition
detail volume
detail vdisk
```

Parameters

Parameter	Description
Detail disk	Displays the properties of the selected disk and the volumes on that disk.
Detail partition	Displays the properties of the selected partition.
Detail volume	Displays the disks on which the current volume resides.
Detail vdisk	Displays the properties of the selected VHD.

Related links

- Command-Line Syntax Key

detail disk

Article • 02/03/2023

Displays the properties of the selected disk and the volumes on that disk. Before you begin, you must select a disk for this operation to succeed. Use the select disk command to select a disk and shift the focus to it. If you select a virtual hard disk (VHD), this command will show the disk's bus type as *Virtual*.

Syntax

```
detail disk
```

Examples

To see the properties of the selected disk, and information about the volumes in the disk, type:

```
detail disk
```

Related links

- Command-Line Syntax Key
- detail command

detail partition

Article • 02/03/2023

Displays the properties of the selected partition. Before you begin, you must select a partition for this operation to succeed. Use the select partition command to select a partition and shift the focus to it.

Syntax

```
detail partition
```

Examples

To see the properties of the selected partition, type:

```
detail partition
```

Related links

- Command-Line Syntax Key
- detail command

detail vdisk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the properties of the selected virtual hard disk (VHD). Before you begin, you must select a VHD for this operation to succeed. Use the select vdisk command to select a VHD and shift the focus to it.

Syntax

```
detail vdisk
```

Examples

To see details about the selected VHD, type:

```
detail vdisk
```

Related links

- Command-Line Syntax Key
- detail command
- attach vdisk command
- compact vdisk command
- detach vdisk command
- expand vdisk command
- merge vdisk command

- select vdisk
- list command

detail volume

Article • 02/03/2023

Displays the disks on which the current volume resides. Before you begin, you must select a volume for this operation to succeed. Use the select volume command to select a volume and shift the focus to it. The volume details aren't applicable to read-only volumes, such as a DVD-ROM or CD-ROM drive.

Syntax

```
detail volume
```

Examples

To see all the disks in which the current volume resides, type:

```
detail volume
```

Related links

- Command-Line Syntax Key
- select volume
- detail command

exit

Article • 10/12/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Exits the command interpreter or the current batch script.

Syntax

```
exit [/b] [<exitcode>]
```

Parameters

Parameter	Description
/b	Exits the current batch script instead of exiting Cmd.exe. If executed from outside a batch script, exits Cmd.exe.
`<exitcode>`	Specifies a numeric number. If **/b** is specified, the ERRORLEVEL environment variable is set to that number. If you are quitting the command interpreter, the process exit code is set to that number.
/?	Displays help at the command prompt.

Examples

To close the command interpreter, type:

```
exit
```

Related links

- Command-Line Syntax Key

expand vdisk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Expands a virtual hard disk (VHD) to a specified size.

A VHD must be selected and detached for this operation to succeed. Use the select vdisk command to select a volume and shift the focus to it.

Syntax

```
expand vdisk maximum=<n>
```

Parameters

Parameter	Description
maximum=`<n>`	Specifies the new size for the VHD in megabytes (MB).

Examples

To expand the selected VHD to 20 GB, type:

```
expand vdisk maximum=20000
```

Related links

- Command-Line Syntax Key
- select vdisk command
- attach vdisk command

- compact vdisk command
- detach vdisk command
- detail vdisk command
- merge vdisk command
- list command

extend

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Extends the volume or partition with focus and its file system into free (unallocated) space on a disk.

Syntax

```
extend [size=<n>] [disk=<n>] [noerr]
extend filesystem [noerr]
```

Parameters

Parameter	Description
size=`<n>`	Specifies the amount of space in megabytes (MB) to add to the current volume or partition. If no size is given, all of the contiguous free space that is available on the disk is used.
disk=`<n>`	Specifies the disk on which the volume or partition is extended. If no disk is specified, the volume or partition is extended on the current disk.
filesystem	Extends the file system of the volume with focus. For use only on disks where the file system was not extended with the volume.
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Remarks

- On basic disks, the free space must be on the same disk as the volume or partition with focus. It must also immediately follow the volume or partition with focus (that is, it must start at the next sector offset).
- On dynamic disks with simple or spanned volumes, a volume can be extended to any free space on any dynamic disk. Using this command, you can convert a simple

dynamic volume into a spanned dynamic volume. Mirrored, RAID-5 and striped volumes cannot be extended.

- If the partition was previously formatted with the NTFS file system, the file system is automatically extended to fill the larger partition and no data loss will occur.
- If the partition was previously formatted with a file system other than NTFS, the command fails with no change to the partition.
- If the partition was not previously formatted with a file system, the partition will still be extended.
- The partition must have an associated volume before it can be extended.

Examples

To extend the volume or partition with focus by 500 megabytes, on disk 3, type:

```
extend size=500 disk=3
```

To extend the file system of a volume after it was extended, type:

```
extend filesystem
```

Related links

- Command-Line Syntax Key

filesystems

Article • 02/03/2023

Displays information about the current file system of the volume with focus and lists the file systems that are supported for formatting the volume.

A volume must be selected for this operation to succeed. Use the select volume command to select a volume and shift the focus to it.

Syntax

```
filesystems
```

Related links

- Command-Line Syntax Key

Format

Article • 09/28/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 11, Windows 10

The **format** command formats a drive to accept Windows files. You must be a member of the Administrators group to format a hard drive.

> **Note**
>
> You can also use the **format** command, with different parameters, from the Recovery Console. For more information about the Recovery Console, see **Windows Recovery Environment (Windows RE)**.

Syntax

```
format volume [/FS:file-system] [/V:label] [/Q] [/L[:state]] [/A:size] [/C]
[/I:state] [/X] [/P:passes] [/S:state]
format volume [/V:label] [/Q] [/F:size] [/P:passes]
format volume [/V:label] [/Q] [/T:tracks /N:sectors] [/P:passes]
format volume [/V:label] [/Q] [/P:passes]
format volume [/Q]
```

Parameters

Parameter	Description
`<volume>`	Specifies the mount point, volume name, or drive letter (followed by a colon) of the drive that you want to format. If you don't specify any of the following command-line options, **format** uses the volume type to determine the default format for the disk.
/FS:`<filesystem>`	Specifies the type of file system (FAT, FAT32, NTFS, exFAT, ReFS, or UDF).
/V:`<label>`	Specifies the volume label. If you omit the **/V** command-line option or use it without specifying a volume label, **format** prompts you for the volume label after the formatting is complete. Use the syntax **/V:** to prevent the prompt for a volume label. If you use a single **format** command to format more than one disk, all of the disks are given the same volume label.

Parameter	Description
/Q	Performs a quick format. Deletes the file table and the root directory of a previously formatted volume, but doesn't perform a sector-by-sector scan for bad areas. You should use the **/Q** command-line option to format only previously formatted volumes that you know are in good condition. **/Q** overrides **/P**.
/C	**NTFS Only**: Files created on the new volume are compressed by default.
/X	Forces the volume to dismount, if necessary, before it's formatted. Any open handles to the volume are no longer be valid.
/R	**NTFS Only**: Files created on the new volume are compressed by default.
/D	UDF 2.50 only. Metadata is duplicated.
/L:`<state>`	NTFS only. Overrides the default size of file record. By default, a nontiered volume is formatted with small size file records and a tiered volume is formatted with large size file records. **/L** and **/L:enable** forces format to use large size file records and **/L:disable** forces format to use small size file records.
/A:`<size>`	Specifies the allocation unit size to use on FAT, FAT32, NTFS, exFAT, or ReFS volumes. If you don't specify *unit size*, it's chosen based on volume size. Default settings are recommended for general use. The following list presents valid values for each type of file system *unit size*: • **FAT and FAT32**: `512`, `1024`, `2048`, `4096`, `8192`, `16K`, `32K`, `64K`. Also `128K` and `256K` for a sector size greater than 512 bytes. • **NTFS**: `512`, `1024`, `2048`, `4096`, `8192`, `16K`, `32K`, `64K`, `128K`, `256K`, `512K`, `1M`, `2M` • **exFAT**: `12`, `1024`, `2048`, `4096`, `8192`, `16K`, `32K`, `64K`, `128K`, `256K`, `512K`, `1M`, `2M`, `4M`, `8M`, `16M`, `32M` • **ReFS**: `4096`, `64K`
/F:`<size>`	Specifies the size of the floppy disk to format. When possible, use this command-line option instead of the **/T** and **/T** command-line options. Windows accepts the following values for size: • `1440` or `1440k` or `1440kb` • `1.44` or `1.44m` or `1.44mb` • `1.44-MB`, `double-sided`, `quadruple-density`, `3.5-inch disk`
/T:`<tracks>`	Specifies the number of tracks on the disk. When possible, use the **/F** command-line option instead. If you use the **/T** option, you must also use the **/N** option. These options together provide an alternative method of specifying the size of the disk that's being formatted. This option isn't valid with the **/F** option.

Parameter	Description
/N:`<sectors>`	Specifies the number of sectors per track. When possible, use the **/F** command-line option instead of **/N**. If you use **/N**, you must also use **/T**. These two options together provide an alternative method of specifying the size of the disk that's being formatted. This option isn't valid with the **/F** option.
/P:`<count>`	Zero every sector on the volume. After that, the volume will be overwritten **count** times using a different random number each time. If **count** is zero, no other overwrites are made after zeroing every sector. This switch is ignored when **/Q** is specified.
/S:`<state>`	Specifies support for short filenames. State is either **enable** or **disable**. Short names are disabled by default.
/TXF:`<state>`	Specifies TxF is enabled/disabled. State is either **enable** or **disable**. TxF is enabled by default
/I:`<state>`	**ReFS Only**: Specifies whether integrity should be enabled on the new volume. State is either **enable** or **disable**. Integrity is enabled on storage that supports data redundancy by default.
/DAX:`<state>`	**NTFS Only**: Enable direct access storage (DAX) mode for this volume. In DAX mode, the volume is accessed via the memory bus, boosting IO performance. A volume can be formatted with DAX mode only if the hardware is DAX capable. State is either **enable** or **disable**. **/DAX** is considered the same as **/DAX:enable**.
/LogSize::`<size>`	**NTFS Only**: Specifies the size for NTFS log file in kilobytes. The minimum supported size is 2MB, so specifying a size smaller than 2MB results in a 2MB log file. Zero indicates the default value. The default value generally depends on the volume size.
/NoRepairLogs	**NTFS Only**: Disables NTFS repair logs. If the **spotfix** flag for chkdsk is specified, then the **/NoReairLogs** parameter doesn't work.
/NoTrim	Skips sending trim (delete notification) during a format.
/DevDrv	**ReFS Only**: Formats the volume as a dev drive. A dev drive or a developer volume is a volume optimized for performance of developer scenarios. Gives administrators control over what mini-filters are attached to this volume.
/SHA256Checksums	**ReFS Only**: Uses SHA-256 in all operations involving checksums.
/Y	Doesn't prompt to force the volume to dismount and assumes an empty label when no label is specified.
/?	Displays help at the command prompt.

Remarks

- The **format** command creates a new root directory and file system for the disk. It can also check for bad areas on the disk, and it can delete all data on the disk. To be able to use a new disk, you must first use this command to format the disk.
- After formatting a floppy disk, **format** displays the following message:

  `Volume label (11 characters, ENTER for none)?`

  To add a volume label, type up to 11 characters (including spaces). If you don't want to add a volume label to the disk, press ENTER.
- When you use the **format** command to format a hard disk, a warning message similar to the following displays:

  ```
  WARNING, ALL DATA ON NON-REMOVABLE DISK
  DRIVE x: WILL BE LOST!
  Proceed with Format (Y/N)? _
  ```

  To format the hard disk, press **Y**. If you don't want to format the disk, press **N**.
- FAT file systems restrict the number of clusters to no more than 65526. FAT32 file systems restrict the number of clusters to between 65527 and 4177917.
- NTFS compression isn't supported for allocation unit sizes above 4096.

  > ⓘ **Note**
  >
  > **Format** will immediately stop processing if it determines that the previous requirements can't be met using the specified cluster size.

- When formatting is complete, **format** displays messages that show the total disk space, the spaces marked as defective, and the space available for your files.
- You can speed up the formatting process by using the **/q** command-line option. Use this option only if there are no bad sectors on your hard disk.
- You shouldn't use the **format** command on a drive that was prepared by using the **subst** command. You can't format disks over a network.
- The following table lists each exit code and a brief description of its meaning.

Exit code	Description
0	The format operation was successful.
1	Incorrect parameters were supplied.
4	A fatal error occurred (which is any error other than 0, 1, or 5).
5	The user pressed N in response to the prompt "Proceed with Format (Y/N)?" to stop the process.

You can check these exit codes by using the ERRORLEVEL environment variable with the **if** batch command.

Examples

To format a new floppy disk in drive A using the default size, type:

```
format a:
```

To perform a quick format operation on a previously formatted floppy disk in drive A, type:

```
format a: /q
```

To format a floppy disk in drive A and assign it the volume label *DATA*, type:

```
format a: /v:DATA
```

Related links

- Command-Line Syntax Key

gpt

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

On basic GUID partition table (gpt) disks, this command assigns the gpt attribute(s) to the partition with focus. Gpt partition attributes give additional information about the use of the partition. Some attributes are specific to the partition type GUID.

You must choose a basic gpt partition for this operation to succeed. Use the select partition command to select a basic gpt partition and shift the focus to it.

> **⊗ Caution**
>
> Changing the gpt attributes might cause your basic data volumes to fail to be assigned drive letters, or to prevent the file system from mounting. We strongly recommend that you don't change the gpt attributes unless you're an original equipment manufacturer (OEM) or an IT professional who's experienced with gpt disks.

Syntax

```
gpt attributes=<n>
```

Parameters

Parameter	Description

Parameter	Description
attributes=`<n>`	Specifies the value for the attribute that you want to apply to the partition with focus. The gpt attribute field is a 64-bit field that contains two subfields. The higher field is interpreted only in the context of the partition ID, while the lower field is common to all partition IDs. Accepted values include: • **0x0000000000000001** - Specifies that the partition is required by the computer to function properly. • **0x8000000000000000** - Specifies that the partition won't receive a drive letter by default when the disk is moved to another computer, or when the disk is seen for the first time by a computer. • **0x4000000000000000** - Hides a partition's volume so it's not detected by the mount manager. • **0x2000000000000000** - Specifies that the partition is a shadow copy of another partition. • **0x1000000000000000** - Specifies that the partition is read-only. This attribute prevents the volume from being written to. For more information about these attributes, see the attributes section at create_PARTITION_PARAMETERS Structure.

Remarks

- The EFI System partition contains only those binaries necessary to start the operating system. This makes it easy for OEM binaries or binaries specific to an operating system to be placed in other partitions.

Examples

To prevent the computer from automatically assigning a drive letter to the partition with focus, while moving a gpt disk, type:

```
gpt attributes=0x8000000000000000
```

Related links

- Command-Line Syntax Key
- select partition command
- create_PARTITION_PARAMETERS Structure

import (diskpart)

Article • 02/03/2023

Imports a foreign disk group into the disk group of the local computer. This command imports every disk that is in the same group as the disk with focus.

> [IMPORTANT] Before you can use this command, you must use the select disk command to select a dynamic disk in a foreign disk group and shift the focus to it.

Syntax

```
import [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To import every disk that is in the same disk group as the disk with focus into the disk group of the local computer, type:

```
import
```

Related links

- Command-Line Syntax Key
- diskpart command

inactive

Article • 02/03/2023

Marks the system partition or boot partition with focus as inactive on basic master boot record (MBR) disks.

An active system or boot partition must be selected for this operation to succeed. Use the select partition command command to select the active partition and shift the focus to it.

> **⊗ Caution**
>
> Your computer might not start without an active partition. Don't mark a system or boot partition as inactive unless you are an experienced user with a thorough understanding of the Windows family of operating systems.
>
> If you're unable to start your computer after marking the system or boot partition as inactive, insert the Windows Setup CD in the CD-ROM drive, restart the computer, and then repair the partition using the **fixmbr** and **fixboot** commands in the Recovery Console.
>
> After you mark the system partition or boot partition as inactive, your computer starts from the next option specified in the BIOS, such as the CD-ROM drive or a Pre-Boot eXecution Environment (PXE).

Syntax

```
inactive
```

Examples

```
inactive
```

Related links

- Command-Line Syntax Key
- select partition command
- Advanced troubleshooting for Windows boot problems

list

Article • 02/03/2023

Displays a list of disks, of partitions in a disk, of volumes in a disk, or of virtual hard disks (VHDs).

Syntax

```
list { disk | partition | volume | vdisk }
```

Parameters

Parameter	Description
disk	Displays a list of disks and information about them, such as their size, amount of available free space, whether the disk is a basic or dynamic disk, and whether the disk uses the master boot record (MBR) or GUID partition table (GPT) partition style.
partition	Displays the partitions listed in the partition table of the current disk.
volume	Displays a list of basic and dynamic volumes on all disks.
vdisk	Displays a list of the VHDs that are attached and/or selected. This command lists detached VHDs if they are currently selected; however, the disk type is set to Unknown until the VHD is attached. The VHD marked with an asterisk (*) has focus.

Remarks

- When listing partitions on a dynamic disk, the partitions might not correspond to the dynamic volumes on the disk. This discrepancy occurs because dynamic disks contain entries in the partition table for the system volume or boot volume (if present on the disk). They also contain a partition that occupies the remainder of the disk in order to reserve the space for use by dynamic volumes.
- The object marked with an asterisk (*) has focus.
- When listing disks, if a disk is missing, its disk number is prefixed with M. For example, the first missing disk is numbered *M0*.

Examples

```
list disk
list partition
list volume
list vdisk
```

Related links

- Command-Line Syntax Key

merge vdisk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Merges a differencing virtual hard disk (VHD) with its corresponding parent VHD. The parent VHD will be modified to include the modifications from the differencing VHD. This command modifies the parent VHD. As a result, other differencing VHDs that are dependent on the parent will no longer be valid.

> **ⓘ Important**
>
> You must choose and detach a VHD for this operation to succeed. Use the **select vdisk** command to select a VHD and shift the focus to it.

Syntax

```
merge vdisk depth=<n>
```

Parameters

Parameter	Description
depth=`<n>`	Indicates the number of parent VHD files to merge together. For example, `depth=1` indicates that the differencing VHD will be merged with one level of the differencing chain.

Examples

To merge a differencing VHD with its parent VHD, type:

```
merge vdisk depth=1
```

Related links

- Command-Line Syntax Key
- attach vdisk command
- compact vdisk command
- detail vdisk command
- detach vdisk command
- expand vdisk command
- select vdisk command
- list command

offline

Article • 02/03/2023

Takes an online disk or volume to the offline state.

Syntax

```
offline disk
offline volume
```

Parameters

Parameter	Description
offline disk	Takes the online disk with focus to the offline state.
offline volume	Takes the online volume with focus to the offline state.

Related links

- Command-Line Syntax Key

offline disk

Article • 02/03/2023

Takes the online disk with focus to the offline state. If a dynamic disk in a disk group is taken offline, the status of the disk changes to **missing** and the group shows a disk that's offline. The missing disk is moved to the invalid group. If the dynamic disk is the last disk in the group, then the status of the disk changes to **offline**, and the empty group is removed.

> **Note**
>
> A disk must be selected for the **offline disk** command to succeed. Use the **select disk** command to select a disk and shift the focus to it.
>
> This command also works on disks in SAN online mode by changing the SAN mode to offline.

Syntax

```
offline disk [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To take the disk with focus offline, type:

```
offline disk
```

Related links

- Command-Line Syntax Key

offline volume

Article • 02/03/2023

Takes the online volume with focus to the offline state.

> **Note**
>
> A volume must be selected for the **offline volume** command to succeed. Use the **select volume** command to select a disk and shift the focus to it.

Syntax

```
offline volume [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To take the disk with focus offline, type:

```
offline volume
```

Related links

- Command-Line Syntax Key

online

Article • 02/03/2023

Takes an offline disk or volume to the online state.

Syntax

```
online disk
online volume
```

Parameters

Parameter	Description
online disk	Takes the offline disk with focus to the online state.
online volume	Takes the offline volume with focus to the online state.

Related links

- Command-Line Syntax Key

online disk

Article • 02/03/2023

Takes the offline disk to the online state. For basic disks, this command attempts to bring online the selected disk and all volumes on that disk. For dynamic disks, this command attempts to bring online all disks that are not marked as foreign on the local computer. It also attempts to bring online all volumes on the set of dynamic disks.

If a dynamic disk in a disk group is brought online and it's the only disk in the group, then the original group is recreated and the disk is moved to that group. If there are other disks in the group and they're online, then the disk is simply added back into the group. If the group of a selected disk contains mirrored or RAID-5 volumes, this command also resynchronizes these volumes.

> **Note**
>
> A disk must be selected for the **online disk** command to succeed. Use the **select disk** command to select a disk and shift the focus to it.

> **Important**
>
> This command will fails if it's used on a read-only disk.

Syntax

```
online disk [noerr]
```

Parameters

For instructions about using this command, see Reactivate a Missing or Offline Dynamic Disk.

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To take the disk with focus online, type:

```
online disk
```

Related links

- Command-Line Syntax Key

online volume

Article • 02/03/2023

Takes the offline volume to the online state. This command works on volumes that have failed, are failing, or are in failed redundancy state.

> **Note**
>
> A volume must be selected for the **online volume** command to succeed. Use the **select volume** command to select a volume and shift the focus to it.

> **Important**
>
> This command will fails if it's used on a read-only disk.

Syntax

```
online volume [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To take the volume with focus online, type:

```
online volume
```

Related links

- Command-Line Syntax Key

recover

Article • 02/03/2023

Recovers readable information from a bad or defective disk. This command reads a file, sector-by-sector, and recovers data from the good sectors. Data in bad sectors is lost. Because all data in bad sectors is lost when you recover a file, you should recover only one file at a time.

Bad sectors reported by the **chkdsk** command were marked as bad when your disk was prepared for operation. They pose no danger, and **recover** does not affect them.

Syntax

```
recover [<drive>:][<path>]<filename>
```

Parameters

Parameter	Description
`[<drive>:][<path>]<filename>`	Specifies the file name (and the location of the file if it is not in the current directory) you want to recover. *Filename* is required and wildcards aren't supported.
/?	Displays help at the command prompt.

Examples

To recover the file *story.txt* in the *fiction* directory on drive D, type:

```
recover d:\fiction\story.txt
```

Related links

- Command-Line Syntax Key

rem

Article • 02/03/2023

Records comments in a script, batch, or config.sys file. If no comment is specified, **rem** adds vertical spacing.

> **Note**
>
> This command is internal to the command-line interpreter, cmd.exe.

Syntax

```
rem [<comment>]
```

Parameters

Parameter	Description
`<comment>`	Specifies a string of characters to include as a comment.
/?	Displays help at the command prompt.

Remarks

- The **rem** command doesn't display comments on the screen. To display comments on the screen, you must include the **echo on** command in your file.
- You can't use a redirection character (`<` or `>`) or pipe (`|`) in a batch file comment.
- Although you can use **rem** without a comment to add vertical spacing to a batch file, you can also use blank lines. Blank lines are ignored when a batch program is processed.

Examples

To add vertical spacing through batch file comments, type:

```
```

```
@echo off
rem  This batch program formats and checks new disks.
rem  It is named Checknew.bat.
rem
rem echo Insert new disk in Drive B.
pause
format b: /v chkdsk b:
```

To include an explanatory comment before the **prompt** command in a config.sys file, type:

```
rem Set prompt to indicate current directory
prompt $p$g
```

To provide a comment about what a script does, type:

```
rem The commands in this script set up 3 drives.
rem The first drive is a primary partition and is
rem assigned the letter D. The second and third drives
rem are logical partitions, and are assigned letters
rem E and F.
create partition primary size=2048
assign d:
create partition extended
create partition logical size=2048
assign e:
create partition logical
assign f:
```

For multi-line comments, use conditional execution:

```
  Rem/||(
    The REM statement evaluates to success,
    so these lines will never be executed.
    Keep in mind that you will need to escape closing parentheses
    within multi-line comment blocks like shown in this example. ^)
  )
```

Related links

- Command-Line Syntax Key

remove

Article • 02/03/2023

Removes a drive letter or mount point from the volume with focus. If the all parameter is used, all current drive letters and mount points are removed. If no drive letter or mount point is specified, then DiskPart removes the first drive letter or mount point it encounters.

The remove command can also be used to change the drive letter associated with a removable drive. You can't remove the drive letters on system, boot, or paging volumes. In addition, you can't remove the drive letter for an OEM partition, any GPT partition with an unrecognized GUID, or any of the special, non-data, GPT partitions such as the EFI system partition.

> **Note**
>
> A volume must be selected for the **remove** command to succeed. Use the **select volume** command to select a disk and shift the focus to it.

Syntax

```
remove [{letter=<drive> | mount=<path> [all]}] [noerr]
```

Parameters

Parameter	Description
letter=`<drive>`	The drive letter to remove.
mount=`<path>`	The mount point path to remove.
all	Removes all current drive letters and mount points.
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To remove the d:\ drive, type:

```
remove letter=d
```

Related links

- Command-Line Syntax Key

repair

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Repairs the RAID-5 volume with focus by replacing the failed disk region with the specified dynamic disk.

A volume in a RAID-5 array must be selected for this operation to succeed. Use the **select volume** command to select a volume and shift the focus to it.

Syntax

```
repair disk=<n> [align=<n>] [noerr]
```

Parameters

Parameter	Description
disk=`<n>`	Specifies the dynamic disk that will replace the failed disk region. Where *n* must have free space greater than or equal to the total size of the failed disk region in the RAID-5 volume.
align=`<n>`	Aligns all volume or partition extents to the closest alignment boundary. Where *n* is the number of kilobytes (KB) from the beginning of the disk to the closest alignment boundary.
noerr	for scripting only. When an error is encountered, DiskPart continues to process commands as if the error didn't occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To replace the volume with focus by replacing it with dynamic disk 4, type:

```
repair disk=4
```

Related links

- Command-Line Syntax Key
- select volume command

rescan

Article • 02/03/2023

Using the diskpart command interpreter, you can locate new disks added to your computer.

Syntax

```
rescan
```

Related links

- Command-Line Syntax Key
- Diskpart command

retain

Article • 02/03/2023

Prepares an existing simple dynamic volume for use as a boot or system volume. If you use a master boot record (MBR) dynamic disk, this command creates a partition entry in the master boot record. If you use a GUID partition table (GPT) dynamic disk, this command creates a partition entry in the GUID partition table.

Syntax

```
retain
```

Related links

- Command-Line Syntax Key

san

Article • 05/04/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays or sets the storage area network (san) policy for the operating system. If used without parameters, the current san policy is displayed.

Syntax

```
san [policy={onlineAll | offlineAll | offlineShared}] [noerr]
```

Parameters

Parameter	Description
policy={onlineAll|offlineAll|offlineShared}]	Sets the san policy for the currently booted operating system. The san policy determines whether a newly discovered disk is brought online or remains offline, and whether it becomes read/write or remains read-only. When a disk is offline, the disk layout can be read, but no volume devices are surfaced through Plug and Play. When offline no file system can be mounted on the disk. When a disk is online, one or more volume devices are installed for the disk. The following parameter can be set: • **onlineAll**. Specifies that all newly discovered disks are online and made read/write. **IMPORTANT:** Specifying **onlineAll** on a server that shares disks could lead to data corruption. Therefore, you shouldn't set this policy if disks are shared among servers unless the server is part of a cluster. • **offlineAll**. Specifies that all newly discovered disks except the startup disk are offline and read-only by default. • **offlineShared**. Specifies that all newly discovered disks that don't reside on a shared bus (such as SCSI and iSCSI) are brought online and made read-write. Disks that are left offline are read-only by default. For more information, see VDS_san_POLICY Enumeration.

Parameter	Description
noerr	Used for scripting only. When an error is encountered, DiskPart continues to process commands as if the error didn't occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To view the current policy, type:

```
san
```

To make all newly discovered disks, except the startup disk, offline and read-only by default, type:

```
san policy=offlineAll
```

Related links

- Command-Line Syntax Key

select commands

Article • 02/03/2023

Shifts the focus to a disk, partition, volume, or virtual hard disk (VHD).

Syntax

```
select disk
select partition
select vdisk
select volume
```

Parameters

Parameter	Description
Select disk	Shifts the focus to a disk.
Select partition	Shifts the focus to a partition.
Select vdisk	Shifts the focus to a VHD.
Select volume	Shifts the focus to a volume.

Remarks

- If a volume is selected with a corresponding partition, the partition will be automatically selected.
- If a partition is selected with a corresponding volume, the volume will be automatically selected.

Related links

- Command-Line Syntax Key

select disk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Selects the specified disk and shifts the focus to it.

Syntax

```
select disk={<n>|<disk path>|system|next}
```

Parameters

Parameter	Description
`<n>`	Specifies the number of the disk to receive focus. You can view the numbers for all the disks on the computer by using the **list disk** command in DiskPart. **NOTE** When configuring systems with multiple disks, don't use **select disk=0** to specify the system disk. The computer may reassign disk numbers when you reboot, and different computers with the same disk configuration can have different disk numbers.
`<disk path>`	Specifies the location of the disk to receive focus, for example, `PCIROOT(0)#PCI(0F02)#atA(C00T00L00)`. To view the location path of a disk, select it and then type **detail disk**.
system	On BIOS computers, this option specifies that disk 0 receives focus. On EFI computers, the disk containing the EFI system partition (ESP), used for the current boot, receives focus. On EFI computers, the command will fail if there's no ESP, if there's more than one ESP, or if the computer is booted from Windows Preinstallation Environment (Windows PE).
next	After a disk is selected, this option iterates over all disks in the disk list. When you run this option, the next disk in the list receives focus.

Examples

To shift the focus to disk 1, type:

```
select disk=1
```

To select a disk by using its location path, type:

```
select disk=PCIROOT(0)#PCI(0100)#atA(C00T00L01)
```

To shift the focus to the system disk, type:

```
select disk=system
```

To shift the focus to the next disk on the computer, type:

```
select disk=next
```

Related links

- Command-Line Syntax Key
- select partition command
- select vdisk command
- select volume command

select partition

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Selects the specified partition and shifts the focus to it. This command can also be used to display the partition that currently has the focus in the selected disk.

Syntax

```
select partition=<n>
```

Parameters

Parameter	Description
partition=`<n>`	The number of the partition to receive the focus. You can view the numbers for all partitions on the disk currently selected by using the **list partition** command in DiskPart.

Remarks

- Before you can select a partition you must first select a disk using the **select disk** command.
    - If no partition number is specified, this option displays the partition that currently has the focus in the selected disk.
    - If a volume is selected with a corresponding partition, the partition is automatically selected.
    - If a partition is selected with a corresponding volume, the volume is automatically selected.

Examples

To shift the focus to *partition 3*, type:

```
select partitition=3
```

To display the partition that currently has the focus in the selected disk, type:

```
select partition
```

Related links

- Command-Line Syntax Key
- create partition efi command
- create partition extended command
- create partition logical command
- create partition msr command
- create partition primary command
- delete partition command
- detail partition command
- select disk command
- select vdisk command
- select volume command

select vdisk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Selects the specified virtual hard disk (VHD) and shifts the focus to it.

Syntax

```
select vdisk file=<full path> [noerr]
```

Parameters

Parameter	Description
file=`<full path>`	Specifies the full path and file name of an existing VHD file.
noerr	Used for scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To shift the focus to the VHD named *c:\test\test.vhd*, type:

```
select vdisk file=c:\test\test.vhd
```

Related links

- Command-Line Syntax Key
- attach vdisk

- compact vdisk
- detach vdisk
- detail vdisk
- expand vdisk
- merge vdisk
- list
- select disk command
- select partition command
- select volume command

select volume

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Selects the specified volume and shifts the focus to it. This command can also be used to display the volume that currently has the focus in the selected disk.

Syntax

```
select volume={<n>|<d>}
```

Parameters

Parameter	Description
`<n>`	The number of the volume to receive the focus. You can view the numbers for all volumes on the disk currently selected by using the **list volume** command in DiskPart.
`<d>`	The drive letter or mount point path of the volume to receive the focus.

Remarks

- If no volume is specified, this command displays the volume that currently has the focus in the selected disk.
- On a basic disk, selecting a volume also gives the focus to the corresponding partition.
    - If a volume is selected with a corresponding partition, the partition will be automatically selected.
    - If a partition is selected with a corresponding volume, the volume will be automatically selected.

Examples

To shift the focus to *volume 2*, type:

```
select volume=2
```

To shift the focus to *Drive C*, type:

```
select volume=c
```

To shift the focus to the volume mounted on a folder named *c:\mountpath*, type:

```
select volume=c:\mountpath
```

To display the volume that currently has the focus in the selected disk, type:

```
select volume
```

Related links

- Command-Line Syntax Key
- add volume command
- attributes volume command
- create volume mirror command
- create volume raid command
- create volume simple command
- create volume stripe command
- delete volume command

- detail volume command
- fsutil volume command
- list volume command
- offline volume command
- onine volume command
- select disk command
- select partition command
- select vdisk command

set id (Diskpart)

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the partition type field for the partition with focus. This command doesn't work on dynamic disks or on Microsoft Reserved partitions.

> **ⓘ Important**
>
> This command is intended for use by original equipment manufacturers (OEMs) only. Changing partition type fields with this parameter might cause your computer to fail or be unable to boot. Unless you are an OEM or experienced with gpt disks, you should not change partition type fields on gpt disks by using this parameter. Instead, always use the **create partition efi** command to create EFI system partitions, the **create partition msr** command to create Microsoft Reserved partitions, and the **create partition primary** command without the ID parameter to create primary partitions on gpt disks.

Syntax

```
set id={ <byte> | <GUID> } [override] [noerr]
```

Parameters

Parameter	Description
`<byte>`	For master boot record (MBR) disks, specifies the new value for the type field, in hexadecimal form, for the partition. Any partition type **byte** can be specified with this parameter except for type 0x42, which specifies an LDM partition. Note that the leading 0x is omitted when specifying the hexadecimal partition type.

Parameter	Description
`<GUID>`	For GUID partition table (gpt) disks, specifies the new GUID value for the type field for the partition. Recognized GUIDs include: • **EFI system partition:** c12a7328-f81f-11d2-ba4b-00a0c93ec93b • **Basic data partition:** ebd0a0a2-b9e5-4433-87c0-68b6b72699c7 Any partition type GUID can be specified with this parameter except the following: • **Microsoft Reserved partition:** e3c9e316-0b5c-4db8-817d-f92df00215ae • **LDM metadata partition on a dynamic disk:** 5808c8aa-7e8f-42e0-85d2-e1e90434cfb3 • **LDM data partition on a dynamic disk:** af9b60a0-1431-4f62-bc68-3311714a69ad • **Cluster metadata partition:** db97dba9-0840-4bae-97f0-ffb9a327c7e1
override	forces the file system on the volume to dismount before changing the partition type. When you run the **set id** command, DiskPart attempts to lock and dismount the file system on the volume. If **override** isn't specified, and the call to lock the file system fails (for example, because there is an open handle), the operation fails. If **override** is specified, DiskPart forces the dismount even if the call to lock the file system fails, and any open handles to the volume will stop being valid.
noerr	Used for scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Remarks

- Other than the limitations previously mentioned, DiskPart doesn't check the validity of the value that you specify (except to ensure that it is a byte in hexadecimal form or a GUID).

Examples

To set the type field to *0x07* and force the file system to dismount, type:

```
set id=0x07 override
```

To set the type field to be a basic data partition, type:

```
set id=ebd0a0a2-b9e5-4433-87c0-68b6b72699c7
```

Related links

- Command-Line Syntax Key

shrink

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

The Diskpart shrink command reduces the size of the selected volume by the amount you specify. This command makes free disk space available from the unused space at the end of the volume.

A volume must be selected for this operation to succeed. Use the **select volume** command to select a volume and shift the focus to it.

> **Note**
>
> This command works on basic volumes, and on simple or spanned dynamic volumes. It doesn't work on original equipment manufacturer (OEM) partitions, Extensible Firmware Interface (EFI) system partitions, or recovery partitions.

Syntax

```
shrink [desired=<n>] [minimum=<n>] [nowait] [noerr]
shrink querymax [noerr]
```

Parameters

Parameter	Description
desired=`<n>`	Specifies the desired amount of space in megabytes (MB) to reduce the size of the volume by.
minimum=`<n>`	Specifies the minimum amount of space in MB to reduce the size of the volume by.
querymax	Returns the maximum amount of space in MB by which the volume can be reduced. This value may change if applications are currently accessing the volume.

Parameter	Description
nowait	Forces the command to return immediately while the shrink process is still in progress.
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Remarks

- You can reduce the size of a volume only if it is formatted using the NTFS file system or if it does not have a file system.
- If a desired amount isn't specified, the volume is reduced by the minimum amount (if specified).
- If a minimum amount isn't specified, the volume is reduced by the desired amount (if specified).
- If neither a minimum amount nor a desired amount is specified, the volume is reduced by as much as possible.
- If a minimum amount is specified, but not enough free space is available, the command fails.

Examples

To reduce the size of the selected volume by the largest possible amount between 250 and 500 megabytes, type:

```
shrink desired=500 minimum=250
```

To display the maximum number of MB that the volume can be reduced by, type:

```
shrink querymax
```

Related links

- Command-Line Syntax Key
- Resize-Partition

uniqueid

Article • 02/03/2023

Displays or sets the GUID partition table (GPT) identifier or master boot record (MBR) signature for the basic or dynamic disk with focus. A basic or dynamic disk must be selected for this operation to succeed. Use the select disk command to select a disk and shift the focus to it.

Syntax

```
uniqueid disk [id={<dword> | <GUID>}] [noerr]
```

Parameters

Parameter	Description
id=`{<dword> | <GUID>}`	For MBR disks, this parameter specifies a 4-byte (DWORD) value in hexadecimal form for the signature. For GPT disks, this parameter specifies a GUID for the identifier.
noerr	For scripting only. When an error occurs, DiskPart continues to process commands as if the error didn't occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To display the signature of the MBR disk with focus, type:

```
uniqueid disk
```

To set the signature of the MBR disk with focus to the DWORD value *5f1b2c36*, type:

```
uniqueid disk id=5f1b2c36
```

To set the identifier of the GPT disk with focus to the GUID value baf784e7-6bbd-4cfb-aaac-e86c96e166ee, type:

```
uniqueid disk id=baf784e7-6bbd-4cfb-aaac-e86c96e166ee
```

Related links

- Command-Line Syntax Key
- select disk command

diskperf

Article • 02/03/2023

The **diskperf** command remotely enables or disables physical or logical disk performance counters on computers running Windows.

Syntax

```
diskperf [-y[d|v] | -n[d|v]] [\\computername]
```

Options

Option	Description
-y	Starts all disk performance counters when the computer restarts.
-yd	Enables disk performance counters for physical drives when the computer restarts.
-yv	Enables disk performance counters for logical drives or storage volumes when the computer restarts.
-n	Disables all disk performance counters when the computer restarts.
-nd	Disable disk performance counters for physical drives when the computer restarts.
-nv	Disable disk performance counters for logical drives or storage volumes when the computer restarts.
`\\ <computername>`	Specifies the name of the computer where you want to enable or disable disk performance counters.
-?	Displays context sensitive help.

Related links

- Command-Line Syntax Key

Diskraid

Article • 02/03/2023

Diskraid is a command-line tool that enables you to configure and manage redundant array of independent (or inexpensive) disks (RAID) storage subsystems.

RAID is typically used on servers to standardize and categorize fault-tolerant disk systems. RAID levels provide various mixes of performance, reliability, and cost. Some servers provide three of the RAID levels: Level 0 (striping), Level 1 (mirroring), and Level 5 (striping with parity).

A hardware RAID subsystem distinguishes physically addressable storage units from one another by using a Logical Unit Number (LUN). A LUN object must have at least one plex, and can have any number of additional plexes. Each plex contains a copy of the data on the LUN object. Plexes can be added to and removed from a LUN object.

Most Diskraid commands operate on a specific host bus adapter (HBA) port, initiator adapter, initiator portal, provider, subsystem, controller, port, drive, LUN, target portal, target, or target portal group. You use the **SELECT** command to select an object. The selected object is said to have focus. Focus simplifies common configuration tasks, such as creating multiple LUNs within the same subsystem.

> ⓘ **Note**
>
> The Diskraid command-line tool works only with storage subsystems that support Virtual Disk Service (VDS).

Diskraid commands

The following commands are available from within the Diskraid tool.

add

Adds an existing LUN to the currently selected LUN, or adds an iSCSI target portal to the currently selected iSCSI target portal group.

Syntax

```
```

```
add plex lun=n [noerr]
add tpgroup tportal=n [noerr]
```

Parameters

Parameter	Description
plex lun=`<n>`	Specifies the LUN number to add as a plex to the currently selected LUN. CAUTION: All data on the LUN being added as a plex will be deleted.
tpgroup tportal=`<n>`	Specifies the iSCSI target portal number to add to the currently selected iSCSI target portal group.
noerr	For scripting only. When an error is encountered, Diskraid continues to process commands as if the error did not occur.

associate

Sets the specified list of controller ports as active for the currently selected LUN (other controller ports are made inactive), or adds the specified controller ports to the list of existing active controller ports for the currently selected LUN, or associates the specified iSCSI target for the currently selected LUN.

Syntax

```
associate controllers [add] <n>[,<n> [,…]]
associate ports [add] <n-m>[,<n-m>[,…]]
associate targets [add] <n>[,<n> [,…]]
```

Parameters

Parameter	Description
controller	Adds to or replaces the list of controllers that are associated with the currently selected LUN. Use only with VDS 1.0 providers.
ports	Adds to or replaces the list of controller ports that are associated with the currently selected LUN. Use only with VDS 1.1 providers.
targets	Adds to or replaces the list of iSCSI targets that are associated with the currently selected LUN. Use only with VDS 1.1 providers.

Parameter	Description
add	**If using VDS 1.0 providers:** Adds the specified controllers to the existing list of controllers associated with the LUN. If this parameter is not specified, the list of controllers replaces the existing list of controllers associated with this LUN. **If using VDS 1.1 providers:** Adds the specified controller ports to the existing list of controller ports associated with the LUN. If this parameter is not specified, the list of controller ports replaces the existing list of controller ports associated with this LUN.
`<n>[,<n>[, ...]]`	Use with the **controllers** or **targets** parameter. Specifies the numbers of the controllers or iSCSI targets to set to active or associate.
`<n-m>[,<n-m>[,…]]`	Use with the **ports** parameter. Specifies the controller ports to set active using a controller number (*n*) and port number (*m*) pair.

Example

To associate and add ports to a LUN that uses a VDS 1.1 provider:

```
DISKRAID> SEL LUN 5
LUN 5 is now the selected LUN.

DISKRAID> ASSOCIATE PORTS 0-0,0-1
Controller port associations changed.
(Controller ports active after this command: Ctlr 0 Port 0, Ctlr 0 Port 1)

DISKRAID> ASSOCIATE PORTS ADD 1-1
Controller port associations changed.
(Controller ports active after this command: Ctlr 0 Port 0, Ctlr 0 Port 1,
Ctlr 1 Port 1)
```

automagic

Sets or clears flags that give hints to providers on how to configure a LUN. Used with no parameters, the **automagic** operation displays a list of flags.

Syntax

```
automagic {set | clear | apply} all <flag=value> [<flag=value> [...]]
```

Parameters

Parameter	Description
set	Sets the specified flags to the specified values.
clear	Clears the specified flags. The **all** keyword clears all the automagic flags.
apply	Applies the current flags to the selected LUN.
`<flag>`	Flags are identified by three-letter acronyms, including: • **FCR** - Fast Crash Recovery Required • **FTL** - Fault Tolerant • **MSR** - Mostly Reads • **MXD** - Maximum drives • **MXS** - Maximum Size Expected • **ORA** - Optimal Read Alignment • **ORS** - Optimal Read Size • **OSR** - Optimize for Sequential Reads • **OSW** - Optimize for Sequential Writes • **OWA** - Optimal Write Alignment • **OWS** - Optimal Write Size • **RBP** - Rebuild Priority • **RBV** - Read Back Verify Enabled • **RMP** - Remap Enabled • **STS** - Strip Size • **WTC** - Write-Through Caching Enabled • **YNK** - Removable

break

Removes the plex from the currently selected LUN. The plex and the data it contained are not retained, and the drive extents may be reclaimed.

> **⊗ Caution**
>
> You must first select a mirrored LUN before using this command. All data on the plex will be deleted. All data contained on the original LUN is not guaranteed to be consistent.

Syntax

```
break plex=<plex_number> [noerr]
```

Parameters

Parameter	Description
plex	Specifies the number of the plex to remove. The plex and the data it contained will not be retained, and the resources used by this plex will be reclaimed. The data contained on the LUN is not guaranteed to be consistent. If you want to retain this plex, use the Volume Shadow Copy Service (VSS).
noerr	For scripting only. When an error is encountered, Diskraid continues to process commands as if the error did not occur.

chap

Sets the Challenge Handshake Authentication Protocol (CHAP) shared secret so that iSCSI initiators and iSCSI targets can communicate with one another.

Syntax

```
chap initiator set secret=[<secret>] [target=<target>]
chap initiator remember secret=[<secret>] target=<target>
chap target set secret=[<secret>] [initiator=<initiatorname>]
chap target remember secret=[<secret>] initiator=<initiatorname>
```

Parameters

Parameter	Description
initiator set	Sets the shared secret in the local iSCSI initiator service used for mutual CHAP authentication when the initiator authenticates the target.
initiator remember	Communicates the CHAP secret of an iSCSI target to the local iSCSI initiator service so that the initiator service can use the secret in order to authenticate itself to the target during CHAP authentication.
target set	Sets the shared secret in the currently selected iSCSI target used for CHAP authentication when the target authenticates the initiator.
target remember	Communicates the CHAP secret of an iSCSI initiator to the current in-focus iSCSI target so that the target can use the secret in order to authenticate itself to the initiator during mutual CHAP authentication.

Parameter	Description
secret	Specifies the secret to use. If empty the secret will be cleared.
target	Specifies a target in the currently selected subsystem to associate with the secret. This is optional when setting a secret on the initiator and leaving it out indicates that the secret will be used for all targets that do not already have an associated secret.
initiatorname	Specifies an initiator iSCSI name to associate with the secret. This is optional when setting a secret on a target and leaving it out indicates that the secret will be used for all initiators that do not already have an associated secret.

create

Creates a new LUN or iSCSI target on the currently selected subsystem, or creates a target portal group on the currently selected target. You can view the actual binding using the **Diskraid list** command.

Syntax

```
create lun simple [size=<n>] [drives=<n>] [noerr]
create lun stripe [size=<n>] [drives=<n, n> [,...]]  [stripesize=<n>]
[noerr]
create lun raid [size=<n>] [drives=<n, n> [,...]] [stripesize=<n>] [noerr]
create lun mirror [size=<n>] [drives=<n, n> [,...]] [stripesize=<n>] [noerr]
create lun automagic size=<n> [noerr]
create target name=<name> [iscsiname=<iscsiname>] [noerr]
create tpgroup [noerr]
```

Parameters

Parameter	Description
simple	Creates a simple LUN.
stripe	Creates a striped LUN.
raid	Creates a striped LUN with parity.
mirror	Creates a mirrored LUN.
automagic	Creates a LUN using the *automagic* hints currently in effect. For more info, see the **automagic** sub-command in this article.

Parameter	Description
size=	Specifies the total LUN size in megabytes. Either the **size**= or the **drives**= parameter must be specified. They can also be used together. If the **size=** parameter is not specified, the LUN created will be the largest possible size allowed by all the specified drives. A provider typically creates a LUN at least as big as the requested size, but the provider may have to round up to the next largest size in some cases. For example, if size is specified as .99 GB and the provider can only allocate GB disk extents, the resulting LUN would be 1 GB. To specify the size using other units, use one of the following recognized suffixes immediately after the size: • **B** - byte • **KB** - kilobyte • **MB** - megabyte • **GB** - gigabyte • **TB** - terabyte • **PB** - petabyte.
drives=	Specifies the *drive_number* for the drives to use to create a LUN. Either the **size**= or the **drives**= parameter must be specified. They can also be used together. If the **size=** parameter is not specified, the LUN created is the largest possible size allowed by all the specified drives. If the **size=** parameter is specified, providers will select drives from the specified drive list to create the LUN. Providers will attempt to use the drives in the order specified when possible.
stripesize=	Specifies the size in megabytes for a *stripe* or *raid* LUN. The stripesize cannot be changed after the LUN is created. To specify the size using other units, use one of the following recognized suffixes immediately after the size: • **B** - byte • **KB** - kilobyte • **MB** - megabyte • **GB** - gigabyte • **TB** - terabyte • **PB** - petabyte.
target	Creates a new iSCSI target on the currently selected subsystem.
name	Supplies the friendly name for the target.
iscsiname	Supplies the iSCSI name for the target and can be omitted to have the provider generate a name.
tpgroup	Creates a new iSCSI target portal group on the currently selected target.
noerr	For scripting only. When an error is encountered, Diskraid continues to process commands as if the error did not occur.

delete

Deletes the currently selected LUN, iSCSI target (as long as there are not any LUNs associated with the iSCSI target) or iSCSI target portal group.

Syntax

```
delete lun [uninstall] [noerr]
delete target [noerr]
delete tpgroup [noerr]
```

Parameters

Parameter	Description
lun	Deletes the currently selected LUN and all data on it.
uninstall	Specifies that the disk on the local system associated with the LUN will be cleaned up before the LUN is deleted.
target	Deletes the currently selected iSCSI target if no LUNs are associated with the target.
tpgroup	Deletes the currently selected iSCSI target portal group.
noerr	For scripting only. When an error is encountered, Diskraid continues to process commands as if the error did not occur.

detail

Displays detailed information about the currently selected object of the specified type.

Syntax

```
detail {hbaport | iadapter | iportal | provider | subsystem | controller |
port | drive | lun | tportal | target | tpgroup} [verbose]
```

Parameters

Parameter	Description
hbaport	Lists detailed information about the currently selected host bus adapter (HBA) port.
iadapter	Lists detailed information about the currently selected iSCSI initiator adapter.
iportal	Lists detailed information about the currently selected iSCSI initiator portal.
provider	Lists detailed information about the currently selected provider.
subsystem	Lists detailed information about the currently selected subsystem.
controller	Lists detailed information about the currently selected controller.
port	Lists detailed information about the currently selected controller port.
drive	Lists detailed information about the currently selected drive, including the occupying LUNs.
lun	Lists detailed information about the currently selected LUN, including the contributing drives. The output differs slightly depending on whether the LUN is part of a Fibre Channel or iSCSI subsystem. If the Unmasked Hosts list contains only an asterisk, this means that the LUN is unmasked to all hosts.
tportal	Lists detailed information about the currently selected iSCSI target portal.
target	Lists detailed information about the currently selected iSCSI target.
tpgroup	Lists detailed information about the currently selected iSCSI target portal group.
verbose	For use only with the LUN parameter. Lists additional information, including its plexes.

dissociate

Sets specified list of controller ports as inactive for the currently selected LUN (other controller ports are not affected), or dissociates the specified list of iSCSI targets for the currently selected LUN.

Syntax

```
dissociate controllers <n> [,<n> [,...]]
dissociate ports <n-m>[,<n-m>[,…]]
dissociate targets <n> [,<n> [,…]]
```

Parameter

Parameter	Description
controllers	Removes controllers from the list of controllers that are associated with the currently selected LUN. Use only with VDS 1.0 providers.
ports	Removes controller ports from the list of controller ports that are associated with the currently selected LUN. Use only with VDS 1.1 providers.
targets	Removes targets from the list of iSCSI targets that are associated with the currently selected LUN. Use only with VDS 1.1 providers.
`<n> [,<n> [,…]]`	For use with the **controllers** or **targets** parameter. Specifies the numbers of the controllers or iSCSI targets to set as inactive or dissociate.
`<n-m>[,<n-m>[,…]]`	For use with the **ports** parameter. Specifies the controller ports to set as inactive by using a controller number (*n*) and port number (*m*) pair.

Example

```
DISKRAID> SEL LUN 5
LUN 5 is now the selected LUN.

DISKRAID> ASSOCIATE PORTS 0-0,0-1
Controller port associations changed.
(Controller ports active after this command: Ctlr 0 Port 0, Ctlr 0 Port 1)

DISKRAID> ASSOCIATE PORTS ADD 1-1
Controller port associations changed.
(Controller ports active after this command: Ctlr 0 Port 0, Ctlr 0 Port 1,
Ctlr 1 Port 1)

DISKRAID> DISSOCIATE PORTS 0-0,1-1
Controller port associations changed.
(Controller ports active after this command: Ctlr 0 Port 1)
```

exit

Exits Diskraid.

Syntax

```
```

```
exit
```

extend

Extends the currently selected LUN by adding sectors to the end of the LUN. Not all providers support extending LUNs. Does not extend any volumes or file systems contained on the LUN. After you extend the LUN, you should extend the associated on-disk structures using the **DiskPart extend** command.

Syntax

```
extend lun [size=<LUN_size>] [drives=<drive_number>, [<drive_number>, ...]]
[noerr]
```

Parameters

Parameter	Description
size	Specifies the size in megabytes to extend the LUN. Either the *size* or the `<drive>` parameter must be specified. They can also be used together. If the **size=** parameter is not specified, the LUN is extended by the largest possible size allowed by all the specified drives. If the **size=** parameter is specified, providers select drives from the list specified by the **drives=** parameter to create the LUN. To specify the size using other units, use one of the following recognized suffixes immediately after the size: • **B** - byte • **KB** - kilobyte • **MB** - megabyte • **GB** - gigabyte • **TB** - terabyte • **PB** - petabyte.
drives=	Specifies the `<drive_number>` for the drives to use when creating a LUN. Either the *size* or the `<drive>` parameter must be specified. They can also be used together. If the **size=** parameter is not specified, the LUN created is the largest possible size allowed by all the specified drives. Providers use the drives in the order specified when possible.
noerr	For scripting only. When an error is encountered, Diskraid continues to process commands as if the error did not occur.

flushcache

Clears the cache on the currently selected controller.

Syntax

```
flushcache controller
```

help

Displays a list of all Diskraid commands.

Syntax

```
help
```

importtarget

Retrieves or sets the current Volume Shadow Copy Service (VSS) import target that is set for the currently selected subsystem.

Syntax

```
importtarget subsystem [set target]
```

Parameter

Parameter	Description
set target	If specified, sets the currently selected target to the VSS import target for the currently selected subsystem. If not specified, the command retrieves the current VSS import target that is set for the currently selected subsystem.

initiator

Retrieves information about the local iSCSI initiator.

Syntax

```
initiator
```

invalidatecache

Invalidates the cache on the currently selected controller.

Syntax

```
invalidatecache controller
```

lbpolicy

Sets the load balance policy on the currently selected LUN.

Syntax

```
lbpolicy set lun type=<type> [paths=<path>-{primary | <weight>}[,<path>-
{primary | <weight>}[,…]]]
lbpolicy set lun paths=<path>-{primary | <weight>}[,<path>-{primary |
<weight>}[,…]]
```

Parameters

Parameter	Description

Parameter	Description
type	Specifies the load balance policy. If the type is not specified, then the **path** parameter must be specified. Type can be one of the following: • **FAILOVER** - Uses one primary path with other paths being backup paths. • **ROUNDROBIN** - Uses all paths in round-robin fashion, which tries each path sequentially. • **SUBSETROUNDROBIN** - Uses all primary paths in round-robin fashion; backup paths are used only if all primary paths fail. • **DYNLQD** - Uses the path with the least number of active requests. • • **WEIGHTED** - Uses the path with the least weight (each path must be assigned a weight). • **LEASTBLOCKS** - Uses the path with the least blocks. • **VENDORSPECIFIC** - Uses a vendor-specific policy.
path	Specifies whether a path is **primary** or has a particular `<weight>`. Any paths not specified are implicitly set as backup. Any paths listed must be one of the currently selected LUN's paths.

list

Displays a list of objects of the specified type.

Syntax

```
list {hbaports | iadapters | iportals | providers | subsystems | controllers
| ports | drives | LUNs | tportals | targets | tpgroups}
```

Parameters

Parameter	Description
hbaports	Lists summary information about all HBA ports known to VDS. The currently selected HBA port is marked by an asterisk (*).
iadapters	Lists summary information about all iSCSI initiator adapters known to VDS. The currently selected initiator adapter is marked by an asterisk (*).
iportals	Lists summary information about all iSCSI initiator portals in the currently selected initiator adapter. The currently selected initiator portal is marked by an asterisk (*).

Parameter	Description
providers	Lists summary information about each provider known to VDS. The currently selected provider is marked by an asterisk (*).
subsystems	Lists summary information about each subsystem in the system. The currently selected subsystem is marked by an asterisk (*).
controllers	Lists summary information about each controller in the currently selected subsystem. The currently selected controller is marked by an asterisk (*).
ports	Lists summary information about each controller port in the currently selected controller. The currently selected port is marked by an asterisk (*).
drives	Lists summary information about each drive in the currently selected subsystem. The currently selected drive is marked by an asterisk (*).
luns	Lists summary information about each LUN in the currently selected subsystem. The currently selected LUN is marked by an asterisk (*).
tportals	Lists summary information about all iSCSI target portals in the currently selected subsystem. The currently selected target portal is marked by an asterisk (*).
targets	Lists summary information about all iSCSI targets in the currently selected subsystem. The currently selected target is marked by an asterisk (*).
tpgroups	Lists summary information about all iSCSI target portal groups in the currently selected target. The currently selected portal group is marked by an asterisk (*).

login

Logs the specified iSCSI initiator adapter into the currently selected iSCSI target.

Syntax

```
login target iadapter=<iadapter> [type={manual | persistent | boot}] [chap=
{none | oneway | mutual}] [iportal=<iportal>] [tportal=<tportal>] [<flag>
[<flag> […]]]
```

Parameters

Parameter	Description

Parameter	Description
type	Specifies the type of login to perform: **manual** or **persistent**. If unspecified, a manual login will be performed.
manual	Login manually. There's also a **boot** option that is intended for future development and isn't currently used.
persistent	Automatically use the same login when the computer is restarted.
chap	Specifies the type of CHAP authentication to use: **none**, **oneway** CHAP, or **mutual** CHAP; if unspecified, no authentication will be used.
tportal	Specifies an optional target portal in the currently selected subsystem to use for the log in.
iportal	Specifies an optional initiator portal in the specified initiator adapter to use for the log in.
`<flag>`	Identified by three-letter acronyms: • **IPS** - Require IPsec • **EMP** - Enable multipath • **EHD** - Enable header digest • **EDD** - Enable data digest

logout

Logs the specified iSCSI initiator adapter out of the currently selected iSCSI target.

Syntax

```
logout target iadapter= <iadapter>
```

Parameters

Parameter	Description
iadapter	Specifies the initiator adapter with a login session to logout from.

maintenance

Performs maintenance operations on the currently selected object of the specified type.

Syntax

```
maintenance <object operation> [count=<iteration>]
```

Parameters

Parameter	Description
`<object>`	Specifies the type of object on which to perform the operation. The *object* type can be a **subsystem**, **controller**, **port, drive** or **LUN**.
`<operation>`	Specifies the maintenance operation to perform. The *operation* type can be **spinup**, **spindown**, **blink**, **beep** or **ping**. An *operation* must be specified.
count=	Specifies the number of times to repeat the *operation*. This is typically used with **blink**, **beep**,or **ping**.

name

Sets the friendly name of the currently selected subsystem, LUN, or iSCSI target to the specified name.

Syntax

```
name {subsystem | lun | target} [<name>]
```

Parameter

Parameter	Description
`<name>`	Specifies a name for the subsystem, LUN, or target. The name must be less than 64 characters in length. If no name is supplied, the existing name, if any, is deleted.

offline

Sets the state of the currently selected object of the specified type to **offline**.

Syntax

```
offline <object>
```

Parameter

Parameter	Description
`<object>`	Specifies the type of object on which to perform this operation. The type can be: **subsystem**, **controller**, **drive**, **LUN**, or **tportal**.

online

Sets the state of the selected object of the specified type to **online**. If object is **hbaport**, changes the status of the paths to the currently selected HBA port to **online**.

Syntax

```
online <object>
```

Parameter

Parameter	Description
`<object>`	Specifies the type of object on which to perform this operation. The type can be: **hbaport**, **subsystem**, **controller**, **drive**, **LUN**, or **tportal**.

recover

Performs operations necessary, such as resynchronization or hot sparing, to repair the currently selected fault-tolerant LUN. For example, RECOVER might cause a hot spare to be bound to a RAID set that has a failed disk or other disk extent reallocation.

Syntax

```
```

```
recover <lun>
```

reenumerate

Reenumerates objects of the specified type. If you use the extend LUN command, you must use the refresh command to update the disk size before using the reenumerate command.

Syntax

```

reenumerate {subsystems | drives}
```

Parameters

Parameter	Description
subsystems	Queries the provider to discover any new subsystems that were added in the currently selected provider.
drives	Queries the internal I/O buses to discover any new drives that were added in the currently selected subsystem.

refresh

Refreshes internal data for the currently selected provider.

Syntax

```

refresh provider
```

rem

Used to comment scripts.

Syntax

```
Rem <comment>
```

remove

Removes the specified iSCSI target portal from the currently selected target portal group.

Syntax

```
remove tpgroup tportal=<tportal> [noerr]
```

Parameter

Parameter	Description
tpgroup tportal= `<tportal>`	Specifies the iSCSI target portal to remove.
noerr	For scripting only. When an error is encountered, Diskraid continues to process commands as if the error did not occur.

replace

Replaces the specified drive with the currently selected drive. The specified drive may not be the currently selected drive.

Syntax

```
replace drive=<drive_number>
```

Parameter

Parameter	Description

Parameter	Description
drive=	Specifies the `<drive_number>` for the drive to be replaced.

reset

Resets the currently selected controller or port.

Syntax

```
reset {controller | port}
```

Parameters

Parameter	Description
controller	Resets the controller.
port	Resets the port.

select

Displays or changes the currently selected object.

Syntax

```
select {hbaport | iadapter | iportal | provider | subsystem | controller |
port | drive | lun | tportal | target | tpgroup } [<n>]
```

Parameters

Parameter	Description
object	Specifies the type of object to select, including: **provider**, **subsystem**, **controller**, **drive**, or **LUN**.

Parameter	Description
hbaport `[<n>]`	Sets the focus to the specified local HBA port. If no HBA port is specified, the command displays the currently selected HBA port (if any). Specifying an invalid HBA port index results in no in-focus HBA port. Selecting an HBA port deselects any selected initiator adapters and initiator portals.
iadapter `[<n>]`	Sets the focus to the specified local iSCSI initiator adapter. If no initiator adapter is specified, the command displays the currently selected initiator adapter (if any). Specifying an invalid initiator adapter index results in no in-focus initiator adapter. Selecting an initiator adapter deselects any selected HBA ports and initiator portals.
iportal `[<n>]`	Sets the focus to the specified local iSCSI initiator portal within the selected iSCSI initiator adapter. If no initiator portal is specified, the command displays the currently selected initiator portal (if any). Specifying an invalid initiator portal index results in no selected initiator portal.
provider `[<n>]`	Sets the focus to the specified provider. If no provider is specified, the command displays the currently selected provider (if any). Specifying an invalid provider index results in no in-focus provider.
subsystem `[<n>]`	Sets the focus to the specified subsystem. If no subsystem is specified, the command displays the subsystem with focus (if any). Specifying an invalid subsystem index results in no in-focus subsystem. Selecting a subsystem implicitly selects its associated provider.
controller `[<n>]`	Sets the focus to the specified controller within the currently selected subsystem. If no controller is specified, the command displays the currently selected controller (if any). Specifying an invalid controller index results in no in-focus controller. Selecting a controller deselects any selected controller ports, drives, LUNs, target portals, targets, and target portal groups.
port `[<n>]`	Sets the focus to the specified controller port within the currently selected controller. If no port is specified, the command displays the currently selected port (if any). Specifying an invalid port index results in no selected port.
drive `[<n>]`	Sets the focus to the specified drive, or physical spindle, within the currently selected subsystem. If no drive is specified, the command displays the currently selected drive (if any). Specifying an invalid drive index results in no in-focus drive. Selecting a drive deselects any selected controllers, controller ports, LUNs, target portals, targets, and target portal groups.
lun `[<n>]`	Sets the focus to the specified LUN within the currently selected subsystem. If no LUN is specified, the command displays the currently selected LUN (if any). Specifying an invalid LUN index results in no selected LUN. Selecting a LUN deselects any selected controllers, controller ports, drives, target portals, targets, and target portal groups.

Parameter	Description
tportal `[<n>]`	Sets the focus to the specified iSCSI target portal within the currently selected subsystem. If no target portal is specified, the command displays the currently selected target portal (if any). Specifying an invalid target portal index results in no selected target portal. Selecting a target portal deselects any controllers, controller ports, drives, LUNs, targets, and target portal groups.
target `[<n>]`	Sets the focus to the specified iSCSI target within the currently selected subsystem. If no target is specified, the command displays the currently selected target (if any). Specifying an invalid target index results in no selected target. Selecting a target deselects any controllers, controller ports, drives, LUNs, target portals, and target portal groups.
tpgroup `[<n>]`	Sets the focus to the specified iSCSI target portal group within the currently selected iSCSI target. If no target portal group is specified, the command displays the currently selected target portal group (if any). Specifying an invalid target portal group index results in no in-focus target portal group.
`[<n>]`	Specifies the `<object number>` to select. If the `<object number>` specified is not valid, any existing selections for objects of the specified type are cleared. If no `<object number>` is specified, the current object is displayed.

setflag

Sets the currently selected drive as a hot spare. Hot spares can't be used for ordinary LUN binding operations. They're reserved for fault handling only. The drive must not be currently bound to any existing LUN.

Syntax

```
setflag drive hotspare={true | false}
```

Parameters

Parameter	Description
true	Selects the currently selected drive as a hot spare.
false	Unselects the currently selected drive as a hot spare.

shrink

Reduces the size of the selected LUN.

Syntax

```
shrink lun size=<n> [noerr]
```

Parameters

Parameter	Description
size	Specifies the desired amount of space in megabytes (MB) to reduce the size of the LUN by. To specify the size using other units, use one of the following recognized suffixes immediately after the size: • **B** - byte • **KB** - kilobyte • **MB** - megabyte • **GB** - gigabyte • **TB** - terabyte • **PB** - petabyte.
noerr	For scripting only. When an error is encountered, Diskraid continues to process commands as if the error did not occur.

standby

Changes the status of the paths to the currently selected host bus adapter (HBA) port to STANDBY.

Syntax

```
standby hbaport
```

Parameters

Parameter	Description

Parameter	Description
hbaport	Changes the status of the paths to the currently selected host bus adapter (HBA) port to STANDBY.

unmask

Makes the currently selected LUNs accessible from the specified hosts.

Syntax

```
unmask lun {all | none | [add] wwn=<hexadecimal_number> [;
<hexadecimal_number> [;…]] | [add] initiator=<initiator>[;<initiator>[;…]]}
[uninstall]
```

Parameters

Parameter	Description
all	Specifies that the LUN should be made accessible from all hosts. However, you cannot unmask the LUN to all targets in an iSCSI subsystem. You must logout of the target before you run the `unmask lun all` command.
none	Specifies that the LUN should not be accessible to any host. You must logout of the target before you run the `unmask lun none` command.
add	Specifies that the hosts specified must be added to the existing list of hosts that this LUN is accessible from. If this parameter is not specified, the list of hosts supplied replaces the existing list of hosts that this LUN is accessible from.
wwn=	Specifies a list of hexadecimal numbers representing world-wide names from which the LUN or hosts should be made accessible. To mask/unmask to a specific set of hosts in a Fibre Channel subsystem, you can type a semicolon-separated list of WWN's for the ports on the host machines of interest.
initiator=	Specifies a list of iSCSI initiators to which the currently selected LUN should be made accessible. To mask/unmask to a specific set of hosts in an iSCSI subsystem, you can type a semicolon-separated list of iSCSI initiator names for the initiators on the host computers of interest.
uninstall	If specified, uninstalls the disk associated with the LUN on the local system before the LUN is masked.

Scripting Diskraid

Diskraid can be scripted on any computer running a supported version of Windows Server, with an associated VDS hardware provider. To invoke a Diskraid script, at the command prompt type:

```
diskraid /s <script.txt>
```

By default, Diskraid stops processing commands and returns an error code if there is a problem in the script. To continue running the script and ignore errors, include the **noerr** parameter on the command. This permits such useful practices as using a single script to delete all the LUNs in a subsystem regardless of the total number of LUNs. Not all commands support the **noerr** parameter. Errors are always returned on command-syntax errors, regardless of whether you included the **noerr** parameter.

Diskraid error codes

Error Code	Error Description
0	No error occurred. The entire script ran without failure.
1	A fatal exception occurred.
2	The arguments specified on a Diskraid command line were incorrect.
3	Diskraid was unable to open the specified script or output file.
4	One of the services Diskraid uses returned a failure.
5	A command syntax error occurred. The script failed because an object was improperly selected or was invalid for use with that command.

Example

To view the status of subsystem 0 on your computer, type:

```
diskraid
```

Press ENTER and output similar to the following is displayed:

```
Microsoft Diskraid version 5.2.xxxx
Copyright (©) 2003 Microsoft Corporation
On computer: COMPUTER_NAME
```

To select subsystem 0, type the following at the Diskraid prompt:

```
select subsystem 0
```

Press ENTER and output similar to the following is displayed:

```
Subsystem 0 is now the selected subsystem.

DISKRAID> list drives

  Drive ###  Status      Health          Size      Free    Bus  Slot  Flags
  ---------  ----------  ------------  --------  --------  ---  ----  -----
  Drive 0    Online      Healthy         107 GB    107 GB    0     1
  Drive 1    Offline     Healthy          29 GB     29 GB    1     0
  Drive 2    Online      Healthy         107 GB    107 GB    0     2
  Drive 3    Not Ready   Healthy          19 GB     19 GB    1     1
```

To exit Diskraid, type the following at the Diskraid prompt:

```
exit
```

Related links

- Command-Line Syntax Key

Diskshadow

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Diskshadow.exe is a tool that exposes the functionality offered by the volume shadow copy Service (VSS). By default, Diskshadow uses an interactive command interpreter similar to that of Diskraid or Diskpart. Diskshadow also includes a scriptable mode.

> **Note**
>
> Membership in the local Administrators group, or equivalent, is the minimum required to run Diskshadow.

Syntax

For interactive mode, type the following at the command prompt to start the Diskshadow command interpreter:

```
diskshadow
```

For script mode, type the following, where *script.txt* is a script file containing Diskshadow commands:

```
diskshadow -s script.txt
```

Parameters

You can run the following commands in the Diskshadow command interpreter or through a script file. At a minimum, only **add** and **create** are necessary to create a shadow copy. However, this forfeits the context and option settings, will be a copy backup, and creates a shadow copy with no backup execution script.

Command	Description
set command	Sets the context, options, verbose mode, and metadata file for creating shadow copies.
load metadata command	Loads a metadata .cab file prior to importing a transportable shadow copy or loads the writer metadata in the case of a restore.
writer command	verifies that a writer or component is included or excludes a writer or component from the backup or restore procedure.
add command	Adds volumes to the set of volumes that are to be shadow copied, or adds aliases to the alias environment.
create command	Starts the shadow copy creation process, using the current context and option settings.
exec command	Executes a file on the local computer.
begin backup command	Starts a full backup session.
end backup command	Ends a full backup session and issues a **backupcomplete** event with the appropriate writer state, if needed.
begin restore command	Starts a restore session and issues a **prerestore** event to involved writers.
end restore command	Ends a restore session and issues a **postrestore** event to involved writers.
reset command	Resets Diskshadow to the default state.
list command	Lists writers, shadow copies, or currently registered shadow copy providers that are on the system.
delete shadows command	Deletes shadow copies.
import command	Imports a transportable shadow copy from a loaded metadata file into the system.
mask command	Removes hardware shadow copies that were imported by using the **import** command.
expose command	Exposes a persistent shadow copy as a drive letter, share, or mount point.
unexpose command	Unexposes a shadow copy that was exposed by using the **expose** command.

Command	Description
break command	Disassociates a shadow copy volume from VSS.
revert command	Reverts a volume back to a specified shadow copy.
exit command	Exits the command interpreter or script.

Examples

This is a sample sequence of commands that will create a shadow copy for backup. It can be saved to file as script.dsh, and executed using `diskshadow /s script.dsh`.

Assume the following:

- You have an existing directory called c:\diskshadowdata.
- Your system volume is C: and your data volume is D:.
- You have a backupscript.cmd file in c:\diskshadowdata.
- Your backupscript.cmd file will perform the copy of shadow data p: and q: to your backup drive.

You can enter these commands manually or script them:

```
#Diskshadow script file
set context persistent nowriters
set metadata c:\diskshadowdata\example.cab
set verbose on
begin backup
add volume c: alias systemvolumeshadow
add volume d: alias datavolumeshadow

create

expose %systemvolumeshadow% p:
expose %datavolumeshadow% q:
exec c:\diskshadowdata\backupscript.cmd
end backup
#End of script
```

Related links

- Command-Line Syntax Key

add (diskshadow)

Article • 10/13/2023

Adds volumes to the set of volumes that are to be shadow copied, or adds aliases to the alias environment. If used without subcommands, **add** lists the current volumes and aliases.

> **Note**
>
> Aliases are not added to the alias environment until the shadow copy is created. Aliases that you need immediately should be added by using **add alias**.

Syntax

```
add
add volume <volume> [provider <providerid>]
add alias <aliasname> <aliasvalue>
```

Parameters

Parameter	Description
volume	Adds a volume to the Shadow Copy Set, which is the set of volumes to be shadow copied. See add volume for syntax and parameters.
alias	Adds the given name and value to the alias environment. See add alias for syntax and parameters.
/?	Displays help at the command line.

Examples

To display the volumes added and the aliases that are currently in the environment, type:

```
add
```

The following output shows that drive C has been added to the Shadow Copy Set:

```
Volume c: alias System1    GUID \\?\Volume{XXXXXXXX-XXXX-XXXX-XXXX-
XXXXXXXXXXXX}\
1 volume in Shadow Copy Set.
No Diskshadow aliases in the environment.
```

Related links

- Command-Line Syntax Key

add alias

Article • 02/03/2023

Adds aliases to the alias environment. If used without parameters, **add alias** displays help at the command prompt. Aliases are saved in the metadata file and will be loaded with the **load metadata** command.

Syntax

```
add alias <aliasname> <aliasvalue>
```

Parameters

Parameter	Description
`<aliasname>`	Specifies the name of the alias.
`<aliasvalue>`	Specifies the value of the alias.
`?	Displays help at the command prompt.

Examples

To list all shadows, including their aliases, type:

```
list shadows all
```

The following excerpt shows a shadow copy to which the default alias, *VSS_SHADOW_x*, has been assigned:

```
* Shadow Copy ID = {ff47165a-1946-4a0c-b7f4-80f46a309278}
%VSS_SHADOW_1%
```

To assign a new alias with the name *System1* to this shadow copy, type:

```
add alias System1 %VSS_SHADOW_1%
```

Alternatively, you can assign the alias by using the shadow copy ID:

```
add alias System1 {ff47165a-1946-4a0c-b7f4-80f46a309278}
```

Related links

- Command-Line Syntax Key
- load metadata command

add volume

Article • 02/03/2023

Adds volumes to the Shadow Copy Set, which is the set of volumes to be shadow copied. When a shadow copy is created, an environment variable links the alias to the shadow ID, so the alias can then be used for scripting.

Volumes are added one at a time. Each time a volume is added, it's checked to make sure VSS supports shadow copy creation for that volume. This check can be invalidated by later use of the **set context** command.

This command is necessary to create shadow copies. If used without parameters, **add volume** displays help at the command prompt.

Syntax

```
add volume <volume> [provider <providerid>]
```

Parameters

Parameter	Description
`<volume>`	Specifies a volume to add to the Shadow Copy Set. At least one volume is required for shadow copy creation.
`[provider \ <providerid>]`	Specifies the Provider ID for a registered provider to use to create the shadow copy. If **provider** is not specified, the default provider is used.

Examples

To view the current list of registered providers, at the `diskshadow>` prompt, type:

```
list providers
```

The following output displays a single provider, which will be used by default:

```
* ProviderID: {b5946137-7b9f-4925-af80-51abd60b20d5}
        Type: [1] VSS_PROV_SYSTEM
        Name: Microsoft Software Shadow Copy provider 1.0
        Version: 1.0.0.7
        CLSID: {65ee1dba-8ff4-4a58-ac1c-3470ee2f376a}
1 provider registered.
```

To add drive C: to the Shadow Copy Set and assign an alias named *System1*, type:

```
add volume c: alias System1
```

Related links

- Command-Line Syntax Key
- set context command

begin backup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2, Windows Server 2012

Starts a full backup session. This command overrides the default copy backup setting.

Syntax

```
begin backup
```

Related links

- Command-Line Syntax Key
- begin restore command

begin restore

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2, Windows Server 2012

Starts a restore session and issues a **PreRestore** event to involved writers.

Syntax

```
begin restore
```

Related links

- Command-Line Syntax Key
- begin backup command
- Prepare for restore

break (diskshadow)

Article • 10/12/2023

Disassociates a shadow copy volume from VSS and makes it accessible as a regular volume. The volume can then be accessed using a drive letter (if assigned) or volume name. If used without parameters, **break** displays help at the command prompt.

> **Note**
>
> This command is relevant only for hardware shadow copies after import.
>
> Exposed volumes, like the shadow copies they originate from, are read-only by default. Access to the volume is made directly to the hardware provider without record of the volume having been a shadow copy.

Syntax

```
break [writable] <setid>
```

Parameters

Parameter	Description
writable	Enables read/write access on the volume.
`<setid>`	Specifies the ID of the shadow copy set. The alias of the shadow copy ID, which is stored as an environment variable by the **load metadata** command, can be used in the *SetID* parameter.

Examples

To make a shadow copy using the alias name Alias1 accessible as a writable volume in the operating system:

```
break writable %Alias1%
```

Related links

- Command-Line Syntax Key

create (diskshadow)

Article • 10/16/2023

Starts the shadow copy creation process using the current context and option settings. Requires at least one volume in the Shadow Copy Set.

Syntax

```
create
```

Remarks

- You must add at least one volume with the add volume command before you can use the create command.
- You can use the begin backup command to specify a full backup rather than a copy backup.
- After you run the create command, you can use the exec command to run a duplication script for backup from the shadow copy.

Related links

- Command-Line Syntax Key

delete shadows

Article • 02/03/2023

Deletes shadow copies.

Syntax

```
delete shadows [all | volume <volume> | oldest <volume> | set <setID> | id <shadowID> | exposed {<drive> | <mountpoint>}]
```

Parameters

Parameter	Description
all	Deletes all shadow copies.
volume `<volume>`	Deletes all shadow copies of the given volume.
oldest `<volume>`	Deletes the oldest shadow copy of the given volume.
set `<setID>`	Deletes the shadow copies in the Shadow Copy Set of the given ID. You can specify an alias by using the % symbol if the alias exists in the current environment.
id `<shadowID>`	Deletes a shadow copy of the given ID. You can specify an alias by using the % symbol if the alias exists in the current environment.
exposed {`<drive>` | `<mountpoint>`}	Deletes shadow copies exposed at the specified drive or mount point.

Related links

- Command-Line Syntax Key
- delete command

end backup

Article • 02/03/2023

Ends a full backup session and issues a **BackupComplete** event with the appropriate writer state, if needed.

Syntax

```
end backup
```

Related links

- Command-Line Syntax Key

Feedback

Was this page helpful? Yes No

end restore

Article • 02/03/2023

Ends a restore session and issues a **PostRestore** event to involved writers.

Syntax

```
end restore
```

Related links

- Command-Line Syntax Key

exec

Article • 02/03/2023

Runs a script file on the local computer. This command also duplicates or restores data as part of a backup or restore sequence. If the script fails, an error is returned and DiskShadow quits.

The file can be a **cmd** script.

Syntax

```
exec <scriptfile.cmd>
```

Parameters

Parameter	Description
`<scriptfile.cmd>`	Specifies the script file to run.

Related links

- Command-Line Syntax Key
- diskshadow command

exit (diskshadow)

Article • 10/16/2023

Exits the DiskShadow command line interpreter.

Syntax

```
exit
```

Related links

- Command-Line Syntax Key

expose

Article • 02/03/2023

Exposes a persistent shadow copy as a drive letter, share, or mount point.

Syntax

```
expose <shadowID> {<drive:> | <share> | <mountpoint>}
```

Parameters

Parameter	Description
shadowID	Specifies the shadow ID of the shadow copy you want to expose. You can also use an existing alias or an environment variable in place of *shadowID*. Use **add** without parameters to see existing aliases.
`<drive:>`	Exposes the specified shadow copy as a drive letter (for example, `p:`).
`<share>`	Exposes the specified shadow copy at a share (for example, `\\machinename`).
`<mountpoint>`	Exposes the specified shadow copy to a mount point (for example, `C:\shadowcopy`).

Examples

To expose the persistent shadow copy associated with the VSS_SHADOW_1 environment variable as drive X, type:

```
expose %vss_shadow_1% x:
```

Related links

- Command-Line Syntax Key
- diskshadow command

import (diskshadow)

Article • 02/03/2023

Imports a transportable shadow copy from a loaded metadata file into the system.

> [IMPORTANT] Before you can use this command, you must use the load metadata command to load a DiskShadow metadata file.

Syntax

```
import
```

Remarks

- Transportable shadow copies aren't stored on the system immediately. Their details are stored in a Backup Components Document XML file, which DiskShadow automatically requests and saves in a .cab metadata file in the working directory. Use the set metadata command to change the path and name of this XML file.

Examples

The following is a sample DiskShadow script that demonstrates the use of the **import** command:

```
#Sample DiskShadow script demonstrating IMPORT
SET CONTEXT PERSISTENT
SET CONTEXT TRANSPORTABLE
SET METADATA transHWshadow_p.cab
#P: is the volume supported by the Hardware Shadow Copy provider
ADD VOLUME P:
CREATE
END BACKUP
#The (transportable) shadow copy is not in the system yet.
#You can reset or exit now if you wish.

LOAD METADATA transHWshadow_p.cab
IMPORT
#The shadow copy will now be loaded into the system.
```

Related links

- Command-Line Syntax Key
- diskshadow command

list (diskshadow)

Article • 10/16/2023

Lists writers, shadow copies, or currently registered shadow copy providers that are on the system. If used without parameters, list displays help at the command prompt.

For examples of how to use this command, see Examples.

Syntax

```
list writers [metadata | detailed | status]
list shadows {all | set <SetID> | id <ShadowID>}
list providers
```

Parameters

Parameter	Description
writers	Lists writers. See List writers for syntax and parameters.
shadows	Lists persistent and existing non-persistent shadow copies. See List shadows for syntax and parameters.
providers	Lists currently registered shadow copy providers. See List providers for syntax and parameters.

Examples

To list all shadow copies, type:

```
list shadows all
```

Related links

- Command-Line Syntax Key

list providers

Article • 02/03/2023

Lists shadow copy providers that are currently registered on the system.

Syntax

```
list providers
```

Examples

To list the currently registered shadow copy providers, type:

```
list providers
```

Output that is similar to the following displays:

```
* ProviderID: {b5946137-7b9f-4925-af80-51abd60b20d5}
        Type: [1] VSS_PROV_SYSTEM
        Name: Microsoft Software Shadow Copy provider 1.0
        Version: 1.0.0.7
        CLSID: {65ee1dba-8ff4-4a58-ac1c-3470ee2f376a}
1 provider registered.
```

Related links

- Command-Line Syntax Key

list shadows

Article • 02/03/2023

Lists persistent and existing non-persistent shadow copies that are on the system.

Syntax

```
list shadows {all | set <setID> | id <shadowID>}
```

Parameters

Parameter	Description
all	Lists all shadow copies.
set `<setID>`	Lists shadow copies that belong to the specified Shadow Copy Set ID.
id `<shadowID>`	Lists any shadow copy with the specified shadow copy ID.

Related links

- Command-Line Syntax Key

list writers

Article • 02/03/2023

Lists writers that are on the system. If used without parameters, **list** displays the output for **list metadata** by default.

Syntax

```
list writers [metadata | detailed | status]
```

Parameters

Parameter	Description
metadata	Lists the identity and status of writers, and displays metadata such as component details and excluded files. This is the default parameter.
detailed	Lists the same information as **metadata**, but also includes the full file list for all components.
status	Lists only the identity and status of registered writers.

Examples

To list only the identity and status of writers, type:

```
list writers status
```

Output that is similar to the following displays:

```
Listing writer status ...
* WRITER System Writer
        - Status: 5 (VSS_WS_WAITING_FOR_BACKUP_COMPLETE)
        - Writer Failure code: 0x00000000 (S_OK)
        - Writer ID: {e8132975-6f93-4464-a53e-1050253ae220}
        - Instance ID: {7e631031-c695-4229-9da1-a7de057e64cb}
* WRITER Shadow Copy Optimization Writer
```

```
        - Status: 1 (VSS_WS_STABLE)
        - Writer Failure code: 0x00000000 (S_OK)
        - Writer ID: {4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
        - Instance ID: {9e362607-9794-4dd4-a7cd-b3d5de0aad20}
* WRITER Registry Writer
        - Status: 1 (VSS_WS_STABLE)
        - Writer Failure code: 0x00000000 (S_OK)
        - Writer ID: {afbab4a2-367d-4d15-a586-71dbb18f8485}
        - Instance ID: {e87ba7e3-f8d8-42d8-b2ee-c76ae26b98e8}
8 writers listed.
```

Related links

- Command-Line Syntax Key

Load metadata

Article • 02/03/2023

Loads a metadata .cab file prior to importing a transportable shadow copy or loads the writer metadata in the case of a restore. If used without parameters, **load metadata** displays help at the command prompt.

Syntax

```
load metadata [<drive>:][<path>]<metadata.cab>
```

Parameters

Parameter	Description
`[<drive>:][<path>]`	Specifies the location of the metadata file.
metadata.cab	Specifies the metadata .cab file to load.

Remarks

- You can use the **import** command to import a transportable shadow copy based on the metadata specified by **load metadata**.
- You must run this command before the **begin restore** command, to load the selected writers and components for the restore.

Examples

To load a metadata file called metafile.cab from the default location, type:

```
load metadata metafile.cab
```

Related links

- Command-Line Syntax Key
- import diskshadow command
- begin restore command

mask

Article • 02/03/2023

Removes hardware shadow copies that were imported by using the **import** command.

Syntax

```
mask <shadowsetID>
```

Parameters

Expand table

Parameter	Description
shadowsetID	Removes shadow copies that belong to the specified Shadow Copy Set ID.

Remarks

- You can use an existing alias or an environment variable in place of *ShadowSetID*. Use **add** without parameters to see existing aliases.

Examples

To remove the imported shadow copy *%Import_1%*, type:

```
mask %Import_1%
```

Related links

- Command-Line Syntax Key

Feedback

Was this page helpful? Yes No

reset

Article • 02/03/2023

Resets DiskShadow.exe to the default state. This command is especially useful in separating compound DiskShadow operations, such as **create**, **import**, **backup**, or **restore**.

> [!IMPORTANT After you run this command, you will lose state information from commands, such as **add**, **set**, **load**, or **writer**. This command also releases IVssBackupComponent interfaces and loses non-persistent shadow copies.

Syntax

```
reset
```

Related links

- Command-Line Syntax Key
- create command
- import command
- backup command
- restore command
- add command
- set command
- load command
- writer command

reset session

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables you to reset (delete) a session on a Remote Desktop Session Host server. You should reset a session only when it malfunctions or appears to have stopped responding.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
reset session {<sessionname> | <sessionID>} [/server:<servername>] [/v]
```

Parameters

Parameter	Description
`<sessionname>`	Specifies the name of the session that you want to reset. To determine the name of the session, use the query session command.
`<sessionID>`	Specifies the ID of the session to reset.
/server:`<servername>`	Specifies the terminal server containing the session that you want to reset. Otherwise, it uses the current Remote Desktop Session Host server. This parameter is required only if you use this command from a remote server.
/v	Displays information about the actions being performed.
/?	Displays help at the command prompt.

Remarks

- You can always reset your own sessions, but you must have **Full Control** access permission to reset another user's session. Be aware that resetting a user's session without warning the user can result in the loss of data at the session.

Examples

To reset the session designated *rdp-tcp#6*, type:

```
reset session rdp-tcp#6
```

To reset the session that uses *session ID 3*, type:

```
reset session 3
```

Related links

- Command-Line Syntax Key
- Remote Desktop Services Command Reference

revert

Article • 02/03/2023

Reverts a volume back to a specified shadow copy. This is supported only for shadow copies in the CLIENTACCESSIBLE context. These shadow copies are persistent and can only be made by the system provider. If used without parameters, **revert** displays help at the command prompt.

Syntax

```
revert <shadowcopyID>
```

Parameters

Parameter	Description
`<shadowcopyID>`	Specifies the shadow copy ID to revert the volume to. If you don't use this parameter, the command displays help at the command prompt.

Related links

- Command-Line Syntax Key

set commands (shadow copy creation)

Article • 02/03/2023

Sets the context, options, verbose mode, and metadata file for shadow copy creation. If used without parameters, **set** lists all current settings.

Syntax

```
set
set context
set option
set verbose
set metadata
```

Parameters

Parameters	Description
set context	Sets the context for shadow copy creation.
set metadata	Sets the name and location of the shadow creation metadata file.
set option	Sets options for shadow copy creation.
set verbose	Turns the verbose output mode on or off.
/?	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

Set context

Article • 02/03/2023

Sets the context for shadow copy creation. If used without parameters, **set context** displays help at the command prompt.

Syntax

```
set context {clientaccessible | persistent [nowriters] | volatile
[nowriters]}
```

Parameters

Parameter	Description
clientaccessible	Specifies that the shadow copy is usable by client versions of Windows. This context is persistent by default.
persistent	Specifies that the shadow copy persists across program exit, reset, or restart.
volatile	Deletes the shadow copy on exit or reset.
nowriters	Specifies that all writers are excluded.

Examples

To prevent shadow copies from being deleted when you exit DiskShadow, type:

```
set context persistent
```

Related links

- Command-Line Syntax Key
- set metadata command
- set option command

- set verbose command

set metadata

Article • 02/03/2023

Sets the name and location of the shadow creation metadata file used to transfer shadow copies from one computer to another. If used without parameters, **set metadata** displays help at the command prompt.

Syntax

```
set metadata [<drive>:][<path>]<metadata.cab>
```

Parameters

Parameter	Description
`[<drive>:][<path>]`	Specifies the location to create the metadata file.
`<metadata.cab>`	Specifies the name of the cab file to store shadow creation metadata.

Related links

- Command-Line Syntax Key
- set context command
- set option command
- set verbose command

set option

Article • 02/03/2023

Sets the options for shadow copy creation. If used without parameters, **set option** displays help at the command prompt.

Syntax

```
set option {[differential | plex] [transportable] [[rollbackrecover]
[txfrecover] | [noautorecover]]}
```

Parameters

Parameter	Description
[differential]	Specifies to create a point-in-time snapshot of specified volumes.
[plex]	Specifies to create a point-in-time clone copy of the data on a specified volume.
[transportable]	Specifies that the shadow copy is not to be imported yet. The metadata .cab file can later be used to import the shadow copy to the same or a different computer.
[rollbackrecover]	Signals writers to use *autorecover* during the **PostSnapshot** event. This is useful if the shadow copy will be used for rollback (for example, with data mining).
[txfrecover]	Requests VSS to make the shadow copy transactionally consistent during creation.
[noautorecover]	Stops writers and the file system from performing any recovery changes to the shadow copy to a transactionally consistent state. **Noautorecover** can't be used with **txfrecover** or **rollbackrecover**.

Related links

- Command-Line Syntax Key
- set context command
- set metadata command

- set verbose command

Set verbose

Article • 02/03/2023

Specifies whether verbose output is provided during shadow copy creation. If used without parameters, **set verbose** displays help at the command prompt.

Syntax

```
set verbose {on | off}
```

Parameters

Parameter	Description
on	Turns on verbose output logging during the shadow copy creation process. If verbose mode is on, **set** provides details of writer inclusion or exclusion and details of metadata compression and extraction.
off	Turns off verbose output logging during the shadow copy creation process.

Related links

- Command-Line Syntax Key
- set context command
- set metadata command
- set option command

Simulate restore

Article • 02/03/2023

Tests whether writer involvement in restore sessions will be successful on the computer without issuing **PreRestore** or **PostRestore** events to writers.

> **Note**
>
> A DiskShadow metadata file must be selected for the **simulate restore** command to succeed. Use the **load metadata command** to load the selected writers and components for the restore.

Syntax

```
simulate restore
```

Related links

- Command-Line Syntax Key
- load metadata command

unexpose

Article • 02/03/2023

Unexposes a shadow copy that was exposed by using the expose command. The exposed shadow copy can be specified by its Shadow ID, drive letter, share, or mount point.

Syntax

```
unexpose {<shadowID> | <drive:> | <share> | <mountpoint>}
```

Parameters

Parameter	Description
`<shadowID>`	Displays the shadow copy specified by the given Shadow ID. You can use an existing alias or an environment variable in place of `<shadowID>`. Use the add command without parameters to see all existing aliases.
`<drive:>`	Displays the shadow copy associated with the specified drive letter (for example, drive P).
`<share>`	Displays the shadow copy associated with the specified share (for example, `\\MachineName`).
`<mountpoint>`	Displays the shadow copy associated with the specified mount point (for example, `C:\shadowcopy\`).
add	Used without parameters will show you the existing aliases.

Examples

To unexpose the shadow copy associated with *drive P:*, type:

```
unexpose P:
```

Related links

- Command-Line Syntax Key
- add command
- expose command

writer

Article • 02/03/2023

Verifies that a writer or component is included or excludes a writer or component from the backup or restore procedure. If used without parameters, **writer** displays help at the command prompt.

Syntax

```
writer verify [writer> | <component>]
writer exclude [<writer> | <component>]
```

Parameters

Parameter	Description
verify	Verifies that the specified writer or component is included in the backup or restore procedure. The backup or restore procedure will fail if the writer or component is not included.
exclude	Excludes the specified writer or component from the backup or restore procedure.

Examples

To verify a writer by specifying its GUID (for this example, 4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f), type:

```
writer verify {4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
```

To exclude a writer with the name *System Writer*, type:

```
writer exclude System Writer
```

Related links

- Command-Line Syntax Key

dispdiag

Article • 02/03/2023

Logs display information to a file.

Syntax

```
dispdiag [-testacpi] [-d] [-delay <seconds>] [-out <filepath>]
```

Parameters

Parameter	Description
- testacpi	Runs hotkey diagnostics test. Displays the key name, code and scan code for any key pressed during the test.
-d	Generates a dump file with test results.
-delay `<seconds>`	Delays the collection of data by specified time in *seconds*.
-out `<filepath>`	Specifies path and filename to save collected data. This must be the last parameter.
-?	Displays available command parameters and provides help for using them.

Related links

- Command-Line Syntax Key

Dnscmd

Article • 03/21/2024

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

A command-line interface for managing DNS servers. This utility is useful in scripting batch files to help automate routine DNS management tasks, or to perform simple unattended setup and configuration of new DNS servers on your network.

Syntax

```
dnscmd <servername> <command> [<command parameters>]
```

Parameters

Expand table

Parameter	Description
`<servername>`	The IP address or host name of a remote or local DNS server.

dnscmd /ageallrecords command

Sets the current time on a time stamp on resource records at a specified zone or node on a DNS server.

Syntax

```
dnscmd [<servername>] /ageallrecords <zonename>[<nodename>] | [/tree]|[/f]
```

Parameters

Expand table

Parameter	Description
`<servername>`	Specifies the DNS server that the administrator plans to manage, represented by IP address, fully qualified domain name (FQDN), or Host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the FQDN of the zone.
`<nodename>`	Specifies a specific node or subtree in the zone, using the following: • @ for root zone or FQDN • The FQDN of a node (the name with a period (.) at the end) • A single label for the name relative to the zone root.
/tree	Specifies that all child nodes also receive the time stamp.
/f	Runs the command without asking for confirmation.

Remarks

- The **ageallrecords** command is for backward compatibility between the current version of DNS and previous releases of DNS in which aging and scavenging weren't supported. It adds a time stamp with the current time to resource records that don't have a time stamp, and it sets the current time on resource records that do have a time stamp.
- Record scavenging doesn't occur unless the records are time stamped. Name server (NS) resource records, start of authority (SOA) resource records, and Windows Internet Name Service (WINS) resource records aren't included in the scavenging process, and they aren't time stamped even when the **ageallrecords** command runs.
- This command fails unless scavenging is enabled for the DNS server and the zone. For information about how to enable scavenging for the zone, see the **aging** parameter, within the syntax of the `dnscmd /config` command in this article.
- The addition of a time stamp to DNS resource records makes them incompatible with DNS servers that run on operating systems other than Windows Server. A time stamp added by using the **ageallrecords** command can't be reversed.
- If none of the optional parameters are specified, the command returns all resource records at the specified node. If a value is specified for at least one of the optional parameters, **dnscmd** enumerates only the resource records that correspond to the value or values that are specified in the optional parameter or parameters.

Examples

Example 1: Set the current time on a time stamp to resource records.

dnscmd /clearcache command

Clears the DNS cache memory of resource records on the specified DNS server.

Syntax

```
dnscmd [<servername>] /clearcache
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.

Example

```
dnscmd dnssvr1.contoso.com /clearcache
```

dnscmd /config command

Changes values in the registry for the DNS server and individual zones. This command also modifies the configuration of the specified server. Accepts server-level and zone-level settings.

> **⊗ Caution**
>
> Don't edit the registry directly unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can degrade performance,

damage your system, or even require you to reinstall Windows. You can safely alter most registry settings by using the programs in Control Panel or Microsoft Management Console (mmc). If you must edit the registry directly, back it up first. Read the registry editor help for more information.

Server-level syntax

```
dnscmd [<servername>] /config <parameter>
```

Parameters

> **Note**
>
> This article contains references to the term slave, a term that Microsoft no longer uses. When the term is removed from the software, we'll remove it from this article.

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server that you're planning to manage, represented by local computer syntax, IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<parameter>`	Specify a setting and, as an option, a value. Parameter values use this syntax: *parameter* [*value*].
/addressanswerlimit `[0|5-28]`	Specifies the maximum number of host records that a DNS server can send in response to a query. The value can be zero (0), or it can be in the range of 5 through 28 records. The default value is zero (0).
/bindsecondaries `[0|1]`	Changes the format of the zone transfer so that it can achieve maximum compression and efficiency. Accepts the values: • **0** - Uses maximum compression and is compatible with BIND versions 4.9.4 and later only • **1** - Sends only one resource record per message to non-Microsoft DNS servers and is compatible with

Parameters	Description
	BIND versions earlier than 4.9.4. This is the default setting.
/bootmethod `[0|1|2|3]`	Determines the source from which the DNS server gets its configuration information. Accepts the values: • **0** - Clears the source of configuration information. • **1** - Loads from the BIND file that is located in the DNS directory, which is `%systemroot%\System32\DNS` by default. • **2** - Loads from the registry. • **3** - Loads from AD DS and the registry. This is the default setting.
/defaultagingstate `[0|1]`	Determines whether the DNS scavenging feature is enabled by default on newly created zones. Accepts the values: • **0** - Disables scavenging. This is the default setting. • **1** - Enables scavenging.
/defaultnorefreshinterval `[0x1-0xFFFFFFFF|0xA8]`	Sets a period of time in which no refreshes are accepted for dynamically updated records. Zones on the server inherit this value automatically. To change the default value, type a value in the range of **0x1-0xFFFFFFFF**. The default value from the server is **0xA8**.
/defaultrefreshinterval `[0x1-0xFFFFFFFF|0xA8]`	Sets a period of time that is allowed for dynamic updates to DNS records. Zones on the server inherit this value automatically. To change the default value, type a value in the range of **0x1-0xFFFFFFFF**. The default value from the server is **0xA8**.
/disableautoreversezones `[0|1]`	Enables or disables the automatic creation of reverse lookup zones. Reverse lookup zones provide resolution of Internet Protocol (IP) addresses to DNS domain names. Accepts the values: • **0** - Enables the automatic creation of reverse lookup zones. This is the default setting. • **1** - Disables the automatic creation of reverse lookup zones.
/disablensrecordsautocreation `[0|1]`	Specifies whether the DNS server automatically creates name server (NS) resource records for zones that it hosts. Accepts the values: • **0** - Automatically creates name server (NS) resource records for zones that the DNS server hosts. • **1** - Doesn't automatically create name server (NS) resource records for zones that the DNS server hosts.

Parameters	Description
/dspollinginterval `<seconds>`	Specifies in seconds how often the DNS server polls AD DS for changes in the AD integrated zones. The minimum accepted value is **30** seconds. If a value isn't specified after this parameter, the default value is set to **0xB4** (3 minutes or 180 seconds).
/dstombstoneinterval `<seconds>`	The amount of time in seconds to retain deleted records in AD DS. This value should be limited to the range from **0x3F480** (3 days or 259,200 seconds) to **0x49D400** (8 weeks or 4,147,200 seconds). The default value should be **0x127500** (14 days or 1,209,600 seconds) if no value is specified for the tombstoneLifetime attribute of the Directory Services object.
/ednscachetimeout `[3600-15724800]`	Specifies the number of seconds that extended DNS (EDNS) information is cached. The minimum value is **3600**, and the maximum value is **15,724,800**. The default value is **604,800** seconds (one week).
/enableednsprobes `[0|1]`	Enables or disables the server to probe other servers to determine if they support EDNS. Accepts the values: • **0** - Disables active support for EDNS probes. • **1** - Enables active support for EDNS probes.
/enablednssec `[0|1]`	Enables or disables support for DNS Security Extensions (DNSSEC). Accepts the values: • **0** - Disables DNSSEC. • **1** - Enables DNSSEC.
/enableglobalnamessupport `[0|1]`	Enables or disables support for the GlobalNames zone. The GlobalNames zone supports resolution of single-label DNS names across a forest. Accepts the values: • **0** - Disables support for the GlobalNames zone. When you set the value of this command to 0, the DNS Server service doesn't resolve single-label names in the GlobalNames zone. • **1** - Enables support for the GlobalNames zone. When you set the value of this command to 1, the DNS Server service resolves single-label names in the GlobalNames zone.
/enableglobalqueryblocklist `[0|1]`	Enables or disables support for the global query block list that blocks name resolution for names in the list. The DNS Server service creates and enables the global query block list by default when the service starts the first time. To view the current global query block list, use the dnscmd /info **/globalqueryblocklist** command. Accepts the values:

Parameters	Description
	• **0** - Disables support for the global query block list. When you set the value of this command to 0, the DNS Server service responds to queries for names in the block list. • **1** - Enables support for the global query block list. When you set the value of this command to 1, the DNS Server service doesn't respond to queries for names in the block list.
/eventloglevel `[0|1|2|4]`	Determines which events are logged in the DNS server log in Event Viewer. Accepts the values: • **0** - Logs no events. • **1** - Logs only errors. • **2** - Logs only errors and warnings. • **4** - Logs errors, warnings, and informational events. This is the default setting.
/forwarddelegations `[0|1]`	Determines how the DNS server handles a query for a delegated subzone. These queries can be sent either to the subzone that is referred to in the query or to the list of forwarders that is named for the DNS server. Entries in the setting are used only when forwarding is enabled. Accepts the values: • **0** - Automatically sends queries that refer to delegated subzones to the appropriate subzone. This is the default setting. • **1** - Forwards queries that refer to the delegated subzone to the existing forwarders.
/forwardingtimeout `[<seconds>]`	Determines how many seconds (**0x1-0xFFFFFFFF**) a DNS server waits for a forwarder to respond before trying another forwarder. The default value is **0x5**, which is 5 seconds.
/globalneamesqueryorder `[0|1]`	Specifies whether the DNS Server service looks first in the GlobalNames zone or local zones when it resolves names. Accepts the values: • **0** - The DNS Server service attempts to resolve names by querying the GlobalNames zone before it queries the zones for which it's authoritative. • **1** - The DNS Server service attempts to resolve names by querying the zones for which it's authoritative before it queries the GlobalNames zone.
/globalqueryblocklist `[[<name> [<name>]...]`	Replaces the current global query block list with a list of the names that you specify. If you don't specify any names, this

Parameters	Description
	command clears the block list. By default, the global query block list contains the following items: • isatap • wpad The DNS Server service can remove either or both of these names when it starts the first time, if it finds these names in an existing zone.
/isslave `[0|1]`	Determines how the DNS server responds when queries that it forwards receive no response. Accepts the values: • **0** - Specifies that the DNS server isn't a subordinate. If the forwarder doesn't respond, the DNS server attempts to resolve the query itself. This is the default setting. • **1** - Specifies that the DNS server is a subordinate. If the forwarder doesn't respond, the DNS server terminates the search and sends a failure message to the resolver.
/localnetpriority `[0|1]`	Determines the order in which host records are returned when the DNS server has multiple host records for the same name. Accepts the values: • **0** - Returns the records in the order in which they're listed in the DNS database. • **1** - Returns the records that have similar IP network addresses first. This is the default setting.
/logfilemaxsize `[<size>]`	Specifies the maximum size in bytes (**0x10000-0xFFFFFFFF**) of the Dns.log file. When the file reaches its maximum size, DNS overwrites the oldest events. The default size is **0x400000**, which is 4 megabytes (MB).
/logfilepath `[<path+logfilename>]`	Specifies the path of the Dns.log file. The default path is `%systemroot%\System32\Dns\Dns.log`. You can specify a different path by using the format `path+logfilename`.
/logipfilterlist `<IPaddress> [, <IPaddress>...]`	Specifies which packets are logged in the debug log file. The entries are a list of IP addresses. Only packets going to and from the IP addresses in the list are logged.
/loglevel `[<eventtype>]`	Determines which types of events are recorded in the Dns.log file. Each event type is represented by a hexadecimal number. If you want more than one event in the log, use hexadecimal addition to add the values, and then enter the sum. Accepts the values: • **0x0** - The DNS server doesn't create a log. This is the default entry.

Parameters	Description
	• **0x10** - Logs queries and notifications. • **0x20** - Logs updates. • **0xFE** - Logs nonquery transactions. • **0x100** - Logs question transactions. • **0x200** - Logs answers. • **0x1000** - Logs send packets. • **0x2000** - Logs receive packets. • **0x4000** - Logs User Datagram Protocol (UDP) packets. • **0x8000** - Logs Transmission Control Protocol (TCP) packets. • **0xFFFF** - Logs all packets. • **0x10000** - Logs active directory write transactions. • **0x20000** - Logs active directory update transactions. • **0x1000000** - Logs full packets. • **0x80000000** - Logs write-through transactions. •
/maxcachesize	Specifies the maximum size, in kilobytes (KB), of the DNS server s memory cache.
/maxcachettl `[<seconds>]`	Determines how many seconds (**0x0-0xFFFFFFFF**) a record is saved in the cache. If the **0x0** setting is used, the DNS server doesn't cache records. The default setting is **0x15180** (86,400 seconds or 1 day).
/maxnegativecachettl `[<seconds>]`	Specifies how many seconds (**0x1-0xFFFFFFFF**) an entry that records a negative answer to a query remains stored in the DNS cache. The default setting is **0x384** (900 seconds).
/namecheckflag `[0|1|2|3]`	Specifies which character standard is used when checking DNS names. Accepts the values: • **0** - Uses ANSI characters that comply with Internet Engineering Task force (IETF) Request for Comments (Rfcs). • **1** - Uses ANSI characters that don't necessarily comply with IETF Rfcs. • **2** - Uses multibyte UCS Transformation format 8 (UTF-8) characters. This is the default setting. • **3** - Uses all characters.
/norecursion `[0|1]`	Determines whether a DNS server performs recursive name resolution. Accepts the values: • **0** - The DNS server performs recursive name resolution if it's requested in a query. This is the default setting. • **1** - The DNS server doesn't perform recursive name resolution.

Parameters	Description
/notcp	This parameter is obsolete, and it has no effect in current versions of Windows Server.
/recursionretry `[<seconds>]`	Determines the number of seconds (**0x1-0xFFFFFFFF**) that a DNS server waits before again trying to contact a remote server. The default setting is **0x3** (three seconds). This value should be increased when recursion occurs over a slow wide area network (WAN) link.
/recursiontimeout `[<seconds>]`	Determines the number of seconds (**0x1-0xFFFFFFFF**) that a DNS server waits before discontinuing attempts to contact a remote server. The settings range from **0x1** through **0xFFFFFFFF**. The default setting is **0xF** (15 seconds). This value should be increased when recursion occurs over a slow WAN link.
/roundrobin `[0|1]`	Determines the order in which host records are returned when a server has multiple host records for the same name. Accepts the values: • **0** - The DNS server doesn't use round robin. Instead, it returns the first record to every query. • **1** - The DNS server rotates among the records that it returns from the top to the bottom of the list of matching records. This is the default setting.
/rpcprotocol `[0x0|0x1|0x2|0x4|0xFFFFFFFF]`	Specifies the protocol that remote procedure call (RPC) uses when it makes a connection from the DNS server. Accepts the values: • **0x0** - Disables RPC for DNS. • **0x01** - Uses TCP/IP • **0x2** - Uses named pipes. • **0x4** - Uses local procedure call (LPC). • **0xFFFFFFFF** - All protocols. This is the default setting.
/scavenginginterval `[<hours>]`	Determines whether the scavenging feature for the DNS server is enabled, and sets the number of hours (**0x0-0xFFFFFFFF**) between scavenging cycles. The default setting is **0x0**, which disables scavenging for the DNS server. A setting greater than **0x0** enables scavenging for the server and sets the number of hours between scavenging cycles.
/secureresponses `[0|1]`	Determines whether DNS filters records that are saved in a cache. Accepts the values: • **0** - Saves all responses to name queries to a cache. This is the default setting. • **1** - Saves only the records that belong to the same DNS subtree to a cache.

Parameters	Description
/sendport `[<port>]`	Specifies the port number (**0x0-0xFFFFFFFF**) that DNS uses to send recursive queries to other DNS servers. The default setting is **0x0**, which means that the port number is selected randomly.
/serverlevelplugindll `[<dllpath>]`	Specifies the path of a custom plug-in. When Dllpath specifies the fully qualified path name of a valid DNS server plug-in, the DNS server calls functions in the plug-in to resolve name queries that are outside the scope of all locally hosted zones. If a queried name is out of the scope of the plug-in, the DNS server performs name resolution using forwarding or recursion, as configured. If Dllpath isn't specified, the DNS server ceases to use a custom plug-in if a custom plug-in was previously configured.
/strictfileparsing `[0|1]`	Determines a DNS server's behavior when it encounters an erroneous record while loading a zone. Accepts the values: • **0** - The DNS server continues to load the zone even if the server encounters an erroneous record. The error is recorded in the DNS log. This is the default setting. • **1** - The DNS server stops loading the zone, and it records the error in the DNS log.
/updateoptions `<RecordValue>`	Prohibits dynamic updates of specified types of records. If you want more than one record type to be prohibited in the log, use hexadecimal addition to add the values, and then enter the sum. Accepts the values: • **0x0** - Doesn't restrict any record types. • **0x1** - Excludes start of authority (SOA) resource records. • **0x2** - Excludes name server (NS) resource records. • **0x4** - Excludes delegation of name server (NS) resource records. • **0x8** - Excludes server host records. • **0x100** - During secure dynamic update, excludes start of authority (SOA) resource records. • **0x200** - During secure dynamic update, excludes root name server (NS) resource records. • **0x30F** - During standard dynamic update, excludes name server (NS) resource records, start of authority (SOA) resource records, and server host records. During secure dynamic update, excludes root name server (NS) resource records and start of authority (SOA) resource records. Allows delegations and server host updates. • **0x400** - During secure dynamic update, excludes delegation name server (NS) resource records. • **0x800** - During secure dynamic update, excludes server host records. • **0x1000000** - Excludes delegation signer (DS) records.

Parameters	Description
	• **0x80000000** - Disables DNS dynamic update.
/writeauthorityns `[0|1]`	Determines when the DNS server writes name server (NS) resource records in the Authority section of a response. Accepts the values: • **0** - Writes name server (NS) resource records in the Authority section of referrals only. This setting complies with Rfc 1034, Domain names concepts and facilities, and with Rfc 2181, Clarifications to the DNS Specification. This is the default setting. • **1** - Writes name server (NS) resource records in the Authority section of all successful authoritative responses.
/xfrconnecttimeout `[<seconds>]`	Determines the number of seconds (**0x0-0xFFFFFFFF**) a primary DNS server waits for a transfer response from its secondary server. The default value is **0x1E** (30 seconds). After the time-out value expires, the connection is terminated.

Zone-level syntax

Modifies the configuration of the specified zone. The zone name must be specified only for zone-level parameters.

```
dnscmd /config <parameters>
```

Parameters

Expand table

Parameters	Description
`<parameter>`	Specify a setting, a zone name, and, as an option, a value. Parameter values use this syntax: `zonename parameter [value]`.
/aging `<zonename>`	Enables or disables scavenging in a specific zone.
/allownsrecordsautocreation `<zonename>` `[value]`	Overrides the DNS server's name server (NS) resource record autocreation setting. Name server (NS) resource records that were previously registered for this zone aren't affected.

Parameters	Description
	Therefore, you must remove them manually if you don't want them.
/allowupdate `<zonename>`	Determines whether the specified zone accepts dynamic updates.
/forwarderslave `<zonename>`	Overrides the DNS server **/isslave** setting.
/forwardertimeout `<zonename>`	Determines how many seconds a DNS zone waits for a forwarder to respond before trying another forwarder. This value overrides the value that is set at the server level.
/norefreshinterval `<zonename>`	Sets a time interval for a zone during which no refreshes can dynamically update DNS records in a specified zone.
/refreshinterval `<zonename>`	Sets a time interval for a zone during which refreshes can dynamically update DNS records in a specified zone.
/securesecondaries `<zonename>`	Determines which secondary servers can receive zone updates from the primary server for this zone.

dnscmd /createbuiltindirectorypartitions command

Creates a DNS application directory partition. When DNS is installed, an application directory partition for the service is created at the forest and domain levels. Use this command to create DNS application directory partitions that were deleted or never created. With no parameter, this command creates a built-in DNS directory partition for the domain.

Syntax

```
dnscmd [<servername>] /createbuiltindirectorypartitions [/forest]
[/alldomains]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
/forest	Creates a DNS directory partition for the forest.
/alldomains	Creates DNS partitions for all domains in the forest.

dnscmd /createdirectorypartition command

Creates a DNS application directory partition. When DNS is installed, an application directory partition for the service is created at the forest and domain levels. This operation creates additional DNS application directory partitions.

Syntax

```
dnscmd [<servername>] /createdirectorypartition <partitionFQDN>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<partitionFQDN>`	The FQDN of the DNS application directory partition that will be created.

dnscmd /deletedirectorypartition command

Removes an existing DNS application directory partition.

Syntax

```
dnscmd [<servername>] /deletedirectorypartition <partitionFQDN>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<partitionFQDN>`	The FQDN of the DNS application directory partition that will be removed.

dnscmd /directorypartitioninfo command

Lists information about a specified DNS application directory partition.

Syntax

```
dnscmd [<servername>] /directorypartitioninfo <partitionFQDN> [/detail]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<partitionFQDN>`	The FQDN of the DNS application directory partition.
/detail	Lists all information about the application directory partition.

dnscmd /enlistdirectorypartition command

Adds the DNS server to the specified directory partition's replica set.

Syntax

```
```

```
dnscmd [<servername>] /enlistdirectorypartition <partitionFQDN>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<partitionFQDN>`	The FQDN of the DNS application directory partition.

dnscmd /enumdirectorypartitions command

Lists the DNS application directory partitions for the specified server.

Syntax

```
dnscmd [<servername>] /enumdirectorypartitions [/custom]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
/custom	Lists only user-created directory partitions.

dnscmd /enumrecords command

Lists the resource records of a specified node in a DNS zone.

Syntax

```
dnscmd [<servername>] /enumrecords <zonename> <nodename> [/type <rrtype>
<rrdata>] [/authority] [/glue] [/additional] [/node | /child |
/startchild<childname>] [/continue | /detail]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
/enumrecords	Lists resource records in the specified zone.
`<zonename>`	Specifies the name of the zone to which the resource records belong.
`<nodename>`	Specifies the name of the node of the resource records.
`[/type <rrtype> <rrdata>]`	Specifies the type of resource records to be listed and the type of data that is expected. Accepts the values: • `<rrtype>` - Specifies the type of resource records to be listed. • `<rrdata>` - Specifies the type of data that is expected record.
/authority	Includes authoritative data.
/glue	Includes glue data.
/additional	Includes all additional information about the listed resource records.
/node	Lists only the resource records of the specified node.
/child	Lists only the resource records of a specified child domain.
/startchild `<childname>`	Begins the list at the specified child domain.
/continue	Lists only the resource records with their type and data.
/detail	Lists all information about the resource records.

Example

```
dnscmd /enumrecords test.contoso.com test /additional
```

dnscmd /enumzones command

Lists the zones that exist on the specified DNS server. The **enumzones** parameters act as filters on the list of zones. If no filters are specified, a complete list of zones is returned. When a filter is specified, only the zones that meet that filter's criteria are included in the returned list of zones.

Syntax

```
dnscmd [<servername>] /enumzones [/primary | /secondary | /forwarder | /stub
| /cache | /auto-created] [/forward | /reverse | /ds | /file]
[/domaindirectorypartition | /forestdirectorypartition |
/customdirectorypartition | /legacydirectorypartition | /directorypartition
<partitionFQDN>]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
/primary	Lists all zones that are either standard primary zones or active directory integrated zones.
/secondary	Lists all standard secondary zones.
/forwarder	Lists zones that forward unresolved queries to another DNS server.
/stub	Lists all stub zones.
/cache	Lists only the zones that are loaded into the cache.
/auto-created]	Lists the zones that were created automatically during the DNS server installation.
/forward	Lists forward lookup zones.
/reverse	Lists reverse lookup zones.
/ds	Lists active directory integrated zones.

Parameters	Description
/file	Lists zones that are backed by files.
/domaindirectorypartition	Lists zones that are stored in the domain directory partition.
/forestdirectorypartition	Lists zones that are stored in the forest DNS application directory partition.
/customdirectorypartition	Lists all zones that are stored in a user-defined application directory partition.
/legacydirectorypartition	Lists all zones that are stored in the domain directory partition.
/directorypartition `<partitionFQDN>`	Lists all zones that are stored in the specified directory partition.

Examples

- Example 2: Display a complete list of zones on a DNS server)
- Example 3: Display a list of autocreated zones on a DNS server

dnscmd /exportsettings command

Creates a text file that lists the configuration details of a DNS server. The text file is named *DnsSettings.txt*. It's located in the `%systemroot%\system32\dns` directory of the server. You can use the information in the file that **dnscmd /exportsettings** creates to troubleshoot configuration problems or to ensure that you have configured multiple servers identically.

Syntax

```
dnscmd [<servername>] /exportsettings
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.

dnscmd /info command

Displays settings from the DNS section of the registry of the specified server `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters`. To display zone-level registry settings, use the `dnscmd zoneinfo` command.

Syntax

```
dnscmd [<servername>] /info [<settings>]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<settings>`	Any setting that the **info** command returns can be specified individually. If a setting isn't specified, a report of common settings is returned.

Example

- Example 4: Display the IsSlave setting from a DNS server
- Example 5: Display the RecursionTimeout setting from a DNS server

dnscmd /ipvalidate command

Tests whether an IP address identifies a functioning DNS server or whether the DNS server can act as a forwarder, a root hint server, or a primary server for a specific zone.

Syntax

```
dnscmd [<servername>] /ipvalidate <context> [<zonename>] [[<IPaddress>]]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<context>`	Specifies the type of test to perform. You can specify any of the following tests: • **/dnsservers** - Tests that the computers with the addresses that you specify are functioning DNS servers. • **/forwarders** - Tests that the addresses that you specify identify DNS servers that can act as forwarders. • **/roothints** - Tests that the addresses that you specify identify DNS servers that can act as root hint name servers. • **/zonemasters** - Tests that the addresses that you specify identify DNS servers that are primary servers for *zonename*.
`<zonename>`	Identifies the zone. Use this parameter with the **/zonemasters** parameter.
`<IPaddress>`	Specifies the IP addresses that the command tests.

Examples

```
nscmd dnssvr1.contoso.com /ipvalidate /dnsservers 10.0.0.1 10.0.0.2
dnscmd dnssvr1.contoso.com /ipvalidate /zonemasters corp.contoso.com
10.0.0.2
```

dnscmd /nodedelete command

Deletes all records for a specified host.

Syntax

```
dnscmd [<servername>] /nodedelete <zonename> <nodename> [/tree] [/f]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone.
`<nodename>`	Specifies the host name of the node to delete.
/tree	Deletes all the child records.
/f	Executes the command without asking for confirmation.

Example

Example 6: Delete the records from a node.

dnscmd /recordadd command

Adds a record to a specified zone in a DNS server.

Syntax

```
dnscmd [<servername>] /recordadd <zonename> <nodename> <rrtype> <rrdata>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the zone in which the record resides.
`<nodename>`	Specifies a specific node in the zone.
`<rrtype>`	Specifies the type of record to be added.
`<rrdata>`	Specifies the type of data that is expected.

> **Note**
>
> After you add a record, make sure that you use the correct data type and data format. For a list of resource record types and the appropriate data types, see Dnscmd Examples.

Examples

```
dnscmd dnssvr1.contoso.com /recordadd test A 10.0.0.5
dnscmd /recordadd test.contoso.com test MX 10 mailserver.test.contoso.com
```

dnscmd /recorddelete command

Deletes a resource record to a specified zone.

Syntax

```
dnscmd [<servername>] /recorddelete <zonename> <nodename> <rrtype> <rrdata>
[/f]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the zone in which the resource record resides.
`<nodename>`	Specifies a name of the host.
`<rrtype>`	Specifies the type of resource record to be deleted.
`<rrdata>`	Specifies the type of data that is expected.
/f	Executes the command without asking for confirmation. Because nodes can have more than one resource record, this command requires you to be specific about the type of resource record that you want to delete. If you specify a data type and you don't specify a type of resource record data, all records with that specific data type for the specified node are deleted.

Examples

```
dnscmd /recorddelete test.contoso.com test MX 10 mailserver.test.contoso.com
```

dnscmd /resetforwarders command

Selects or resets the IP addresses to which the DNS server forwards DNS queries when it can't resolve them locally.

Syntax

```
dnscmd [<servername>] /resetforwarders <IPaddress> [,<IPaddress>]...]
[/timeout <timeout>] [/slave | /noslave]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<IPaddress>`	Lists the IP addresses to which the DNS server forwards unresolved queries.
/timeout `<timeout>`	Sets the number of seconds that the DNS server waits for a response from the forwarder. By default, this value is five seconds.
/slave	Prevents the DNS server from performing its own iterative queries if the forwarder fails to resolve a query.
/noslave	Allows the DNS server to perform its own iterative queries if the forwarder fails to resolve a query. This is the default setting.
/f	Executes the command without asking for confirmation. Because nodes can have more than one resource record, this command requires you to be specific about the type of resource record that you want to delete. If you specify a data type and you don't specify a type of resource record data, all records with that specific data type for the specified node are deleted.

Remarks

- By default, a DNS server performs iterative queries when it can't resolve a query.
- Setting IP addresses by using the **resetforwarders** command causes the DNS server to perform recursive queries to the DNS servers at the specified IP addresses. If the forwarders don't resolve the query, the DNS server can then perform its own iterative queries.
- If the **/slave** parameter is used, the DNS server doesn't perform its own iterative queries. This means that the DNS server forwards unresolved queries only to the DNS servers in the list, and it doesn't attempt iterative queries if the forwarders don't resolve them. It's more efficient to set one IP address as a forwarder for a DNS server. You can use the **resetforwarders** command for internal servers in a network to forward their unresolved queries to one DNS server that has an external connection.
- Listing a forwarder's IP address twice causes the DNS server to attempt to forward to that server twice.

Examples

```
```

```
dnscmd dnssvr1.contoso.com /resetforwarders 10.0.0.1 /timeout 7 /slave
dnscmd dnssvr1.contoso.com /resetforwarders /noslave
```

dnscmd /resetlistenaddresses command

Specifies the IP addresses on a server that listens for DNS client requests. By default, all IP addresses on a DNS server listen for client DNS requests.

Syntax

```
dnscmd [<servername>] /resetlistenaddresses <listenaddress>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<listenaddress>`	Specifies an IP address on the DNS server that listens for DNS client requests. If no listen address is specified, all IP addresses on the server listen for client requests.

Examples

```
dnscmd dnssvr1.contoso.com /resetlistenaddresses 10.0.0.1
```

dnscmd /startscavenging command

Tells a DNS server to attempt an immediate search for stale resource records in a specified DNS server.

Syntax

```
dnscmd [<servername>] /startscavenging
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.

Remarks

- Successful completion of this command starts a scavenge immediately. If the scavenge fails, no warning message appears.
- Although the command to start the scavenge appears to complete successfully, the scavenge doesn't start unless the following preconditions are met:
  - Scavenging is enabled for both the server and the zone.
  - The zone is started.
  - The resource records have a time stamp.
- For information about how to enable scavenging for the server, see the **scavenginginterval** parameter under **Server-level syntax** in the **/config** section.
- For information about how to enable scavenging for the zone, see the **aging** parameter under **Zone-level syntax** in the **/config** section.
- For information about how to restart a paused zone, see the **zoneresume** parameter in this article.
- For information about how to check resource records for a time stamp, see the **ageallrecords** parameter in this article.

Examples

```
```

```
dnscmd dnssvr1.contoso.com /startscavenging
```

dnscmd /statistics command

Displays or clears data for a specified DNS server.

Syntax

```
dnscmd [<servername>] /statistics [<statid>] [/clear]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<statid>`	Specifies which statistic or combination of statistics to display. The **statistics** command displays counters that begin on the DNS server when it's started or resumed. An identification number is used to identify a statistic. If no statistic ID number is specified, all statistics display. The numbers that can be specified, along with the corresponding statistic that displays, can include: • **00000001** - Time • **00000002** - Query • **00000004** - Query2 • **00000008** - Recurse • **00000010** - Master • **00000020** - Secondary • **00000040** - WINS • **00000100** - Update • **00000200** - SkwanSec • **00000400** - Ds • **00010000** - Memory • **00100000** - PacketMem • **00040000** - Dbase • **00080000** - Records • **00200000** - NbstatMem • **/clear** - Resets the specified statistics counter to zero.

Examples

- Example 7:
- Example 8: Display NbstatMem statistics for a DNS server

dnscmd /unenlistdirectorypartition command

Removes the DNS server from the specified directory partition's replica set.

Syntax

```
dnscmd [<servername>] /unenlistdirectorypartition <partitionFQDN>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<partitionFQDN>`	The FQDN of the DNS application directory partition that will be removed.

dnscmd /writebackfiles command

Checks the DNS server memory for changes, and writes them to persistent storage. The **writebackfiles** command updates all dirty zones or a specified zone. A zone is dirty when there are changes in memory that haven't yet been written to persistent storage. This is a server-level operation that checks all zones. You can specify one zone in this operation or you can use the **zonewriteback** operation.

Syntax

```
dnscmd [<servername>] /writebackfiles <zonename>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone to be updated.

Examples

```
dnscmd dnssvr1.contoso.com /writebackfiles
```

dnscmd /zoneadd command

Adds a zone to the DNS server.

Syntax

```
dnscmd [<servername>] /zoneadd <zonename> <zonetype> [/dp <FQDN> | {/domain
| enterprise | legacy}]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone.
`<zonetype>`	Specifies the type of zone to create. Specifying a zone type of **/forwarder** or **/dsforwarder** creates a zone that performs conditional forwarding. Each zone type has different required parameters:

Parameters	Description
	• **/dsprimary** - Creates an active directory integrated zone. • **/primary /file** `<filename>` - Creates a standard primary zone, and specifies the name of the file that will store the zone information. • **/secondary** `<masterIPaddress> [<masterIPaddress>...]` - Creates a standard secondary zone. • **/stub** `<masterIPaddress> [<masterIPaddress>...]` **/file** `<filename>` - Creates a file-backed stub zone. • **/dsstub** `<masterIPaddress> [<masterIPaddress>...]` - Creates an active directory integrated stub zone. • **/forwarder** `<masterIPaddress> [<masterIPaddress>]` **... /file** `<filename>` - Specifies that the created zone forwards unresolved queries to another DNS server. • **/dsforwarder** - Specifies that the created active directory integrated zone forwards unresolved queries to another DNS server.
`<FQDN>`	Specifies FQDN of the directory partition.
/domain	Stores the zone on the domain directory partition.
/enterprise	Stores the zone on the enterprise directory partition.
/legacy	Stores the zone on a legacy directory partition.

Examples

```
dnscmd dnssvr1.contoso.com /zoneadd test.contoso.com /dsprimary
dnscmd dnssvr1.contoso.com /zoneadd secondtest.contoso.com /secondary
10.0.0.2
```

dnscmd /zonechangedirectorypartition command

Changes the directory partition on which the specified zone resides.

Syntax

```
dnscmd [<servername>] /zonechangedirectorypartition <zonename>
```

```
{[<newpartitionname>] | [<zonetype>]}
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	The FQDN of the current directory partition on which the zone resides.
`<newpartitionname>`	The FQDN of the directory partition that the zone will be moved to.
`<zonetype>`	Specifies the type of directory partition that the zone will be moved to.
/domain	Moves the zone to the built-in domain directory partition.
/forest	Moves the zone to the built-in forest directory partition.
/legacy	Moves the zone to the directory partition that is created for pre active directory domain controllers. These directory partitions aren't necessary for native mode.

dnscmd /zonedelete command

Deletes a specified zone.

Syntax

```
dnscmd [<servername>] /zonedelete <zonename> [/dsdel] [/f]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.

Parameters	Description
`<zonename>`	Specifies the name of the zone to be deleted.
/dsdel	Deletes the zone from Azure Directory Domain Services (AD DS).
/f	Runs the command without asking for confirmation.

Examples

- Example 9: Delete a zone from a DNS server

dnscmd /zoneexport command

Creates a text file that lists the resource records of a specified zone. The **zoneexport** operation creates a file of resource records for an active directory integrated zone for troubleshooting purposes. By default, the file that this command creates is placed in the DNS directory, which is by default the `%systemroot%/System32/Dns` directory.

Syntax

```
dnscmd [<servername>] /zoneexport <zonename> <zoneexportfile>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone.
`<zoneexportfile>`	Specifies the name of the file to create.

Examples

- Example 10: Export zone resource records list to a file

dnscmd /zoneinfo

Displays settings from the section of the registry of the specified zone: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\Zones\<zonename>`

Syntax

```
dnscmd [<servername>] /zoneinfo <zonename> [<setting>]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone.
`<setting>`	You can individually specify any setting that the **zoneinfo** command returns. If you don't specify a setting, all settings are returned.

Remarks

- To display server-level registry settings, use the **/info** command.
- To see a list of settings that you can display with this command, see the **/config** command.

Examples

- Example 11: Display RefreshInterval setting from the registry
- Example 12: Display Aging setting from the registry

dnscmd /zonepause command

Pauses the specified zone, which then ignores query requests.

Syntax

```
dnscmd [<servername>] /zonepause <zonename>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone to be paused.

Remarks

- To resume a zone and make it available after it has been paused, use the **/zoneresume** command.

Examples

```
dnscmd dnssvr1.contoso.com /zonepause test.contoso.com
```

dnscmd /zoneprint command

Lists the records in a zone.

Syntax

```
dnscmd [<servername>] /zoneprint <zonename>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone to be listed.

dnscmd /zonerefresh command

Forces a secondary DNS zone to update from the master zone.

Syntax

```
dnscmd [<servername>] /zonerefresh <zonename>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone to be refreshed.

Remarks

- The **zonerefresh** command forces a check of the version number in the primary server s start of authority (SOA) resource record. If the version number on the primary server is higher than the secondary server's version number, a zone transfer is initiated that updates the secondary server. If the version number is the same, no zone transfer occurs.
- The forced check occurs by default every 15 minutes. To change the default, use the `dnscmd config refreshinterval` command.

Examples

```
dnscmd dnssvr1.contoso.com /zonerefresh test.contoso.com
```

dnscmd /zonereload command

Copies zone information from its source.

Syntax

```
dnscmd [<servername>] /zonereload <zonename>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone to be reloaded.

Remarks

- If the zone is active directory integrated, it reloads from Active Directory Domain Services (AD DS).
- If the zone is a standard file-backed zone, it reloads from a file.

Examples

```
dnscmd dnssvr1.contoso.com /zonereload test.contoso.com
```

dnscmd /zoneresetmasters command

Resets the IP addresses of the primary server that provides zone transfer information to a secondary zone.

Syntax

```
dnscmd [<servername>] /zoneresetmasters <zonename> [/local] [<IPaddress>
[<IPaddress>]...]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone to be reset.
/local	Sets a local master list. This parameter is used for active directory integrated zones.
`<IPaddress>`	The IP addresses of the primary servers of the secondary zone.

Remarks

- This value is originally set when the secondary zone is created. Use the **zoneresetmasters** command on the secondary server. This value has no effect if it's set on the master DNS server.

Examples

```
dnscmd dnssvr1.contoso.com /zoneresetmasters test.contoso.com 10.0.0.1
dnscmd dnssvr1.contoso.com /zoneresetmasters test.contoso.com /local
```

dnscmd /zoneresetscavengeservers command

Changes the IP addresses of the servers that can scavenge the specified zone.

Syntax

```
dnscmd [<servername>] /zoneresetscavengeservers <zonename> [/local]
[<IPaddress> [<IPaddress>]...]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the zone to scavenge.
/local	Sets a local master list. This parameter is used for active directory integrated zones.
`<IPaddress>`	Lists the IP addresses of the servers that can perform the scavenge. If this parameter is omitted, all servers that host this zone can scavenge it.

Remarks

- By default, all servers that host a zone can scavenge that zone.
- If a zone is hosted on more than one DNS server, you can use this command to reduce the number of times a zone is scavenged.
- Scavenging must be enabled on the DNS server and zone that is affected by this command.

Examples

```
dnscmd dnssvr1.contoso.com /zoneresetscavengeservers test.contoso.com
```

```
10.0.0.1 10.0.0.2
```

dnscmd /zoneresetsecondaries command

Specifies a list of IP addresses of secondary servers to which a primary server responds when it's asked for a zone transfer.

Syntax

```
dnscmd [<servername>] /zoneresetsecondaries <zonename> {/noxfr | /nonsecure
| /securens | /securelist <securityIPaddresses>} {/nonotify | /notify |
/notifylist <notifyIPaddresses>}
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone that will have its secondary servers reset.
/local	Sets a local master list. This parameter is used for active directory integrated zones.
/noxfr	Specifies that no zone transfers are allowed.
/nonsecure	Specifies that all zone transfer requests are granted.
/securens	Specifies that only the server that is listed in the name server (NS) resource record for the zone is granted a transfer.
/securelist	Specifies that zone transfers are granted only to the list of servers. This parameter must be followed by an IP address or addresses that the primary server uses.
`<securityIPaddresses>`	Lists the IP addresses that receive zone transfers from the primary server. This parameter is used only with the **/securelist** parameter.
/nonotify	Specifies that no change notifications are sent to secondary servers.
/notify	Specifies that change notifications are sent to all secondary servers.

Parameters	Description
/notifylist	Specifies that change notifications are sent to only the list of servers. This command must be followed by an IP address or addresses that the primary server uses.
`<notifyIPaddresses>`	Specifies the IP address or addresses of the secondary server or servers to which change notifications are sent. This list is used only with the **/notifylist** parameter.

Remarks

- Use the **zoneresetsecondaries** command on the primary server to specify how it responds to zone transfer requests from secondary servers.

Examples

```
dnscmd dnssvr1.contoso.com /zoneresetsecondaries test.contoso.com /noxfr
/nonotify
dnscmd dnssvr1.contoso.com /zoneresetsecondaries test.contoso.com
/securelist 11.0.0.2
```

dnscmd /zoneresettype command

Changes the type of the zone.

Syntax

```
dnscmd [<servername>] /zoneresettype <zonename> <zonetype> [/overwrite_mem |
/overwrite_ds]
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Identifies the zone on which the type will be changed.
`<zonetype>`	Specifies the type of zone to create. Each type has different required parameters, including: • **/dsprimary** - Creates an active directory integrated zone. • **/primary /file** `<filename>` - Creates a standard primary zone. • **/secondary** `<masterIPaddress> [,<masterIPaddress>...]` - Creates a standard secondary zone. • **/stub** `<masterIPaddress>[,<masterIPaddress>...]` **/file** `<filename>` - Creates a file-backed stub zone. • **/dsstub** `<masterIPaddress>[,<masterIPaddress>...]` - Creates an active directory integrated stub zone. • **/forwarder** `<masterIPaddress[,<masterIPaddress>]` **... /file** `<filename>` - Specifies that the created zone forwards unresolved queries to another DNS server. • **/dsforwarder** - Specifies that the created active directory integrated zone forwards unresolved queries to another DNS server.
/overwrite_mem	Overwrites DNS data from data in AD DS.
/overwrite_ds	Overwrites existing data in AD DS.

Remarks

- Setting the zone type as **/dsforwarder** creates a zone that performs conditional forwarding.

Examples

```
dnscmd dnssvr1.contoso.com /zoneresettype test.contoso.com /primary /file
test.contoso.com.dns
dnscmd dnssvr1.contoso.com /zoneresettype second.contoso.com /secondary
10.0.0.2
```

dnscmd /zoneresume command

Starts a specified zone that was previously paused.

Syntax

```
dnscmd [<servername>] /zoneresume <zonename>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone to resume.

Remarks

- You can use this operation to restart from the **/zonepause** operation.

Examples

```
dnscmd dnssvr1.contoso.com /zoneresume test.contoso.com
```

dnscmd /zoneupdatefromds command

Updates the specified active directory integrated zone from AD DS.

Syntax

```
dnscmd [<servername>] /zoneupdatefromds <zonename>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.
`<zonename>`	Specifies the name of the zone to update.

Remarks

- Active directory integrated zones perform this update by default every five minutes. To change this parameter, use the `dnscmd config dspollinginterval` command.

Examples

```
dnscmd dnssvr1.contoso.com /zoneupdatefromds
```

dnscmd /zonewriteback command

Checks DNS server memory for changes that are relevant to a specified zone, and writes them to persistent storage.

Syntax

```
dnscmd [<servername>] /zonewriteback <zonename>
```

Parameters

Expand table

Parameters	Description
`<servername>`	Specifies the DNS server to manage, represented by IP address, FQDN, or host name. If this parameter is omitted, the local server is used.

Parameters	Description
`<zonename>`	Specifies the name of the zone to update.

Remarks

- This is a zone-level operation. You can update all zones on a DNS server by using the **/writebackfiles** operation.

Examples

```
dnscmd dnssvr1.contoso.com /zonewriteback test.contoso.com
```

Related links

- Command-Line Syntax Key

doskey

Article • 02/03/2023

Calls Doskey.exe, which recalls previously entered command-line commands, edits command lines, and creates macros.

Syntax

```
doskey [/reinstall] [/listsize=<size>] [/macros:[all | <exename>] [/history]
[/insert | /overstrike] [/exename=<exename>] [/macrofile=<filename>]
[<macroname>=[<text>]]
```

Parameters

Parameter	Description
/reinstall	Installs a new copy of Doskey.exe and clears the command history buffer.
/listsize=`<size>`	Specifies the maximum number of commands in the history buffer.
/macros	Displays a list of all **doskey** macros. You can use the redirection symbol (`>`) with **/macros** to redirect the list to a file. You can abbreviate **/macros** to **/m**.
/macros:all	Displays **doskey** macros for all executables.
/macros:`<exename>`	Displays **doskey** macros for the executable specified by *exename*.
/history	Displays all commands that are stored in memory. You can use the redirection symbol (`>`) with **/history** to redirect the list to a file. You can abbreviate **/history** as **/h**.
/insert	Specifies that new text you type is inserted in old text.
/overstrike	Specifies that new text overwrites old text.
/exename=`<exename>`	Specifies the program (that is, executable) in which the **doskey** macro runs.
/macrofile=`<filename>`	Specifies a file that contains the macros that you want to install.

Parameter	Description
`<macroname>=[<text>]`	Creates a macro that carries out the commands specified by *Text*. *MacroName* specifies the name you want to assign to the macro. *Text* specifies the commands you want to record. If *Text* is left blank, *MacroName* is cleared of any assigned commands.
/?	Displays help at the command prompt.

Remarks

- Certain character-based, interactive programs, such as program debuggers or file transfer programs (FTP) automatically use Doskey.exe. To use Doskey.exe, a program must be a console process and use buffered input. Program key assignments override **doskey** key assignments. For example, if the program uses the F7 key for a function, you cannot get a **doskey** command history in a pop-up window.
- You can use Doskey.exe to edit the current command line, but you can't use the command-line options from a program's command prompt. You must run **doskey** command-line options before you start a program. If you use Doskey.exe within a program, that program's key assignments take precedence and some Doskey.exe editing keys might not work.
- With Doskey.exe, you can maintain a command history for each program that you start or repeat. You can edit previous commands at the program's prompt, and start **doskey** macros created for the program. If you exit and then restart a program from the same Command Prompt window, the command history from the previous program session is available.
- To recall a command, you can use any of the following keys after you start Doskey.exe:

Key	Description
UP ARROW	Recalls the command that you used before the one that is displayed.
DOWN ARROW	Recalls the command that you used after the one that is displayed.
PAGE UP	Recalls the first command that you used in the current session.
PAGE DOWN	Recalls the most recent command that you used in the current session.

- The following table lists **doskey** editing keys and their functions:

Key or key combination	Description
LEFT ARROW	Moves the insertion point back one character.
RIGHT ARROW	Moves the insertion point forward one character.
CTRL+LEFT ARROW	Moves the insertion point back one word.
CTRL+RIGHT ARROW	Moves the insertion point forward one word.
HOME	Moves the insertion point to the beginning of the line.
END	Moves the insertion point to the end of the line.
ESC	Clears the command from the display.
F1	Copies one character from a column in the template to the same column in the Command Prompt window. (The template is a memory buffer that holds the last command you typed.)
F2	Searches forward in the template for the next key that you type after you press F2. Doskey.exe inserts the text from the template—up to, but not including, the character you specify.
F3	Copies the remainder of the template to the command line. Doskey.exe begins copying characters from the position in the template that corresponds to the position indicated by the insertion point on the command line.
F4	Deletes all characters from the current insertion point position up to, but not including, the next occurrence of the character that you type after you press F4.
F5	Copies the template into the current command line.
F6	Places an end-of-file character (CTRL+Z) at the current insertion point position.
F7	Displays (in a dialog box) all commands for this program that are stored in memory. Use the UP ARROW key and the DOWN ARROW key to select the command you want, and press ENTER to run the command. You can also note the sequential number in front of the command and use this number in conjunction with the F9 key.
ALT+F7	Deletes all commands stored in memory for the current history buffer.
F8	Displays all commands in the history buffer that start with the characters in the current command.

Key or key combination	Description
F9	Prompts you for a history buffer command number, and then displays the command associated with the number that you specify. Press ENTER to run the command. To display all the numbers and their associated commands, press F7.
ALT+F10	Deletes all macro definitions.

- If you press the INSERT key, you can type text on the **doskey** command line in the midst of existing text without replacing the text. However, after you press ENTER, Doskey.exe returns your keyboard to **Replace** mode. You must press INSERT again to return to **Insert** mode.
- The insertion point changes shape when you use the INSERT key to change from one mode to the other.
- If you want to customize how Doskey.exe works with a program and create **doskey** macros for that program, you can create a batch program that modifies Doskey.exe and starts the program.
- You can use Doskey.exe to create macros that carry out one or more commands. The following table lists special characters that you can use to control command operations when you define a macro.

Character	Description
`$G` or `$g`	Redirects output. Use either of these special characters to send output to a device or a file instead of to the screen. This character is equivalent to the redirection symbol for output (`>`).
`$G$G` or `$g$g`	Appends output to the end of a file. Use either of these double characters to append output to an existing file instead of replacing the data in the file. These double characters are equivalent to the append redirection symbol for output (`>>`).
`$L` or `$l`	Redirects input. Use either of these special characters to read input from a device or a file instead of from the keyboard. This character is equivalent to the redirection symbol for input (`<`).
`$B` or `$b`	Sends macro output to a command. These special characters are equivalent to using the pipe `(` and `*`.

Character	Description
`$T` or `$t`	Separates commands. Use either of these special characters to separate commands when you create macros or type commands on the **doskey** command line. These special characters are equivalent to using the ampersand (`&`) on a command line.
`$$`	Specifies the dollar-sign character (`$`).
`$1` through `$9`	Represent any command-line information you want to specify when you run the macro. The special characters `$1` through `$9` are batch parameters that enable you to use different data on the command line each time you run the macro. The `$1` character in a **doskey** command is similar to the `%1` character in a batch program.
`$*`	Represents all the command-line information that you want to specify when you type the macro name. The special character `$*` is a replaceable parameter that is similar to the batch parameters `$1` through `$9`, with one important difference: everything you type on the command line after the macro name is substituted for the `$*` in the macro.

- To run a macro, type the macro name at the command prompt, starting at the first position. If the macro was defined with `$*` or any of the batch parameters `$1` through `$9`, use a space to separate the parameters. You cannot run a **doskey** macro from a batch program.
- If you always use a particular command with specific command-line options, you can create a macro that has the same name as the command. To specify whether you want to run the macro or the command, follow these guidelines:
  - To run the macro, type the macro name at the command prompt. Do not add a space before the macro name.
  - To run the command, insert one or more spaces at the command prompt, and then type the command name.

Examples

The **/macros** and **/history** command-line options are useful for creating batch programs to save macros and commands. For example, to store all current **doskey** macros, type:

```
doskey /macros > macinit
```

To use the macros stored in Macinit, type:

```
doskey /macrofile=macinit
```

To create a batch program named Tmp.bat that contains recently used commands, type:

```
doskey /history> tmp.bat
```

To define a macro with multiple commands, use `$t` to separate commands, as follows:

```
doskey tx=cd temp$tdir/w $*
```

In the preceding example, the TX macro changes the current directory to Temp and then displays a directory listing in wide display format. You can use `$*` at the end of the macro to append other command-line options to **dir** when you run the tx option.

The following macro uses a batch parameter for a new directory name:

```
doskey mc=md $1$tcd $1
```

The macro creates a new directory and then changes to the new directory from the current directory.

To use the preceding macro to create and change to a directory named *Books*, type:

```
mc books
```

To create a **doskey** macro for a program called *Ftp.exe*, include **/exename** as follows:

```
doskey /exename=ftp.exe go=open 172.27.1.100$tmget *.TXT c:\reports$tbye
```

To use the preceding macro, start FTP. At the FTP prompt, type:

```
go
```

FTP runs the **open**, **mget**, and **bye** commands.

To create a macro that quickly and unconditionally formats a disk, type:

```
doskey qf=format $1 /q /u
```

To quickly and unconditionally format a disk in drive A, type:

```
qf a:
```

To delete a macro called *vlist*, type:

```
doskey vlist =
```

Related links

- Command-Line Syntax Key

driverquery

Article • 02/03/2023

Enables an administrator to display a list of installed device drivers and their properties. If used without parameters, **driverquery** runs on the local computer.

Syntax

```
driverquery [/s <system> [/u [<domain>\]<username> [/p <password>]]] [/fo
{table | list | csv}] [/nh] [/v | /si]
```

Parameters

Parameter	Description
/s `<system>`	Specifies the name or IP address of a remote computer. Do not use backslashes. The default is the local computer.
/u `[<domain>]` `<username>`	Runs the command with the credentials of the user account as specified by *user* or *domain\user*. By default, */s* uses the credentials of the user who is currently logged on to the computer that is issuing the command. **/u** can't be used unless **/s** is specified.
/p `<password>`	Specifies the password of the user account that is specified in the **/u** parameter. **/p** cannot be used unless **/u** is specified.
/fo table	Formats the output as a table. This is the default.
/fo list	Formats the output as a list.
/fo csv	Formats the output with comma-separated values.
/nh	Omits the header row from the displayed driver information. Not valid if the **/fo** parameter is set to **list**.
/v	Displays verbose output. **/v** is not valid for signed drivers.
/si	Provides information about signed drivers.
/?	Displays help at the command prompt.

Examples

To display a list of installed device drivers on the local computer, type:

```
driverquery
```

To display the output in a comma-separated values (CSV) format, type:

```
driverquery /fo csv
```

To hide the header row in the output, type:

```
driverquery /nh
```

To use the **driverquery** command on a remote server named *server1* using your current credentials on the local computer, type:

```
driverquery /s server1
```

To use the **driverquery** command on a remote server named *server1* using the credentials for *user1* on the domain *maindom*, type:

```
driverquery /s server1 /u maindom\user1 /p p@ssw3d
```

Related links

- Command-Line Syntax Key

DTrace

Article • 04/19/2024

Beginning with Windows Server 2025, `dtrace` is included as a built-in tool. DTrace is a command-line utility that allows users to monitor and debug their system performance in real-time. With `dtrace`, users can dynamically instrument the kernel and user-space code without modifying the code itself.

This powerful tool supports various data collection and analysis techniques, including aggregations, histograms, and tracing of user-level events. Probes can be specified in `dtrace` scripts where the script defines the probes to be monitored and the actions to be taken when the probes fire. A probe is a specific point in the code where data can be collected to perform these actions.

> **Note**
>
> This built-in port of `dtrace` differs from the MSI installer of DTrace for Windows surrounding parameters and other capabilities. To learn more about DTrace for Windows, see DTrace on Windows.
>
> For a comprehensive guide on using DTrace, see the Dynamic Tracing Guide.

Enable DTrace

Before `dtrace` can be used, it must first be enabled. To enable `dtrace`, open an elevated command prompt or PowerShell as admin and run:

```
bcdedit /set dtrace on
```

A reboot is required for this change to take effect.

Syntax

```
dtrace [-BCeFhlqSvVwYZ] [-b bufsz] [-c cmd] [-D name[=def]] [-I path]
[-L path] [-o output] [-p pid] [-s script] [-U name] [-x opt[=val]] [-X
a|c|s|t]
```

```
[-y symbol path]

[-P provider [[ predicate ] action ]] [-m [ provider: ]
module [[ predicate ] action ]] [-f [[ provider: ] module: ]
func [[ predicate ] action ]] [-n [[[ provider: ] module: ] func: ]
name [[ predicate ] action ]] [-i probe-id [[ predicate ] action ]] [ args
... ]
```

> **Note**
>
> The parameters for dtrace.exe are *case-sensitive*. Make sure to use the correct casing when specifying parameters to avoid any unexpected behavior.

Expand table

Parameter	Description
-b `<bufsz>`	Sets the size of the buffer used to store trace data, where *bufsz* is the desired size of the buffer in bytes, kilobytes (**k**), megabytes (**m**), or gigabytes (**g**).
-c `<cmd>`	Runs the specified command and exits once it completes, where *cmd* is the command that you want to run before starting the trace. If more than one instance of **-c** is used, dtrace exits when all commands finish running and reports the exit status for each child process.
-C	Runs the ucpp preprocessor on script files before running the trace.
-D `<name>` = `<def>`	Defines a symbol when invoking the preprocessor, where *name* is the name of the symbol to define, and *def* is an optional value to assign to the symbol.
-e	Exits after compiling a request but before enabling probes.
-f	Enables or lists probes that match the specified function name.
-F	Combines the trace output by function, making it easier to analyze.
-h	Generates a header file with definitions for static probes.
-i `<probe-id>`	Enables or lists probes that match the specified probe ID, where *probe-id* is the identifier for the probe to be traced.
-I `<path>`	Adds the specified directory to the preprocessor search path, where *path* is the directory that you want to add that contain the *#include* files.
-l	Lists probes that match specified criteria based on the **-P**, **-m**, **-f**, **-n**, **-i**, and **-s** parameters. If these parameters aren't specified, all probes are listed.
-L `<path>`	Adds the specified directory to the library search path, where *path* is the library directory that you want to add that contain common definitions.

Parameter	Description
-m	Enables or lists probes that match the specified module name in an argument using the format *provider:module* or *module*. If qualifiers aren't specified besides the module name, all probes with that module name are matched.
-n	Enables or lists probes that match the specified probe name in an argument using the format *provider:module:function:name*, *module:function:name*, *function:name*, or *name*. If qualifiers aren't specified besides the probe name, all probes with that name are matched.
-o `<output>`	Sets the output file for the trace data, where *output* is the name of the file that you want to use for the trace data.
-p `<pid>`	Grabs the specified process-ID (PID) and caches its symbol tables, which can be used to analyze the program's behavior.
-P `<provider>`	Enables or lists probes that match the specified provider name, where *provider* is the name of the provider. More than one instance of the **-P** parameter can be used at the same time.
-q	Sets quiet mode, which only outputs explicitly traced data.
-s `<script>`	Enables or lists probes according to the specified D script, where *script* is the name of the script that you want to run. If **-e** is specified, the program is compiled but no data collection is performed. If **-l** is specified, the program is compiled and the list of probes matched are displayed, but no data collection is performed. If **-e** or **-l** aren't specified, the program is compiled, data collection is performed according to the probes specified and tracing begins.
-S	Prints the D-language compiler intermediate code for debugging to *stderr*.
-U `<name>`	Undefines a symbol when invoking the preprocessor, where *name* is the name of the symbol that you want to undefine.
-v	Sets verbose mode, which reports stability attributes and arguments.
-V	Displays the version of the dtrace API.
-w	Permits destructive actions when specified with the **-s**, **-P**, **-m**, **-f**, **-n**, or **-i** parameters. Destructive actions can include actions such as modifying kernel variables, changing the behavior of system calls, or crashing the system.
-x `<opt>` = `<val>`	Enables or modifies the compiler and tracing options, where *opt* is the name of the option that you want to enable or modify, and *val* is an optional value.
-X `<a|c|s|t>`	Controls how strict the C code being compiled adheres to the ISO C standard when invoking the cpp. The available arguments are: • `-Xa` (default): provides ISO C plus K&R compatibility extensions with semantic changes required by ISO C. The predefined macro __STDC__ has a value of **0** when cpp is invoked.

Parameter	Description
	• `-Xc` (conformance): Provides a strict conformant of ISO C without K&R C compatibility extensions. The predefined macro __STDC__ has a value of **1** when cpp is invoked. • `-Xs` (K&R C): Provides K&R C only, and the __STDC__ macro isn't defined when cpp is invoked. • `-Xt` (transition): Provides ISO C plus K&R C compatibility extensions without semantic changes required by ISO C. The predefined macro __STDC__ has a value of **0** when cpp is invoked.
-y `<symbol path>`	Sets the symbol search path for the dtrace script to resolve, where *symbol path* is the path to the shared library or directory that contains the symbols. To learn more, see Symbol Paths.
-Y	Uses the **default** symbol search path for the dtrace script.
-Z	Permits probe descriptions that match zero probes for debugging.

The following list describes the remaining descriptions:

- **Predicate**: The predicate is enclosed in forward slashes (`/ /`) and is a D-expression, which is a boolean expression that can reference variables, constants, and functions. Predicates can be used to filter the output of `dtrace` based on these events. This expression is evaluated each time a probe fires. If the predicate evaluates to true, the associated action is executed.

- **Action**: The action is enclosed in curly braces (`{ }`) and is a set of D-language statements that are executed when a probe fires and its associated predicate, if any, evaluates to true. Actions can be used to print output statements, record data, or perform other operations, such as sending a signal or modifying a variable.

- **Module**: A component of a provider that contains a set of related probes. Modules can be specified in `dtrace` scripts to limit the scope of the script to a specific module or set of modules.

- **Func**: A function name that is associated with a probe. For example, the `syscall::NtReadFile` probe is associated with the `read` function. Functions can be specified in `dtrace` scripts to limit the scope of the script to a specific function or set of functions.

- **Args**: The arguments that are passed to the action expression when a probe fires and its associated predicate, if any, evaluates to true. Args can be used to capture data from the probe context, such as the values of function arguments or system

call return values. Args can also be used to pass data between probes or to modify the behavior of the script.

Examples

To trace all system calls, print the name of the executable and the name of the system call being made, run:

Windows Command Prompt

```
dtrace -n 'syscall:::entry { printf("%s called syscall %s", execname,
probefunc); }'
```

This command traces the "function_name" function in the process with the specified PID and prints the name of the function, the PID of the process calling it, and the name of the executable.

Windows Command Prompt

```
dtrace -n 'pid$target::function_name:entry { printf("Function %s called by
process %d (%s)", probefunc, pid, execname); }' -p <PID>
```

For further examples on using `dtrace`, see Getting started with DTrace - One line commands.

See also

- DTrace Programming
- DTrace Code Samples
- DTrace Event Tracing for Windows
- DTrace Live Dump

echo

Article • 02/16/2024

Displays messages or turns on or off the command echoing feature. If used without parameters, **echo** displays the current echo setting.

Syntax

```
echo [<message>]
echo [on | off]
```

Parameters

Expand table

Parameter	Description
[on | off]	Turns on or off the command echoing feature. Command echoing is on by default.
`<message>`	Specifies the text to display on the screen.
/?	Displays help at the command prompt.

Remarks

- The `echo <message>` command is more useful when **echo** is turned off. To display a message that is several lines long without displaying any commands, you can include several `echo <message>` commands after the **echo off** command in your batch program.
- After **echo** is turned off, the command prompt doesn't appear in the Command Prompt window. To display the command prompt, type **echo on.**
- If used in a batch file, **echo on** and **echo off** don't affect the setting at the command prompt.
- If there's an empty variable in a batch file while using **echo**, it displays "ECHO is off". To prevent seeing this message, and produce a blank line instead, place a colon (`:`) between **echo** and the variable. For example, `echo:%var%`.

- To prevent echoing a particular command in a batch file, insert an (`@`) sign in front of the command. To prevent echoing all commands in a batch file, include the **echo off** command at the beginning of the file.
- To display an exclamation mark (`!`) in batch scripts, wrap the word or phrase in double quotes followed by a caret before the exclamation mark (`"Hello World^!"`). Alternatively, a double caret (`^^`) can be used without the need for double quotes (`Hello World^^!`).
- To display a pipe (`|`), ampersand (`&`) or redirection character (`<` or `>`) when you're using **echo**, use a caret (`^`) immediately before that character. For example, `^|`, `^&`, `^>`, or `^<`. To display a caret, type two carets in succession (`^^`).
- When inside a block terminated by parentheses (`()`), both opening and closing parentheses must also be escaped using the caret (`^`) immediately before each one. For example, `This is ^(now^) correct` will correctly display `This is (now) correct`.

Examples

To display the current **echo** setting, type:

```
echo
```

To echo a blank line on the screen, type:

```
echo.
```

> ⓘ **Note**
>
> Don't include a space before the period. Otherwise, the period appears instead of a blank line.

To prevent echoing commands at the command prompt, type:

```
```

```
echo off
```

> **Note**
>
> When **echo** is turned off, the command prompt doesn't appear in the Command Prompt window. To display the command prompt again, type **echo on**.

To prevent all commands in a batch file (including the **echo off** command) from displaying on the screen, on the first line of the batch file type:

```
@echo off
```

You can use the **echo** command as part of an **if** statement. For example, to search the current directory for any file with the .rpt file name extension, and to echo a message if such a file is found, type:

```
if exist *.rpt echo The report has arrived.
```

The following batch file searches the current directory for files with the .txt file name extension, and displays a message indicating the results of the search:

```
@echo off
if not exist *.txt (
echo This directory contains no text files.
) else (
   echo This directory contains the following text file^(s^):
   echo.
   dir /b *.txt
   )
```

If no .txt files are found when the batch file is run, the following message displays:

```
This directory contains no text files.
```

If .txt files are found when the batch file is run the following output displays (for this example, assume the files File1.txt, File2.txt, and File3.txt exist):

```
This directory contains the following text file(s):

File1.txt
File2.txt
File3.txt
```

Related links

- Command-Line Syntax Key

edit

Article • 02/03/2023

Starts the MS-DOS Editor, which creates and changes ASCII text files.

Syntax

```
edit [/b] [/h] [/r] [/s] [/<nnn>] [[<drive>:][<path>]<filename> [<filename2> [...]]]
```

Parameters

Parameter	Description
`[<drive>:][<path>]<filename> [<filename2> [...]]`	Specifies the location and name of one or more ASCII text files. If the file doens't exist, MS-DOS Editor creates it. If the file exists, MS-DOS Editor opens it and displays its contents on the screen. The *filename* option can contain wildcard characters (* and ?). Separate multiple file names with spaces.
/b	Forces monochrome mode, so that MS-DOS Editor displays in black and white.
/h	Displays the maximum number of lines possible for the current monitor.
/r	Loads file(s) in read-only mode.
/s	Forces the use of short filenames.
`<nnn>`	Loads binary file(s), wrapping lines to *nnn* characters wide.
/?	Displays help at the command prompt.

Remarks

- For additional help, open MS-DOS Editor, and then press the F1 key.
- Some monitors don't support the display of shortcut keys by default. If your monitor doesn't display shortcut keys, use **/b**.

Examples

To open MS-DOS Editor, type:

```
edit
```

To create and edit a file named *newtextfile.txt* in the current directory, type:

```
edit newtextfile.txt
```

Related links

- Command-Line Syntax Key

endlocal

Article • 02/03/2023

Ends localization of environment changes in a batch file, and restores environment variables to their values before the corresponding **setlocal** command was run.

Syntax

```
endlocal
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.

Remarks

- The **endlocal** command has no effect outside a script or batch file.
- There is an implicit **endlocal** command at the end of a batch file.
- If command extensions are enabled (command extensions are enabled by default), the **endlocal** command restores the state of command extensions (that is, enabled or disabled) to what it was before the corresponding **setlocal** command was run.

> **Note**
>
> For more information about enabling and disabling command extensions, see the **Cmd command**.

Examples

You can localize environment variables in a batch file. For example, the following program starts the *superapp* batch program on the network, directs the output to a file, and displays the file in Notepad:

```
@echo off
setlocal
path=g:\programs\superapp;%path%
call superapp>c:\superapp.out
endlocal
start notepad c:\superapp.out
```

Related links

- Command-Line Syntax Key

erase

Article • 02/03/2023

Deletes one or more files. If you use **erase** to delete a file from your disk, you can't retrieve it.

> **Note**
>
> This command is the same as the **del command**.

Syntax

```
erase [/p] [/f] [/s] [/q] [/a[:]<attributes>] <names>
del [/p] [/f] [/s] [/q] [/a[:]<attributes>] <names>
```

Parameters

Parameter	Description
`<names>`	Specifies a list of one or more files or directories. Wildcards may be used to delete multiple files. If a directory is specified, all files within the directory will be deleted.
/p	Prompts for confirmation before deleting the specified file.
/f	Forces deletion of read-only files.
/s	Deletes specified files from the current directory and all subdirectories. Displays the names of the files as they are being deleted.
/q	Specifies quiet mode. You are not prompted for delete confirmation.
/a[:]`<attributes>`	Deletes files based on the following file attributes: • **r** Read-only files • **h** Hidden files • **i** Not content indexed files • **s** System files • **a** Files ready for archiving • **l** Reparse points • **-** Used as a prefix meaning 'not'

Parameter	Description
/?	Displays help at the command prompt.

Remarks

- If you use the `erase /p` command, you'll see the following message:

  `FileName, Delete (Y/N)?`

  To confirm the deletion, press **Y**. To cancel the deletion and to display the next file name (if you specified a group of files), press **N**. To stop the **erase** command, press CTRL+C.

- If you disable command extension, the **/s** parameter will display the names of any files that weren't found ,instead of displaying the names of files that are being deleted.

- If you specify specific folders in the `<names>` parameter, all of the included files will also be deleted. For example, if you want to delete all of the files in the *\work* folder, type:

  ```
  erase \work
  ```

- You can use wildcards (***** and **?**) to delete more than one file at a time. However, to avoid deleting files unintentionally, you should use wildcards cautiously. For example, if you type the following command:

  ```
  erase *.*
  ```

  The **erase** command displays the following prompt:

  `Are you sure (Y/N)?`

  To delete all of the files in the current directory, press **Y** and then press ENTER. To cancel the deletion, press **N** and then press ENTER.

  > ⓘ **Note**

Before you use wildcard characters with the **erase** command, use the same wildcard characters with the **dir** command to list all the files that will be deleted.

Examples

To delete all the files in a folder named Test on drive C, type either of the following:

```
erase c:\test
erase c:\test\*.*
```

To delete all files with the .bat file name extension from the current directory, type:

```
erase *.bat
```

To delete all read-only files in the current directory, type:

```
erase /a:r *.*
```

Related links

- Command-Line Syntax Key
- del command

eventcreate

Article • 02/03/2023

Enables an administrator to create a custom event in a specified event log.

> **ⓘ Important**
>
> Custom events can't be written to the security log.

Syntax

```
eventcreate [/s <computer> [/u <domain\user> [/p <password>]] {[/l
{APPLICATION|SYSTEM}]|[/so <srcname>]} /t
{ERROR|WARNING|INFORMATION|SUCCESSAUDIT|FAILUREAUDIT} /id <eventID> /d
<description>
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
/u `<domain\user>`	Runs the command with the account permissions of the user specified by `<user>` or `<domain\user>`. The default is the permissions of the current logged on user on the computer issuing the command.
/p `<password>`	Specifies the password of the user account that is specified in the **/u** parameter.
/l `{APPLICATION | SYSTEM}`	Specifies the name of the event log where the event will be created. The valid log names are **APPLICATION** or **SYSTEM**.
/so `<srcname>`	Specifies the source to use for the event. A valid source can be any string and should represent the application or component that is generating the event.
/t `{ERROR | WARNING | INFORMATION | SUCCESSAUDIT | FAILUREAUDIT}`	Specifies the type of event to create. The valid types are **ERROR**, **WARNING**, **INFORMATION**, **SUCCESSAUDIT**, and **FAILUREAUDIT**.

Parameter	Description
/id `<eventID>`	Specifies the event ID for the event. A valid ID is any number from 1 to 1000.
/d `<description>`	Specifies the description to use for the newly created event.
/?	Displays help at the command prompt.

Examples

The following examples show how you can use the **eventcreate** command:

```
eventcreate /t ERROR /id 100 /l application /d "Create event in application log"
eventcreate /t INFORMATION /id 1000 /d "Create event in WinMgmt source"
eventcreate /t ERROR /id 201 /so winword /l application /d "New src Winword in application log"
eventcreate /s server /t ERROR /id 100 /l application /d "Remote machine without user credentials"
eventcreate /s server /u user /p password /id 100 /t ERROR /l application /d "Remote machine with user credentials"
eventcreate /s server1 /s server2 /u user /p password /id 100 /t ERROR /d "Creating events on Multiple remote machines"
eventcreate /s server /u user /id 100 /t WARNING /d "Remote machine with partial user credentials"
```

Related links

- Command-Line Syntax Key

evntcmd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configures the translation of events to traps, trap destinations, or both based on information in a configuration file.

Syntax

```
evntcmd [/s <computername>] [/v <verbositylevel>] [/n] <filename>
```

Parameters

Parameter	Description
/s `<computername>`	Specifies, by name, the computer on which you want to configure the translation of events to traps, trap destinations, or both. If you do not specify a computer, the configuration occurs on the local computer.
/v `<verbositylevel>`	Specifies which types of status messages appear as traps and trap destinations are configured. This parameter must be an integer between 0 and 10. If you specify 10, all types of messages appear, including tracing messages and warnings about whether trap configuration was successful. If you specify 0, no messages appear.
/n	Specifies that the SNMP service should not be restarted if this computer receives trap configuration changes.
`<filename>`	Specifies, by name, the configuration file that contains information about the translation of events to traps and trap destinations you want to configure.
/?	Displays help at the command prompt.

Remarks

- if you want to configure traps but not trap destinations, you can create a valid configuration file by using Event to Trap Translator, which is a graphical utility. If you have the SNMP service installed, you can start Event to Trap Translator by

typing **evntwin** at a command prompt. After you have defined the traps you want, click **Export** to create a file suitable for use with **evntcmd**. You can use Event to Trap Translator to easily create a configuration file and then use the configuration file with **evntcmd** at the command prompt to quickly configure traps on multiple computers.

- The syntax for configuring a trap is as follows:

```
#pragma add <eventlogfile> <eventsource> <eventID> [<count> [<period>]]
```

  Where the text following is true:

  - **#pragma** must appear at the beginning of every entry in the file.
  - The parameter **add** specifies that you want to add an event to trap configuration.
  - The parameters **eventlogfile**, **eventsource**, and **eventID** are required, and where **eventlogfile** specifies the file in which the event is recorded, **eventsource** specifies the application that generates the event and **eventID** specifies the unique number that identifies each event.

  To determine what values correspond to each event, start the Event to Trap Translator by typing **evntwin** at a command prompt. Click **Custom**, and then click **edit**. Under **Event Sources**, browse the folders until you locate the event you want to configure, click it, and then click **add**. Information about the event source, the event log file, and the event ID appear under **Source, Log**, and **Trap specific ID**, respectively.

  - The **count** parameter is optional, and it specifies how many times the event must occur before a trap message is sent. If you don't use this parameter, the trap message is sent after the event occurs once.
  - The **period** parameter is optional, but it requires you to use the **count** parameter. The **period** parameter specifies a length of time (in seconds) during which the event must occur the number of times specified with the **count** parameter before a trap message is sent. If you don't use this parameter, a trap message is sent after the event occurs the number of times specified with the ***count*** parameter, no matter how much time elapses between occurrences.

- The syntax for removing a trap is as follows:

```
```

```
#pragma delete <eventlogfile> <eventsource> <eventID>
```

Where the text following is true:

- **#pragma** must appear at the beginning of every entry in the file.
- The parameter **delete** specifies that you want to remove an event to trap configuration.
- The parameters **eventlogfile**, **eventsource**, and **eventID** are required, and where **eventlogfile** specifies the file in which the event is recorded, **eventsource** specifies the application that generates the event and **eventID** specifies the unique number that identifies each event.

To determine what values correspond to each event, start the Event to Trap Translator by typing **evntwin** at a command prompt. Click **Custom**, and then click **edit**. Under **Event Sources**, browse the folders until you locate the event you want to configure, click it, and then click **add**. Information about the event source, the event log file, and the event ID appear under **Source, Log**, and **Trap specific ID**, respectively.

- The syntax for configuring a trap destination is as follows:

```
#pragma add_TRAP_DEST <communityname> <hostID>
```

Where the text following is true:

- **#pragma** must appear at the beginning of every entry in the file.
- The parameter **add_TRAP_DEST** specifies that you want trap messages to be sent to a specified host within a community.
- The parameter **communityname** specifies, by name, the community in which trap messages are sent.
- The parameter **hostID** specifies, by name or IP address, the host to which you want trap messages to be sent.

- The syntax for removing a trap destination is as follows:

```
```

```
#pragma delete_TRAP_DEST <communityname> <hostID>
```

Where the text following is true:

- **#pragma** must appear at the beginning of every entry in the file.
- The parameter **delete_TRAP_DEST** specifies that you do not want trap messages to be sent to a specified host within a community.
- The parameter **communityname** specifies, by name, the community to which trap messages shouldn't be sent.
- The parameter **hostID** specifies, by name or IP address, the host to which you don't want trap messages to be sent.

Examples

The following examples illustrate entries in the configuration file for the **evntcmd** command. They are not designed to be typed at a command prompt.

To send a trap message if the Event Log service is restarted, type:

```
#pragma add System Eventlog 2147489653
```

To send a trap message if the Event Log service is restarted twice in three minutes, type:

```
#pragma add System Eventlog 2147489653 2 180
```

To stop sending a trap message whenever the Event Log service is restarted, type:

```
#pragma delete System Eventlog 2147489653
```

To send trap messages within the community named *Public* to the host with the IP address *192.168.100.100*, type:

```
#pragma add_TRAP_DEST public 192.168.100.100
```

To send trap messages within the community named *Private* to the host named *Host1*, type:

```

#pragma add_TRAP_DEST private Host1
```

To stop sending trap messages within the community named *Private* to the same computer on which you are configuring trap destinations, type:

```

#pragma delete_TRAP_DEST private localhost
```

Related links

- Command-Line Syntax Key

expand

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Expands one or more compressed files. You can also use this command to retrieve compressed files from distribution disks.

The **expand** command can also run from the Windows Recovery Console, using different parameters. For more information, see Windows Recovery Environment (WinRE).

Syntax

```
expand [-r] <source> <destination>
expand -r <source> [<destination>]
expand -i <source> [<destination>]
expand -d <source>.cab [-f:<files>]
expand <source>.cab -f:<files> <destination>
```

Parameters

Parameter	Description
-r	Renames expanded files.
source	Specifies the files to expand. *Source* can consist of a drive letter and colon, a directory name, a file name, or a combination of these. You can use wildcards (* or ?).
destination	Specifies where files are to be expanded. If *source* consists of multiple files and you don't specify **-r**, the *destination* must be a directory that already exists. *Destination* can consist of a drive letter and colon, a directory name, a file name, or a combination of these. Destination `file | path` specification.
-i	Renames expanded files but ignores the directory structure.
-d	Displays a list of files in the source location. Doesn't expand or extract the files.
-f:`<files>`	Specifies the files in a cabinet (.cab) file that you want to expand. You can use wildcards (* or ?).

Parameter	Description
/?	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

extract / extrac32

Article • 02/03/2023

Extracts files from a cabinet or source.

> **Note**
>
> On Windows Server 2016 and newer, and on Windows 10, the program file Extract.exe is neither provided nor supported. It is replaced by Extrac32.exe, originally part of Internet Explorer, now part of the operating system.

Syntax

Extract.exe

```
extract [/y] [/a] [/d | /e] [/l dir] cabinet [filename ...]
extract [/y] source [newname]
extract [/y] /c source destination
```

Parameters

Parameter	Description
cabinet	Use if you want to extract two or more files.
filename	Name of the file to extract from the cabinet. Wild cards and multiple filenames (separated by blanks) may be used.
source	Compressed file (a cabinet with only one file).
newname	New filename to give the extracted file. If not supplied, the original name is used.
/a	Process ALL cabinets. Follows cabinet chain starting in first cabinet mentioned.
/c	Copy source file to destination (to copy from DMF disks).
/d	Display cabinet directory (use with filename to avoid extract).
/e	Extract (use instead of . to extract all files).

Parameter	Description
/l dir	Location to place extracted files (default is current directory).
/y	Don't prompt before overwriting an existing file.

Extrac32.exe

> ⓘ Note
>
> Extrac32.exe can be used from the command line, but does not display any output on the console. Redirect the help output through the **more** command, like this: `extrac32.exe /? | more`

```
Extrac32 [/Y] [/A] [/D | /E] [/L dir] cabinet [filename ...]
Extrac32 [/Y] source [newname]
Extrac32 [/Y] /C source destination
```

Parameters

Parameter	Description
cabinet	Cabinet file (contains two or more files).
filename	Name of the file to extract from the cabinet. Wild cards and multiple filenames (separated by blanks) may be used.
source	Compressed file (a cabinet with only one file).
newname	New filename to give the extracted file. If not supplied, the original name is used.
/A	Process ALL cabinets. Follows cabinet chain starting in first cabinet mentioned.
/C	Copy source file to destination (to copy from DMF disks).
/D	Display cabinet directory (use with filename to avoid extract).
/E	Extract (use instead of . to extract all files).
/L dir	Location to place extracted files (default is current directory).
/Y	Do not prompt before overwriting an existing file.

Related links

- Command-Line Syntax Key

fc

Article • 02/03/2023

Compares two files or sets of files and displays the differences between them.

Syntax

```
fc /a [/c] [/l] [/lb<n>] [/n] [/off[line]] [/t] [/u] [/w] [/<nnnn>]
[<drive1>:][<path1>]<filename1> [<drive2>:][<path2>]<filename2>
fc /b [<drive1:>][<path1>]<filename1> [<drive2:>][<path2>]<filename2>
```

Parameters

Parameter	Description
/a	Abbreviates the output of an ASCII comparison. Instead of displaying all of the lines that are different, **fc** displays only the first and last line for each set of differences.
/b	Compares the two files in binary mode, byte by byte, and does not attempt to resynchronize the files after finding a mismatch. This is the default mode for comparing files that have the following file extensions: .exe, .com, .sys, .obj, .lib, or .bin.
/c	Ignores the letter case.
/l	Compares the files in ASCII mode, line-by-line, and attempts to resynchronize the files after finding a mismatch. This is the default mode for comparing files, except files with the following file extensions: .exe, .com, .sys, .obj, .lib, or .bin.
/lb`<n>`	Sets the number of lines for the internal line buffer to *N*. The default length of the line buffer is 100 lines. If the files that you are comparing have more than 100 consecutive differing lines, **fc** cancels the comparison.
/n	Displays the line numbers during an ASCII comparison.
/off[line]	Doesn't skip files that have the offline attribute set.
/t	Prevents **fc** from converting tabs to spaces. The default behavior is to treat tabs as spaces, with stops at each eighth character position.
/u	Compares files as Unicode text files.

Parameter	Description
/w	Compresses white space (that is, tabs and spaces) during the comparison. If a line contains many consecutive spaces or tabs, **/w** treats these characters as a single space. When used with **/w**, **fc** ignores white space at the beginning and end of a line.
/`<nnnn>`	Specifies the number of consecutive lines that must match following a mismatch, before **fc** considers the files to be resynchronized. If the number of matching lines in the files is less than *nnnn*, **fc** displays the matching lines as differences. The default value is 2.
`[<drive1>:]` `[<path1>]` `<filename1>`	Specifies the location and name of the first file or set of files to compare. *filename1* is required.
`[<drive2>:]` `[<path2>]` `<filename2>`	Specifies the location and name of the second file or set of files to compare. *filename2* is required.
/?	Displays help at the command prompt.

Remarks

- This command is implemented by c:\WINDOWS\fc.exe. You can use this command within PowerShell, but be sure to spell out the full executable (fc.exe) since 'fc' is also an alias for Format-Custom.
- When you use **fc** for an ASCII comparison, **fc** displays the differences between two files in the following order:
  - Name of the first file
  - Lines from *filename1* that differ between the files
  - First line to match in both files
  - Name of the second file
  - Lines from *filename2* that differ
  - First line to match
- **/b** displays mismatches that are found during a binary comparison in the following syntax:

  `\<XXXXXXXX: YY ZZ>`

The value of *XXXXXXXX* specifies the relative hexadecimal address for the pair of bytes, measured from the beginning of the file. Addresses start at 00000000. The hexadecimal values for *YY* and *ZZ* represent the mismatched bytes from *filename1* and *filename2*, respectively.

- You can use wildcard characters (***** and **?**) in *filename1* and *filename2*. If you use a wildcard in *filename1*, **fc** compares all the specified files to the file or set of files specified by *filename2*. If you use a wildcard in *filename2*, **fc** uses the corresponding value from *filename1*.

- When comparing ASCII files, **fc** uses an internal buffer (large enough to hold 100 lines) as storage. If the files are larger than the buffer, **fc** compares what it can load into the buffer. If **fc** doesn't find a match in the loaded portions of the files, it stops and displays the following message:

  `Resynch failed. Files are too different.`

  When comparing binary files that are larger than the available memory, **fc** compares both files completely, overlaying the portions in memory with the next portions from the disk. The output is the same as that for files that fit completely in memory.

Examples

To make an ASCII comparison of two text files, *monthly.rpt* and *sales.rpt*, and display the results in abbreviated format, type:

```
fc /a monthly.rpt sales.rpt
```

To make a binary comparison of two batch files, *profits.bat* and *earnings.bat*, type:

```
fc /b profits.bat earnings.bat
```

Results similar to the following appear:

```
00000002: 72 43
00000004: 65 3A
0000000E: 56 92
```

```
000005E8: 00 6E
FC: earnings.bat longer than profits.bat
```

If the profits.bat and earnings.bat files are identical, **fc** displays the following message:

```
Comparing files profits.bat and earnings.bat
FC: no differences encountered
```

To compare every .bat file in the current directory with the file *new.bat*, type:

```
fc *.bat new.bat
```

To compare the file *new.bat* on drive C with the file *new.bat* on drive D, type:

```
fc c:new.bat d:*.bat
```

To compare each batch file in the root directory on drive C to the file with the same name in the root directory on drive D, type:

```
fc c:*.bat d:*.bat
```

Related links

- Command-Line Syntax Key

find

Article • 02/03/2023

Searches for a string of text in a file or files, and displays lines of text that contain the specified string.

Syntax

```
find [/v] [/c] [/n] [/i] [/off[line]] <"string"> [[<drive>:][<path>]
<filename>[...]]
```

Parameters

Parameter	Description
/v	Displays all lines that don't contain the specified `<string>`.
/c	Counts the lines that contain the specified `<string>` and displays the total.
/n	Precedes each line with the file's line number.
/i	Specifies that the search is not case-sensitive.
[/off[line]]	Doesn't skip files that have the offline attribute set.
`<"string">`	Required. Specifies the group of characters (enclosed in quotation marks) that you want to search for.
`[<drive>:][<path>] <filename>`	Specifies the location and name of the file in which to search for the specified string.
/?	Displays help at the command prompt.

Exit codes

Exit code	Description
0	The searched string was found
1	Searched string not found

Exit code	Description
2	Searched file not found or invalid command line switch was given

Remarks

- If you don't use **/i**, this command searches for exactly what you specify for *string*. For example, this command treats the characters `a` and `A` differently. If you use **/i**, however, the search becomes case insensitive, and it treats `a` and `A` as the same character.
- If the string you want to search for contains quotation marks, you must use double quotation marks for each quotation mark contained within the string (for example, """This string contains quotation marks""").
- If you omit a file name, this command acts as a filter, taking input from the standard input source (usually the keyboard, a pipe (|), or a redirected file) and then displays any lines that contain *string*.
- To exit the console search use `CTRL-X` or `CTRL-z`.
- You can type parameters and command-line options for the **find** command in any order.
- You can't use wildcards (***** and **?**) in the searched string. To search for a string with wild cards and regex patterns, you can use the **FINDSTR** command.
- If you use **/c** and **/v** in the same command line, this command displays a count of the lines that don't contain the specified string. If you specify **/c** and **/n** in the same command line, **find** ignores **/n**.
- This command doesn't recognize carriage returns. When you use this command to search for text in a file that includes carriage returns, you must limit the search string to text that can be found between carriage returns (that is, a string that is not likely to be interrupted by a carriage return). For example, this command doesn't report a match for the string tax file if a carriage return occurs between the words tax and file.
- The command accepts wildcards for file names. When searching in file (or files) it will print the file of the processed file preceded by ten dashes.
- **Find** command cannot read alternate data streams. For searching in alternate data streams use **findstr**, **more** or **for /f** commands.

Examples

To display all lines from *pencil.md* that contain the string *pencil sharpener*, type:

```
find "pencil sharpener" pencil.md
```

To find the text, "*The scientists labeled their paper for discussion only. It is not a final report.*" (including the quotes) in the *report.txt* file, type:

```
find """The scientists labeled their paper for discussion only. It is not a
final report.""" < report.txt
```

To search for a set of files, you can use wildcards. To search the current directory for files that have the extension *.bat* and that contain the string *PROMPT* ignoring the case, type:

```
find /i "PROMPT" *.bat
```

To find files names in a directory that contain the string *CPU*, use the pipe (|) to direct the output of the *dir* command to the find command as follows:

```
dir c:\temp /s /b | find "CPU"
```

Find all running processes that do NOT contain *agent*:

```
tasklist | find /v /i "agent"
```

Check if a service is running:

```
sc query  Winmgmt | find "RUNNING" >nul 2>&1 && (echo service is started) ||
(echo service is stopped)
```

Related links

- Command-Line Syntax Key
- findstr command

findstr

Article • 02/03/2023

Searches for patterns of text in files.

Syntax

```
findstr [/b] [/e] [/l | /r] [/s] [/i] [/x] [/v] [/n] [/m] [/o] [/p] [/f:
<file>] [/c:<string>] [/g:<file>] [/d:<dirlist>] [/a:<colorattribute>]
[/off[line]] <strings> [<drive>:][<path>]<filename>[ ...]
```

Parameters

Parameter	Description
/b	Matches the text pattern if it is at the beginning of a line.
/e	Matches the text pattern if it is at the end of a line.
/l	Processes search strings literally.
/r	Processes search strings as regular expressions. This is the default setting.
/s	Searches the current directory and all subdirectories.
/i	Ignores the case of the characters when searching for the string.
/x	Prints lines that match exactly.
/v	Prints only lines that don't contain a match.
/n	Prints the line number of each line that matches.
/m	Prints only the file name if a file contains a match.
/o	Prints character offset before each matching line.
/p	Skips files with non-printable characters.
/off[line]	Does not skip files that have the offline attribute set.
/f:`<file>`	Gets a file list from the specified file.
/c:`<string>`	Uses the specified text as a literal search string.

Parameter	Description
/g:`<file>`	Gets search strings from the specified file.
/d:`<dirlist>`	Searches the specified list of directories. Each directory must be separated with a semicolon (;), for example `dir1;dir2;dir3`.
/a:`<colorattribute>`	Specifies color attributes with two hexadecimal digits. Type `color /?` for additional information.
`<strings>`	Specifies the text to search for in *filename*. Required.
`[\<drive>:][<path>] <filename>[...]`	Specifies the location and file or files to search. At least one file name is required.
/?	Displays Help at the command prompt.

Remarks

- All **findstr** command-line options must precede *strings* and *filename* in the command string.
- Regular expressions use both literal characters and meta-characters to find patterns of text, rather than exact strings of characters.
  - A literal character is a character that doesn't have a special meaning in the regular-expression syntax; instead, it matches an occurrence of that character. For example, letters and numbers are literal characters.
  - A meta-character is a symbol with special meaning (an operator or delimiter) in the regular-expression syntax.

    The accepted meta-characters are:

Meta-character	Value
`.`	**Wildcard** - Any character
`*`	**Repeat** - Zero or more occurrences of the previous character or class.
`^`	**Beginning line position** - Beginning of the line.
`$`	**Ending line position** - End of the line.
`[class]`	**Character class** - Any one character in a set.
`[^class]`	**Inverse class** - Any one character not in a set.

Meta-character	Value
`[x-y]`	**Range** - Any characters within the specified range.
`\x`	**Escape** - Literal use of a meta-character.
`\<string`	**Beginning word position** - Beginning of the word.
`string\>`	**Ending word position** - End of the word.

The special characters in regular expression syntax have the most power when you use them together. For example, use the combination of the wildcard character (`.`) and repeat (`*`) character to match any string of characters: `.*`

Use the following expression as part of a larger expression to match any string beginning with *b* and ending with *ing*: `b.*ing`

- To search for multiple strings in a set of files, you must create a text file that contains each search criterion on a separate line.
- Use spaces to separate multiple search strings unless the argument is prefixed with **/c**.

Examples

To search for *hello* or *there* in file *x.y*, type:

```
findstr hello there x.y
```

To search for *hello there* in file *x.y*, type:

```
findstr /c:"hello there" x.y
```

To find all occurrences of the word *Windows* (with an initial capital letter W) in the file *proposal.txt*, type:

```
findstr Windows proposal.txt
```

To search every file in the current directory and all subdirectories that contained the word *Windows*, regardless of the letter case, type:

```
findstr /s /i Windows *.*
```

To find all occurrences of lines that begin with *FOR* and are preceded by zero or more spaces (as in a computer program loop), and to display the line number where each occurrence is found, type:

```
findstr /b /n /r /c:^ *FOR *.bas
```

To list the exact files that you want to search in a text file, use the search criteria in the file *stringlist.txt*, to search the files listed in *filelist.txt*, and then to store the results in the file *results.out*, type:

```
findstr /g:stringlist.txt /f:filelist.txt > results.out
```

To list every file containing the word *computer* within the current directory and all subdirectories, regardless of case, type:

```
findstr /s /i /m \<computer\> *.*
```

To list every file containing the word computer and any other words that begin with comp, (such as compliment and compete), type:

```
findstr /s /i /m \<comp.* *.*
```

Related links

- Command-Line Syntax Key

finger

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about users on a specified remote computer (typically a computer running UNIX) that is running the finger service or daemon. The remote computer specifies the format and output of the user information display. Used without parameters, **finger** displays help.

> **ⓘ Important**
>
> This command is available only if the Internet Protocol (TCP/IP) protocol is installed as a component in the properties of a network adapter in Network Connections.

Syntax

```
finger [-l] [<user>] [@<host>] [...]
```

Parameters

Parameter	Description
-l	Displays user information in long list format.
`<user>`	Specifies the user about which you want information. If you omit the *user* parameter, this command displays information about all users on the specified computer.
`@<host>`	Specifies the remote computer running the finger service where you are looking for user information. You can specify a computer name or IP address.
/?	Displays help at the command prompt.

Remarks

- You must prefix **finger** parameters with a hyphen (-) rather than a slash (/).

- Multiple `user@host` parameters can be specified.

Examples

To display information for *user1* on the computer *users.microsoft.com*, type:

```
finger user1@users.microsoft.com
```

To display information for *all users* on the computer *users.microsoft.com*, type:

```
finger @users.microsoft.com
```

Related links

- Command-Line Syntax Key

flattemp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables or disables flat temporary folders. You must have administrative credentials to run this command.

> **Note**
>
> This command is only available if you have installed the Remote Desktop Session Host role service.

Syntax

```
flattemp {/query | /enable | /disable}
```

Parameters

Parameter	Description
/query	Queries the current setting.
/enable	Enables flat temporary folders. Users will share the temporary folder unless the temporary folder resides in the user's home folder.
/disable	Disables flat temporary folders. Each user's temporary folder will reside in a separate folder (determined by the user's Session ID).
/?	Displays help at the command prompt.

Remarks

- After each user has a unique temporary folder, use `flattemp /enable` to enable flat temporary folders.

- The default method for creating temporary folders for multiple users (usually pointed to by the TEMP and TMP environment variables) is to create subfolders in the **\Temp** folder, by using the logonID as the subfolder name. For example, if the TEMP environment variable points to C:\Temp, the temporary folder assigned to the user logonID 4 is C:\Temp\4.

  Using **flattemp**, you can point directly to the \Temp folder and prevent subfolders from forming. This is useful when you want the user temporary folders to be contained in home folders, whether on an Remote Desktop Session Host server local drive or on a shared network drive. You should use the `flattemp /enable*` command only when each user has a separate temporary folder.

- You might encounter app errors if the user's temporary folder is on a network drive. This occurs when the shared network drive becomes momentarily inaccessible on the network. Because the temporary files of the app are either inaccessible or out of synchronization, it responds as if the disk has stopped. Moving the temporary folder to a network drive is not recommended. The default is to keep temporary folders on the local hard disk. If you experience unexpected behavior or disk-corruption errors with certain applications, stabilize your network or move the temporary folders back to the local hard disk.

- If you disable using separate temporary folders per-session, **flattemp** settings are ignored. This option is set in the Remote Desktop Services Configuration tool.

Examples

To display the current setting for flat temporary folders, type:

```
flattemp /query
```

To enable flat temporary folders, type:

```
flattemp /enable
```

To disable flat temporary folders, type:

```
flattemp /disable
```

Related links

- Command-Line Syntax Key

fondue

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables Windows optional features by downloading required files from Windows Update or another source specified by Group Policy. The manifest file for the feature must already be installed in your Windows image.

Syntax

```
fondue.exe /enable-feature:<feature_name> [/caller-name:<program_name>]
[/hide-ux:{all | rebootrequest}]
```

Parameters

Parameter	Description
/enable-feature: `<feature_name>`	Specifies the name of the Windows optional feature you want to enable. You can only enable one feature per command line. To enable multiple features, use fondue.exe for each feature.
/caller-name: `<program_name>`	Specifies the program or process name when you call fondue.exe from a script or batch file. You can use this option to add the program name to the SQM report if there is an error.
/hide-ux: `{all | rebootrequest}`	Use **all** to hide all messages to the user including progress and permission requests to access Windows Update. If permission is required, the operation will fail. Use **rebootrequest** to only hide user messages asking for permission to reboot the computer. Use this option if you have a script that controls reboot requests.

Examples

To enable Microsoft .NET Framework 4.8, type:

```
fondue.exe /enable-feature:NETFX4
```

To enable Microsoft .NET Framework 4.8, add the program name to the SQM report, and not display messages to the user, type:

```
fondue.exe /enable-feature:NETFX4 /caller-name:Admin.bat /hide-ux:all
```

Related links

- Command-Line Syntax Key
- Microsoft .NET Framework 4.8 Download

for

Article • 10/05/2023

Runs a specified command for each file, within a set of files.

Syntax

```
for {%% | %}<variable> in (<set>) do <command> [<commandlineoptions>]
```

Parameters

Parameter	Description
`{%% | %}<variable>`	Required. Represents a replaceable parameter. Use a single percent sign (`%`) to carry out the **for** command at the command prompt. Use double percent signs (`%%`) to carry out the **for** command within a batch file. Variables are case sensitive, and they must be represented with an alphabetical value such as %**a**, %**b**, or %**c**.
(`<set>`)	Required. Specifies one or more files, directories, or text strings, or a range of values on which to run the command. The parentheses are required.
`<command>`	Required. Specifies the command that you want to carry out on each file, directory, or text string, or on the range of values included in *set*.
`<commandlineoptions>`	Specifies any command-line options that you want to use with the specified command.
/?	Displays help at the command prompt.

Remarks

- You can use this command within a batch file or directly from the command prompt.
- The following attributes apply to the **for** command:
  - This command replaces `% variable` or `%% variable` with each text string in the specified set until the specified command processes all of the files.

- Variable names are case sensitive, global, and no more than 52 can be active at a time.
- To avoid confusion with the batch parameters, `%0` through `%9`, you can use any character for *variable* except the numerals **0** through **9**. For simple batch files, a single character such as `%%f` will work.
- You can use multiple values for *variable* in complex batch files to distinguish different replaceable variables.

- The *set* parameter can represent a single group of files or several groups of files. You can use wildcard characters (***** and **?**) to specify a file set. The following are valid file sets:

```
(*.doc)
(*.doc *.txt *.me)
(jan*.doc jan*.rpt feb*.doc feb*.rpt)
(ar??1991.* ap??1991.*)
```

- When you use this command, the first value in *set* replaces `% variable` or `%% variable`, and then the specified command processes this value. This continues until all of the files (or groups of files) that correspond to the *set* value are processed.
- **In** and **do** aren't parameters, but you must use them with this command. If you omit either of these keywords, an error message appears.
- If command extensions are enabled (that is the default), the following additional forms of **for** are supported:
  - **Directories only:** If *set* contains wildcard characters (***** or **?**), the specified *command* executes for each directory (instead of a set of files in a specified directory) that matches *set*. The syntax is:

```
for /d {%%|%}<Variable> in (<Set>) do <Command>
[<CommandLineOptions>]
```

  - **Recursive:** Walks the directory tree that is rooted at *drive*:*path* and executes the **for** statement in each directory of the tree. If no directory is specified after **/r**,

the current directory is used as the root directory. If *set* is just a single period (.), it only enumerates the directory tree. The syntax is:

```
for /r [[<drive>:]<path>] {%%|%}<variable> in (<set>) do <command>
[<commandlinepptions>]
```

- **Iterating a range of values:** Use an iterative variable to set the starting value (*start#*) and then step through a set range of values until the value exceeds the set ending value (*end#*). **/l** executes the iterative by comparing *start#* with *end#*. If *start#* is less than *end#* the command executes. When the iterative variable exceeds *end#*, the command shell exits the loop. You can also use a negative *step#* to step through a range in decreasing values. For example, (1,1,5) generates the sequence 1 2 3 4 5 and (5,-1,1) generates the sequence 5 4 3 2 1. The syntax is:

```
for /l {%%|%}<variable> in (<start#>,<step#>,<end#>) do <command>
[<commandlinepptions>]
```

- **Iterating and file parsing:** Use file parsing to process command output, strings, and file content. Use iterative variables to define the content or strings that you want to examine, and use the various *parsingkeywords* options to further modify the parsing. Use the *parsingkeywords* token option to specify which tokens should be passed as iterative variables. When used without the token option, **/f** will only examine the first token.

  File parsing consists of reading the output, string, or file content, and then breaking it into individual lines of text and parsing each line into zero or more tokens. The **for** loop is then called with the iterative variable value set to the token. By default, **/f** passes the first blank separated token from each line of each file. Blank lines are skipped.

  The syntaxes are:

```
for /f [<parsingkeywords>] {%%|%}<variable> in (<set>) do <command>
[<commandlinepptions>]
for /f [<parsingkeywords>] {%%|%}<variable> in (<literalstring>) do
<command> [<commandlinepptions>]
```

```
for /f [<parsingkeywords>] {%%|%}<variable> in ('<command>') do
<command> [<commandlinepptions>]
```

The *set* argument specifies one or more file names. Each file is opened, read, and processed before moving to the next file in *set*. To override the default parsing behavior, specify *parsingkeywords*. This is a quoted string that contains one or more keywords to specify different parsing options.

If you use the **usebackq** option, use one of the following syntaxes:

```
for /f [usebackq <parsingkeywords>] {%%|%}<variable> in (<Set>) do
<command> [<commandlinepptions>]
for /f [usebackq <parsingkeywords>] {%%|%}<variable> in
('<LiteralString>') do <command> [<commandlinepptions>]
for /f [usebackq <parsingkeywords>] {%%|%}<variable> in
(`<command>`) do <command> [<commandlinepptions>]
```

The following table lists the parsing keywords that you can use for *parsingkeywords*.

Keyword	Description
eol=`<c>`	Specifies an end of line character (just one character).
skip=`<n>`	Specifies the number of lines to skip at the beginning of the file.
delims=`<xxx>`	Specifies a delimiter set. This replaces the default delimiter set of space and tab.
tokens=`<x,y,m-n>`	Specifies which tokens from each line are to be passed to the **for** loop for each iteration. As a result, additional variable names are allocated. *m-n* specifies a range, from the *m*th through the *n*th tokens. If the last character in the **tokens=** string is an asterisk (*****), an additional variable is allocated, and it receives the remaining text on the line after the last token that is parsed.
usebackq	Specifies to run a back-quoted string as a command, use a single-quoted string as a literal string, or, for long file names that contain spaces, allow file names in `<set>`, to each be enclosed in double-quotation marks.

- **Variable substitution:** The following table lists optional syntax (for any variable **I**):

Variable with modifier	Description
`%~I`	Expands `%I` which removes any surrounding quotation marks.
`%~fI`	Expands `%I` to a fully qualified path name.
`%~dI`	Expands `%I` to a drive letter only.
`%~pI`	Expands `%I` to a path only.
`%~nI`	Expands `%I` to a file name only.
`%~xI`	Expands `%I` to a file name extension only.
`%~sI`	Expands path to contain short names only.
`%~aI`	Expands `%I` to the file attributes of file.
`%~tI`	Expands `%I` to the date and time of file.
`%~zI`	Expands `%I` to the size of the file.
`%~$PATH:I`	Searches the directories listed in the PATH environment variable and expands `%I` to the fully qualified name of the first directory found. If the environment variable name isn't defined or the file isn't found by the search, this modifier expands to the empty string.

The following table lists modifier combinations that you can use to get compound results.

Variable with combined modifiers	Description
`%~dpI`	Expands `%I` to a drive letter and path only.
`%~nxI`	Expands `%I` to a file name and extension only.
`%~fsI`	Expands `%I` to a full path name with short names only.
`%~dp$PATH:I`	Searches the directories that are listed in the PATH environment variable for `%I` and expands to the drive letter and path of the first one found.
`%~ftzaI`	Expands `%I` to an output line that is like **dir**.

In the above examples, you can replace `%I` and PATH with other valid values. A valid **for** variable name ends the %~ syntax.

By using uppercase variable names such as `%I`, you can make your code more readable and avoid confusion with the modifiers, which aren't case sensitive.

- **Parsing a string:** You can use the `for /f` parsing logic on an immediate string by wrapping `<literalstring>` in either: double quotes (*without* usebackq) or in single quotes (*with* usebackq) --for example, (MyString) or ('MyString'). `<literalstring>` is treated as a single line of input from a file. When parsing `<literalstring>` in double-quotes, command symbols such as (`\ & | > < ^`) are treated as ordinary characters.

- **Parsing output:** You can use the `for /f` command to parse the output of a command by placing a back-quoted `<command>` between the parentheses. It's treated as a command line, which is passed to a child Cmd.exe. The output is captured into memory and parsed as if it's a file.

Examples

To use **for** in a batch file, use the following syntax:

```
for {%%|%}<variable> in (<set>) do <command> [<commandlineoptions>]
```

To display the contents of all the files in the current directory that have the extension .doc or .txt by using the replaceable variable **%f**, type:

```
for %f in (*.doc *.txt) do type %f
```

In the preceding example, each file that has the .doc or .txt extension in the current directory is substituted for the **%f** variable until the contents of every file are displayed. To use this command in a batch file, replace every occurrence of **%f** with **%%f**. Otherwise, the variable is ignored and an error message is displayed.

To parse a file, ignoring commented lines, type:

```
for /f eol=; tokens=2,3* delims=, %i in (myfile.txt) do @echo %i %j %k
```

This command parses each line in *myfile.txt*. It ignores lines that begin with a semicolon and passes the second and third token from each line to the **for** body (tokens are delimited by commas or spaces). The body of the **for** statement references **%i** to get the second token, **%j** to get the third token, and **%k** to get all of the remaining tokens. If the file names that you supply contain spaces, use quotation marks around the text (for example, File Name). To use quotation marks, you must use **usebackq**. Otherwise, the quotation marks are interpreted as defining a literal string to parse.

%i is explicitly declared in the **for** statement. **%j** and **%k** are implicitly declared by using **tokens=**. You can use **tokens=** to specify up to 26 tokens, if it doesn't cause an attempt to declare a variable higher than the letter z or Z.

To parse the output of a command by placing *set* between the parentheses, type:

```
for /f "usebackq delims==" %i in (`set`) do @echo %i
```

To perform a recursive loop of all files in a directory, including subdirectories and echo their full path, when they were last modified, and their file size, type:

```
for /r "C:\My Dir\" %A in (*.*) do echo %~ftzA
```

Related links

- Command-Line Syntax Key

forfiles

Article • 02/03/2023

Selects and runs a command on a file or set of files. This command is most commonly used in batch files.

Syntax

```
forfiles [/P pathname] [/M searchmask] [/S] [/C command] [/D [+ | -]
[{<date> | <days>}]]
```

Parameters

Parameter	Description
/P `<pathname>`	Specifies the path from which to start the search. By default, searching starts in the current working directory.
/M `<searchmask>`	Searches files according to the specified search mask. The default searchmask is `*`.
/S	Instructs the **forfiles** command to search in subdirectories recursively.
/C `<command>`	Runs the specified command on each file. Command strings should be wrapped in double quotes. The default command is `"cmd /c echo @file"`.
/D `[{+|-}] [{<date> | <days>}]`	Selects files with a last modified date within the specified time frame: • Selects files with a last modified date later than or equal to (+) or earlier than or equal to (-) the specified date, where *date* is in the format MM/DD/YYYY. • Selects files with a last modified date later than or equal to (+) the current date plus the number of days specified, or earlier than or equal to (-) the current date minus the number of days specified. • Valid values for *days* include any number in the range 0–32,768. If no sign is specified, + is used by default.
/?	Displays the help text in the cmd window.

Remarks

- The `forfiles /S` command is similar to `dir /S`.

- You can use the following variables in the command string as specified by the **/C** command-line option:

Variable	Description
@FILE	File name.
@FNAME	File name without extension.
@EXT	File name extension.
@PATH	Full path of the file.
@RELPATH	Relative path of the file.
@ISDIR	Evaluates to TRUE if a file type is a directory. Otherwise, this variable evaluates to FALSE.
@FSIZE	File size, in bytes.
@FDATE	Last modified date stamp on the file.
@FTIME	Last modified time stamp on the file.

- The **forfiles** command lets you run a command on or pass arguments to multiple files. For example, you could run the **type** command on all files in a tree with the .txt file name extension. Or you could execute every batch file (*.bat) on drive C, with the file name Myinput.txt as the first argument.
- This command can:
  - Select files by an absolute date or a relative date by using the **/d** parameter.
  - Build an archive tree of files by using variables such as @FSIZE and @FDATE.
  - Differentiate files from directories by using the @ISDIR variable.
  - Include special characters in the command line by using the hexadecimal code for the character, in 0x*HH* format (for example, 0x09 for a tab).
- This command works by implementing the `recurse subdirectories` flag on tools that are designed to process only a single file.

Examples

To list all of the batch files on drive C, type:

```
```

```
forfiles /P c:\ /S /M *.bat /C "cmd /c echo @file is a batch file"
```

To list all of the directories on drive C, type:

```
forfiles /P c:\ /S /M * /C "cmd /c if @isdir==TRUE echo @file is a
directory"
```

To list all of the files in the current directory that are at least one year old, type:

```
forfiles /S /M *.* /D -365 /C "cmd /c echo @file is at least one year old."
```

To display the text *file* is outdated for each of the files in the current directory that are older than January 1, 2007, type:

```
forfiles /S /M *.* /D -01/01/2007 /C "cmd /c echo @file is outdated."
```

To list the file name extensions of all the files in the current directory in column format, and add a tab before the extension, type:

```
forfiles /S /M *.* /C "cmd /c echo The extension of @file is 0x09@ext"
```

Related links

- Command-Line Syntax Key

freedisk

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Checks to see if the specified amount of disk space is available before continuing with an installation process.

Syntax

```
freedisk [/s <computer> [/u [<domain>\]<user> [/p [<password>]]]] [/d
<drive>] [<value>]
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer. This parameter applies to all files and folders specified in the command.
/u [`<domain>`\] `<user>`	Runs the script with the permissions of the specified user account. The default is system permissions.
/p [`<password>`]	Specifies the password of the user account that is specified in **/u**.
/d `<drive>`	Specifies the drive for which you want to find out the availability of free space. You must specify `<drive>` for a remote computer.
`<value>`	Checks for a specific amount of free disk space. You can specify `<value>` in bytes, KB, MB, GB, TB, PB, EB, ZB, or YB.

Remarks

- Using the **/s**, **/u**, and **/p** command-line options are available only when you use **/s**. You must use **/p** with **/u**to provide the user's password.
- For unattended installations, you can use **freedisk** in installation batch files to check for the prerequisite amount free space before continuing with the

installation.

- When you use **freedisk** in a batch file, it returns a **0** if there's enough space and a **1** if there's not enough space.

Examples

To determine whether there are at least 50 MB of free space available on drive C, type:

```
freedisk 50mb
```

Output similar to the following example appears on the screen:

```
INFO: The specified 52,428,800 byte(s) of free space is available on current
drive.
```

Related links

- Command-Line Syntax Key

fsutil

Article • 09/06/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7

Performs tasks that are related to file allocation table (FAT) and NTFS file systems, such as managing reparse points, managing sparse files, or dismounting a volume. If it's used without parameters, **fsutil** displays a list of supported subcommands.

> **Note**
>
> You must be logged on as an administrator or a member of the Administrators group to use **fsutil**. This command is quite powerful and should be used only by advanced users who have a thorough knowledge of Windows operating systems.

Parameters

Subcommand	Description
fsutil 8dot3name	Queries or changes the settings for short name behavior on the system, for example, generates 8.3 character-length file names. Removes short names for all files within a directory. Scans a directory and identifies registry keys that might be impacted if short names were stripped from the files in the directory.
fsutil devdrv	Manages dev drive, which is a volume tuned for performance of developer scenarios. Dev drive also lets an administrator of the device control the file system minifilters that are attached to the volume.
fsutil dirty	Queries whether the volume's dirty bit is set or sets a volume's dirty bit. When a volume's dirty bit is set, **autochk** automatically checks the volume for errors the next time the computer is restarted.
fsutil file	Finds a file by user name (if Disk Quotas are enabled), queries allocated ranges for a file, sets a file's short name, sets a file's valid data length, sets zero data for a file, creates a new file of a specified size, finds a file ID if given the name, or finds a file link name for a specified file ID.
fsutil fsinfo	Lists all drives and queries the drive type, volume information, NTFS-specific volume information, or file system statistics.

Subcommand	Description
fsutil hardlink	Lists hard links for a file, or creates a hard link (a directory entry for a file). Every file can be considered to have at least one hard link. On NTFS volumes, each file can have multiple hard links, so a single file can appear in many directories (or even in the same directory, with different names). Because all of the links reference the same file, programs can open any of the links and modify the file. A file is deleted from the file system only after all links to it are deleted. After you create a hard link, programs can use it like any other file name.
fsutil objectid	Manages object identifiers, which are used by the Windows operating system to track objects such as files and directories.
fsutil quota	Manages disk quotas on NTFS volumes to provide more precise control of network-based storage. Disk quotas are implemented on a per-volume basis and enable both hard- and soft-storage limits to be implemented on a per-user basis.
fsutil repair	Queries or sets the self-healing state of the volume. Self-healing NTFS attempts to correct corruptions of the NTFS file system online without requiring **Chkdsk.exe** to be run. Includes initiating on-disk verification and waiting for repair completion.
fsutil reparsepoint	Queries or deletes reparse points (NTFS file system objects that have a definable attribute containing user-controlled data). Reparse points are used to extend functionality in the input/output (I/O) subsystem. They are used for directory junction points and volume mount points. They are also used by file system filter drivers to mark certain files as special to that driver.
fsutil resource	Creates a Secondary Transactional Resource Manager, starts or stops a Transactional Resource Manager, displays information about a Transactional Resource Manager or modifies its behavior.
fsutil sparse	Manages sparse files. A sparse file is a file with one or more regions of unallocated data in it. A program will see these unallocated regions as containing bytes with the value zero, but no disk space is used to represent these zeros. All meaningful or nonzero data is allocated, whereas all non-meaningful data (large strings of data composed of zeros) is not allocated. When a sparse file is read, allocated data is returned as stored, and unallocated data is returned as zeros (by default in accordance with the C2 security requirement specification). Sparse file support allows data to be deallocated from anywhere in the file.
fsutil tiering	Enables management of storage tier functions, such as setting and disabling flags and listing of tiers.
fsutil transaction	Commits a specified transaction, rolls back a specified transaction, or displays info about the transaction.
fsutil usn	Manages the update sequence number (USN) change journal, which provides a persistent log of all changes made to files on the volume.

Subcommand	Description
fsutil volume	Manages a volume. Dismounts a volume, queries to see how much free space is available on a disk, or finds a file that is using a specified cluster.
fsutil wim	Provides functions to discover and manage WIM-backed files.

Related links

- Command-Line Syntax Key

fsutil 8dot3name

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Queries or changes the settings for short name (8dot3 name) behavior, which includes:

- Querying the current setting for the short name behavior.
- Scanning the specified directory path for registry keys that might be impacted if short names were stripped from the specified directory path.
- Changing the setting that controls the short name behavior. This setting can be applied to a specified volume or to the default volume setting.
- Removing the short names for all files within a directory.

> **Important**
>
> Permanently removing 8dot3 file names and not modifying registry keys that point to the 8dot3 file names may lead to unexpected application failures, including the inability to uninstall an application. It is recommended you first back up your directory or volume before you attempt to remove 8dot3 file names.

Syntax

```
fsutil 8dot3name [query] [<volumepath>]
fsutil 8dot3name [scan] [/s] [/l [<log file>] ] [/v] <directorypath>
fsutil 8dot3name [set] { <defaultvalue> | <volumepath> {1|0}}
fsutil 8dot3name [strip] [/t] [/s] [/f] [/l [<log file.] ] [/v] <directorypath>
```

Parameters

Parameter	Description
query `[<volumepath>]`	Queries the file system for the state of the 8dot3 short name creation behavior. If a *volumepath* isn't specified as a parameter, the default 8dot3name creation behavior setting for all volumes is displayed.
scan `<directorypath>`	Scans the files that are located in the specified *directorypath* for registry keys that might be impacted if 8dot3 short names were stripped from the file names.

Parameter	Description
set { `<defaultvalue>` | `<volumepath>}`	Changes the file system behavior for 8dot3 name creation in the following instances: • When *defaultvalue* is specified, the registry key, **HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation**, is set to the *defaultvalue*. The *DefaultValue* can have the following values: ◦ **0**: Enables 8dot3 name creation for all volumes on the system. ◦ **1**: Disables 8dot3 name creation for all volumes on the system. ◦ **2**: Sets 8dot3 name creation on a per volume basis. ◦ **3**: Disables 8dot3 name creation for all volumes except the system volume. • When a *volumepath* is specified, the specified volumes on disk flag 8dot3name properties are set to enable 8dot3 name creation for a specified volume (**0**) or set to disable 8dot3 name creation on the specified volume (**1**). You must set the default file system behavior for 8dot3 name creation to the value **2** before you can enable or disable 8dot3 name creation for a specified volume.
strip `<directorypath>`	Removes the 8dot3 file names for all files that are located in the specified *directorypath*. The 8dot3 file name is not removed for any files where the *directorypath* combined with the file name contains more than 260 characters. This command lists, but does not modify the registry keys that point to the files that had 8dot3 file names permanently removed.
`<volumepath>`	Specifies the drive name followed by a colon or the GUID in the format `volume{GUID}`.
/f	Specifies that all files that are located in the specified *directorypath* have the 8dot3 file names removed even if there are registry keys that point to files using the 8dot3 file name. In this case, the operation removes the 8dot3 file names, but does not modify any registry keys that point to the files that are using the 8dot3 file names. **Warning:** It's recommended that you back up your directory or volume prior to using the **/f** parameter because it may lead to unexpected application failures, including the inability to uninstall programs.
/l `[<log file>]`	Specifies a log file where information is written. If the **/l** parameter isn't specified, all information is written to the default log file: `%temp%\8dot3_removal_log@(GMT YYYY-MM-DD HH-MM-SS)`.log**
/s	Specifies that the operation should be applied to the subdirectories of the specified *directorypath*.
/t	Specifies that the removal of 8dot3 file names should be run in test mode. All operations except the actual removal of the 8dot3 file names are performed. You can use test mode to discover which registry keys point to files that use the 8dot3 file names.
/v	Specifies that all information that is written to the log file is also displayed on the command-line.

Examples

To query for the disable 8dot3 name behavior for a disk volume that is specified with the GUID, {928842df-5a01-11de-a85c-806e6f6e6963}, type:

```
fsutil 8dot3name query volume{928842df-5a01-11de-a85c-806e6f6e6963}
```

You can also query the 8dot3 name behavior by using the **behavior** subcommand.

To remove 8dot3 file names in the *D:\MyData* directory and all subdirectories, while writing the information to the log file that is specified as *mylogfile.log*, type:

```
fsutil 8dot3name strip /l mylogfile.log /s d:\MyData
```

Related links

- Command-Line Syntax Key
- fsutil
- fsutil behavior

fsutil behavior

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Queries or sets NTFS volume behavior, which includes:

- Creating the 8.3 character-length file names.
- Extending character use in 8.3 character-length short file names on NTFS volumes.
- Updating of the **Last Access Time** stamp when directories are listed on NTFS volumes.
- The frequency with which quota events are written to the system log and to NTFS paged pool and NTFS non-paged pool memory cache levels.
- The size of the master file table zone (MFT Zone).
- Silent deletion of data when the system encounters corruption on an NTFS volume.
- File-delete notification (also known as trim or unmap).

Syntax

```
fsutil behavior query {allowextchar | bugcheckoncorrupt | disable8dot3
[<volumepath>] | disablecompression | disablecompressionlimit |
disableencryption | disablefilemetadataoptimization | disablelastaccess |
disablespotcorruptionhandling | disabletxf | disablewriteautotiering |
encryptpagingfile | mftzone | memoryusage | quotanotify | symlinkevaluation
| disabledeletenotify}

fsutil behavior set {allowextchar {1|0} | bugcheckoncorrupt {1|0} |
disable8dot3 [ <value> | [<volumepath> {1|0}] ] | disablecompression {1|0} |
disablecompressionlimit {1|0} | disableencryption {1|0} |
disablefilemetadataoptimization {1|0} | disablelastaccess {1|0} |
disablespotcorruptionhandling {1|0} | disabletxf {1|0} |
disablewriteautotiering {1|0} | encryptpagingfile {1|0} | mftzone <Value> |
memoryusage <Value> | quotanotify <frequency> | symlinkevaluation
<symboliclinktype> | disabledeletenotify {1|0}}
```

Parameters

Parameter	Description
query	Queries the file system behavior parameters.
set	Changes the file system behavior parameters.
allowextchar `{1|0}`	Allows (**1**) or disallows (**0**) characters from the extended character set (including diacritic characters) to be used in 8.3 character-length short file names on NTFS volumes. You must restart your computer for this parameter to take effect.
Bugcheckoncorrupt `{1|0}`	Allows (**1**) or disallows (**0**) generation of a bug check when there is corruption on an NTFS volume. This feature can be used to prevent NTFS from silently deleting data when used with the Self-Healing NTFS feature. You must restart your computer for this parameter to take effect.
disable8dot3 [`<volumepath>`] `{1|0}`	Disables (**1**) or enables (**0**) the creation of 8.3 character-length file names on FAT- and NTFS-formatted volumes. Optionally, prefix with the *volumepath* specified as a drive name followed by a colon or GUID.
disablecompression `{1|0}`	Disables **(1)** or enables **(0)** NTFS compression. You must restart your computer for this parameter to take effect.
disablecompressionlimit `{1|0}`	Disables **(1)** or enables **(0)** NTFS compression limit on NTFS volume. When a compressed file reaches a certain level of fragmentation, rather than failing to extend the file, NTFS stops compressing additional extents of the file. This was done to allow compressed files to be larger than they normally would be. Setting this value to **TRUE** disables this feature which limits the size of compressed files on the system. We don't recommend disabling this feature. You must restart your computer for this parameter to take effect.
disableencryption `{1|0}`	Disables **(1)** or enables **(0)** the encryption of folders and files on NTFS volumes. You must restart your computer for this parameter to take effect.

Parameter	Description
disablefilemetadataoptimization `{1|0}`	Disables **(1)** or enables **(0)** file metadata optimization. NTFS has a limit on how many extents a given file can have. Compressed and sparse files can become very fragmented. By default, NTFS periodically compacts its internal metadata structures to allow for more fragmented files. Setting this value to **TRUE** disables this internal optimization. We don't recommend disabling this feature. You must restart your computer for this parameter to take effect.
disablelastaccess `{1|0}`	Disables (**1**) or enables (**0**) updates to the Last Access Time stamp on each directory when directories are listed on an NTFS volume. You must restart your computer for this parameter to take effect.
disablespotcorruptionhandling `{1|0}`	Disables **(1)** or enables **(0)** spot corruption handling. Also allows system administrators to run CHKDSK to analyze the state of a volume without taking it offline. We don't recommend disabling this feature. You must restart your computer for this parameter to take effect.
disabletxf `{1|0}`	Disables **(1)** or enables **(0)** txf on the specified NTFS volume. TxF is an NTFS feature that provides transaction like semantics to file system operations. TxF is presently deprecated, but the functionality is still available. We don't recommend disabling this feature on the C: volume. You must restart your computer for this parameter to take effect.
disablewriteautotiering `{1|0}`	Disables ReFS v2 auto tiering logic for tiered volumes. You must restart your computer for this parameter to take effect.
encryptpagingfile `{1|0}`	Encrypts (**1**) or doesn't encrypt (**0**) the memory paging file in the Windows operating system. You must restart your computer for this parameter to take effect.

Parameter	Description
mftzone `<value>`	Sets the size of the MFT Zone, and is expressed as a multiple of 200MB units. Set *value* to a number from **1** (default is 200 MB) to **4** (maximum is 800 MB). You must restart your computer for this parameter to take effect.
memoryusage `<value>`	Configures the internal cache levels of NTFS paged-pool memory and NTFS nonpaged-pool memory. Set to **1** or **2**. When set to **1** (the default), NTFS uses the default amount of paged-pool memory. When set to **2**, NTFS increases the size of its lookaside lists and memory thresholds. (A lookaside list is a pool of fixed-size memory buffers that the kernel and device drivers create as private memory caches for file system operations, such as reading a file.) You must restart your computer for this parameter to take effect.
quotanotify `<frequency>`	Configures how frequently NTFS quota violations are reported in the system log. Valid values for are in the range **0 – 4294967295**. The default frequency is **3600** seconds (one hour). You must restart your computer for this parameter to take effect.
symlinkevaluation `<symboliclinktype>`	Controls the kind of symbolic links that can be created on a computer. Valid choices are: • **1** - Local to local symbolic links, `L2L:{0|1}` • **2** - Local to remote symbolic links, `L2R:{1|0}` • **3** - Remote to local symbolic links, `R2L:{1|0}` • **4** - Remote to remote symbolic links, `R2R:{1|0}`

Parameter	Description
disabledeletenotify	Disables (**1**) or enables (**0**) delete notifications. Delete notifications (also known as trim or unmap) is a feature that notifies the underlying storage device of clusters that have been freed due to a file delete operation. In addition: • For systems using ReFS v2, trim is disabled by default. • For systems using ReFS v1, trim is enabled by default. • For systems using NTFS, trim is enabled by default unless an administrator disables it. • If your hard disk drive or SAN reports that it doesn't support trim, then your hard disk drive and SANs don't get trim notifications. • Enabling or disabling doesn't require a restart. • Trim is effective when the next unmap command is issued. • Existing inflight IO are not impacted by the registry change. • Doesn't require any service restart when you enable or disable trim.

Remarks

- The MFT Zone is a reserved area that enables the master file table (MFT) to expand as needed to prevent MFT fragmentation. If the average file size on the volume is 2 KB or less, it can be beneficial to set the **mftzone** value to **2**. If the average file size on the volume is 1 KB or less, it can be beneficial to set the **mftzone** value to **4**.
- When **disable8dot3** is set to **0**, every time you create a file with a long file name, NTFS creates a second file entry that has an 8.3 character-length file name. When NTFS creates files in a directory, it must look up the 8.3 character-length file names that are associated with the long file names. This parameter updates the **HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation** registry key.
- The **allowextchar** parameter updates the **HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsAllowExtendedCharacterIn8dot3Name** registry key.
- The **disablelastaccess** parameter reduces the impact of logging updates to the **Last Access Time** stamp on files and directories. Disabling the **Last Access Time** feature improves the speed of file and directory access. This parameter updates the

HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate registry key.

Notes:

- File-based **Last Access Time** queries are accurate even if all on-disk values aren't current. NTFS returns the correct value on queries because the accurate value is stored in memory.
- One hour is the maximum amount of time that NTFS can defer updating **Last Access Time** on disk. If NTFS updates other file attributes such as **Last Modify Time**, and a **Last Access Time** update is pending, NTFS updates **Last Access Time** with the other updates without additional performance impact.
- The **disablelastaccess** parameter can affect programs such as Backup and Remote Storage, which rely on this feature.

- Increasing the physical memory doesn't always increase the amount of paged pool memory available to NTFS. Setting **memoryusage** to **2** raises the limit of paged pool memory. This might improve performance if your system is opening and closing many files in the same file set and is not already using large amounts of system memory for other apps or for cache memory. If your computer is already using large amounts of system memory for other apps or for cache memory, increasing the limit of NTFS paged and non-paged pool memory reduces the available pool memory for other processes. This might reduce overall system performance. This parameter updates the **HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsMemoryUsage** registry key.

- The value specified in the **mftzone** parameter is an approximation of the initial size of the MFT plus the MFT Zone on a new volume, and it is set at mount time for each file system. As space on the volume is used, NTFS adjusts the space reserved for future MFT growth. If the MFT Zone is already large, the full MFT Zone size is not reserved again. Because the MFT Zone is based on the contiguous range past the end of the MFT, it shrinks as the space is used.

  The file system doesn't determine the new MFT Zone location until the current MFT Zone is completely used. Note that this never occurs on a typical system.

- Some devices may experience performance degradation when the delete notification feature is turned on. In this case, use the **disabledeletenotify** option to turn off the notification feature.

Examples

To query for the disable 8dot3 name behavior for a disk volume specified with the GUID, {928842df-5a01-11de-a85c-806e6f6e6963}, type:

```
fsutil behavior query disable8dot3 volume{928842df-5a01-11de-a85c-
806e6f6e6963}
```

You can also query the 8dot3 name behavior by using the **8dot3name** subcommand.

To query the system to see if TRIM is enabled or not, type:

```
fsutil behavior query DisableDeleteNotify
```

This yields an output similar to this:

```
NTFS DisableDeleteNotify = 1
ReFS DisableDeleteNotify is not currently set
```

To override the default behavior for TRIM (disabledeletenotify) for ReFS v2, type:

```
fsutil behavior set disabledeletenotify ReFS 0
```

To override the default behavior for TRIM (disabledeletenotify) for NTFS and ReFS v1, type:

```
fsutil behavior set disabledeletenotify 1
```

Related links

- Command-Line Syntax Key
- fsutil

- fsutil 8dot3name

fsutil devdrv

Article • 09/06/2023

> Applies to: Windows 11

Dev drive or a developer volume is a volume that is tuned for performance of developer scenarios. The command also lets an administrator of the device control the file system minifilters that are attached to the volume.

Devdrv commands supported

Command	Description
query	Query dev drive information.
enable	Enable dev drive support on this system.
disable	Disable dev drive support on this system.
trust	Trust the given dev drive.
untrust	Untrust the given dev drive.
setFiltersAllowed	Set the list of allowed filters for dev drive.
clearFiltersAllowed	Clear the list of allowed filters for dev drive.

Syntax

```
fsutil devdrv query [<volume path>]

fsutil devdrv enable [/allowAv|/disallowAv]

fsutil devdrv disable

fsutil devdrv trust [/f] <volume path>

fsutil devdrv untrust [/f] <volume path>

fsutil devdrv setFiltersAllowed [[/f] /volume <volume path>] "filter1,
filter 2, ..."

fsutil devdrv clearFiltersAllowed [[/f] <volume path>]
```

fsutil devdrv query

Queries information about dev drives or the given dev drive. The command shows if the given volume is a dev drive and if it's trusted. The command also lists the filters allowed to attach and currently attached to the dev drive.

fsutil devdrv query examples

The following example shows the output of the command for the query command.

Example 1: Query dev drive information

The command queries information about dev drives on this system.

```
fsutil devdrv query
```

Example 2: Query dev drive information for a specified volume

The following command queries dev drive related information for `D:`. The command lists the filters currently attached to `D:` if it's a dev drive.

```
fsutil devdrv query D:
```

fsutil devdrv enable

Enable dev drive support on this system.

fsutil devdrv enable examples

The following example shows the output of the command for the enable command.

Example 1: Enable dev drive support

This command enables the dev drive and let the system decide whether to allow antivirus filter to attach on a dev drive.

```
```

```
fsutil devdrv enable
```

Example 2: Enable dev drive support and allow antivirus filter to attach

In this command, the dev drive is enabled while allowing antivirus filter to be attached on a dev drive.

```
fsutil devdrv enable /allowAv
```

Example 3: Enable dev drive support and disallow antivirus filter to attach

The following command enables dev drive without allowing antivirus filter to be attached on a dev drive.

```
fsutil devdrv enable /disallowAv
```

fsutil devdrv disable

Disable dev drive support on this system.

> ⓘ **Note**
>
> Existing dev drives will function as a regular volume i.e., all filters are allowed to attach.

fsutil devdrv trust

Trust the specified dev drive. The dev drive filter attach policy is honored only for a trusted dev drive.

fsutil devdrv trust parameters

Parameter	Description
/F	Force dismount the volume for the change to take effect immediately even if the volume is in use. Otherwise the volume is dismounted only if it isn't in use.

fsutil devdrv trust examples

The following examples show the output of the command for the trust command.

Example 1: Trust a dev drive for a specified volume

This command trusts the volume `D:`. The volume won't be dismounted if it is in use, the change takes effect next time the volume mounts.

```
fsutil devdrv trust D:
```

Example 2: Trust a dev drive for a specified volume immediately

In this command, the volume is trusted and is dismounted forcefully for the change to take effect immediately.

```
fsutil devdrv trust /f D:
```

fsutil devdrv untrust

Untrust the given dev drive. The dev drive filter attach policy isn't honored for an untrusted dev drive.

fsutil devdrv untrust parameters

Parameter	Description
/F	Force dismount the volume for the change to take effect immediately even if the volume is in use. Otherwise the volume is dismounted only if it isn't in use.

fsutil devdrv untrust examples

The following examples show the output of the command for the untrust command.

Example 1: Untrust a dev drive for a specified volume

The following command untrusts the volume `D:`. The volume won't be dismounted if it is in use and the change would take effect next time the volume mounts.

```
fsutil devdrv untrust D:
```

Example 2: Untrust a dev drive for a specified volume immediately

The command untrusts the volume `D:` and dismounts it forcefully for the change to take effect immediately.

```
fsutil devdrv untrust /f D:
```

fsutil devdrv setFiltersAllowed

Set the list of allowed filters for the specified dev drive or any dev drive on this system.

fsutil devdrv setFiltersAllowed parameters

Parameter	Description
/F	Force dismount the volume for the change to take effect immediately even if the volume is in use. Otherwise the volume, if specified, is dismounted only if it isn't in use. Note: the parameter is available only when `<volume path>` is provided.
/Volume	If specified, the allowed list of filters is set only for this volume.

fsutil devdrv setFiltersAllowed examples

The following examples show the output of the command for the setFiltersAllowed command.

Example 1: Set the list of allowed filters for any dev drive on the system

The command allows `filter1` and `filter2` to be attached to any dev drive on the system. The change will take effect next time a dev drive is mounted.

```
fsutil devdrv setFiltersAllowed "filter1, filter 2"
```

Example 2: Set the list of allowed filters for a specified volume

The command, `filter1` and `filter2` are allowed to attach to dev drive `D:`. The volume won't be dismounted if it is in use and the change would take effect next time the volume mounts.

```
fsutil devdrv setFiltersAllowed /volume D: filter1,filter2
```

Example 3: Set the list of allowed filters for a specified volume immediately

The following command allows `filter1` and `filter2` to attach to dev drive `D:`. The command forcefully dismounts the volume for the change to take effect immediately.

```
fsutil devdrv setFiltersAllowed /f /volume D: filter1,filter2
```

fsutil devdrv clearFiltersAllowed

Clear the list of allowed filters for the specified dev drive or any dev drive on this system.

fsutil devdrv clearFiltersAllowed parameters

Parameter	Description
/F	Force dismount the volume for the change to take effect immediately even if the volume is in use. Otherwise the volume, if specified, is dismounted only if it isn't in

Parameter	Description
	use. Note: the parameter is available only when `<volume path>` is provided.
/Volume	If specified, the allowed list of filters is set only for this volume.

fsutil devdrv clearFiltersAllowed examples

The following examples show the output of the command for the clearFiltersAllowed command.

Example 1: Clear the list of allowed filters for any dev drive on this system

This command clears the list of allowed filters for any dev drive on this system. The change will take effect next time a dev drive is mounted on this system.

```
fsutil devdrv clearFiltersAllowed
```

Example 2: Clear the list of allowed filters for a specified volume

The following command clears the list of allowed filters `D:`. The volume won't be dismounted if it is in use, the change takes effect next time the volume mounts.

```
fsutil devdrv clearFiltersAllowed D:
```

> ⓘ Note
>
> `D:` must be a dev drive.

Example 3: Clear the list of allowed filters for a specified volume immediately

The following command clears the list of allowed filters on `D:`. The command forcefully dismounts the volume for the change to take effect immediately.

```
fsutil devdrv clearFiltersAllowed /f D:
```

> **Note**
>
> `D:` must be a dev drive.

Related links

- Command-Line Syntax Key
- fsutil
- Dev Drive

fsutil dirty

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Queries or sets a volume's dirty bit. When a volume's dirty bit is set, **autochk** automatically checks the volume for errors the next time the computer is restarted.

Syntax

```
fsutil dirty {query | set} <volumepath>
```

Parameters

Parameter	Description
query	Queries the specified volume's dirty bit.
set	Sets the specified volume's dirty bit.
`<volumepath>`	Specifies the drive name followed by a colon or GUID in the following format: `volume{GUID}`.

Remarks

- A volume's dirty bit indicates that the file system may be in an inconsistent state. The dirty bit can be set because:
  - The volume is online and it has outstanding changes.
  - Changes were made to the volume and the computer was shut down before the changes were committed to the disk.
  - Corruption was detected on the volume.
- If the dirty bit is set when the computer restarts, **chkdsk** runs to verify the file system integrity and to attempt to fix any issues with the volume.

Examples

To query the dirty bit on drive C, type:

```
fsutil dirty query c:
```

- If the volume is dirty, the following output displays: `Volume C: is dirty`
- If the volume isn't dirty, the following output displays: `Volume C: is not dirty`

To set the dirty bit on drive C, type:

```
fsutil dirty set C:
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil file

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Finds a file by user name (if Disk Quotas are enabled), queries allocated ranges for a file, sets a file's short name, sets a file's valid data length, sets zero data for a file, or creates a new file.

Syntax

```
fsutil file [createnew] <filename> <length>
fsutil file [findbysid] <username> <directory>
fsutil file [optimizemetadata] [/A] <filename>
fsutil file [queryallocranges] offset=<offset> length=<length> <filename>
fsutil file [queryextents] [/R] <filename> [<startingvcn> [<numvcns>]]
fsutil file [queryfileid] <filename>
fsutil file [queryfilenamebyid] <volume> <fileid>
fsutil file [queryoptimizemetadata] <filename>
fsutil file [queryvaliddata] [/R] [/D] <filename>
fsutil file [seteof] <filename> <length>
fsutil file [setshortname] <filename> <shortname>
fsutil file [setvaliddata] <filename> <datalength>
fsutil file [setzerodata] offset=<offset> length=<length> <filename>
```

Parameters

Parameter	Description
createnew	Creates a file of the specified name and size, with content that consists of zeroes.
`<length>`	Specifies the file's valid data length.
findbysid	Finds files that belong to a specified user on NTFS volumes where Disk Quotas are enabled.
`<username>`	Specifies the user's user name or logon name.
`<directory>`	Specifies the full path to the directory, for example C:\users.

Parameter	Description
optimizemetadata	This performs an immediate compaction of the metadata for a given file.
/a	Analyze file metadata before and after optimization.
queryallocranges	Queries the allocated ranges for a file on an NTFS volume. Useful for determining whether a file has sparse regions.
offset=`<offset>`	Specifies the start of the range that should be set to zeroes.
length=`<length>`	Specifies the length of the range (in bytes).
queryextents	Queries extents for a file.
/r	If `<filename>` is a reparse point, open it rather than its target.
`<startingvcn>`	Specifies first VCN to query. If omitted, start at VCN 0.
`<numvcns>`	Number of VCNs to query. If omitted or 0, query until EOF.
queryfileid	Queries the file ID of a file on an NTFS volume.
`<volume>`	Specifies the volume as drive name followed by a colon.
queryfilenamebyid	Displays a random link name for a specified file ID on an NTFS volume. Since a file can have more than one link name pointing to that file, it is not guaranteed which file link will be provided as a result of the query for the file name.
`<fileid>`	Specifies the ID of the file on an NTFS volume.
queryoptimizemetadata	Queries the metadata state of a file.
queryvaliddata	Queries the valid data length for a file.
/d	Display detailed valid data information.
seteof	Sets the EOF of the given file.
setshortname	Sets the short name (8.3 character-length file name) for a file on an NTFS volume.
`<shortname>`	Specifies the file's short name.
setvaliddata	Sets the valid data length for a file on an NTFS volume.
`<datalength>`	Specifies the length of the file in bytes.

Parameter	Description
setzerodata	Sets a range (specified by *offset* and *length*) of the file to zeroes, which empties the file. If the file is a sparse file, the underlying allocation units are decommitted.

Remarks

- In NTFS, there are two important concepts of file length: the end-of-file (EOF) marker and the Valid Data Length (VDL). The EOF indicates the actual length of the file. The VDL identifies the length of valid data on disk. Any reads between VDL and EOF automatically return 0 to preserve the C2 object reuse requirement.
- The **setvaliddata** parameter is only available for administrators because it requires the Perform volume maintenance tasks (SeManageVolumePrivilege) privilege. This feature is only required for advanced multimedia and system area network scenarios. The **setvaliddata** parameter must be a positive value that is greater than the current VDL, but less than the current file size.

  It is useful for programs to set a VDL when:

  - Writing raw clusters directly to disk through a hardware channel. This allows the program to inform the file system that this range contains valid data that can be returned to the user.
  - Creating large files when performance is an issue. This avoids the time it takes to fill the file with zeroes when the file is created or extended.

Examples

To find files that are owned by *scottb* on drive C, type:

```
fsutil file findbysid scottb c:\users
```

To query the allocated ranges for a file on an NTFS volume, type:

```
fsutil file queryallocranges offset=1024 length=64 c:\temp\sample.txt
```

To optimize metadata for a file, type:

```
fsutil file optimizemetadata C:\largefragmentedfile.txt
```

To query the extents for a file, type:

```
fsutil file queryextents C:\Temp\sample.txt
```

To set the EOF for a file, type:

```
fsutil file seteof C:\testfile.txt 1000
```

To set the short name for the file, *longfilename.txt* on drive C to *longfile.txt*, type:

```
fsutil file setshortname c:\longfilename.txt longfile.txt
```

To set the valid data length to *4096 bytes* for a file named *testfile.txt* on an NTFS volume, type:

```
fsutil file setvaliddata c:\testfile.txt 4096
```

To set a range of a file on an NTFS volume to zeros to empty it, type:

```
fsutil file setzerodata offset=100 length=150 c:\temp\sample.txt
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil fsinfo

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Lists all drives, queries the drive type, queries volume information, queries NTFS-specific volume information, or queries file system statistics.

Syntax

```
fsutil fsinfo [drives]
fsutil fsinfo [drivetype] <volumepath>
fsutil fsinfo [ntfsinfo] <rootpath>
fsutil fsinfo [statistics] <volumepath>
fsutil fsinfo [volumeinfo] <rootpath>
```

Parameters

Parameter	Description
drives	Lists all drives in the computer.
drivetype	Queries a drive and lists its type, for example CD-ROM drive.
ntfsinfo	Lists NTFS specific volume information for the specified volume, such as the number of sectors, total clusters, free clusters, and the start and end of the MFT Zone.
sectorinfo	Lists information about the hardware's sector size and alignment.
statistics	Lists file system statistics for the specified volume, such as metadata, log file, and MFT reads and writes.
volumeinfo	Lists information for the specified volume, such as the file system, and whether the volume supports case-sensitive file names, unicode in file names, disk quotas, or is a DirectAccess (DAX) volume.
`<volumepath>:`	Specifies the drive letter (followed by a colon).
`<rootpath>:`	Specifies the drive letter (followed by a colon) of the root drive.

Examples

To list all of the drives in the computer, type:

```
fsutil fsinfo drives
```

Output similar to the following displays:

```
Drives: A:\ C:\ D:\ E:\
```

To query the drive type of drive C, type:

```
fsutil fsinfo drivetype c:
```

Possible results of the query include:

```
Unknown Drive
No such Root Directory
Removable Drive, for example floppy
Fixed Drive
Remote/Network Drive
CD-ROM Drive
Ram Disk
```

To query the volume information for volume E, type:

```
fsutil fsinfo volumeinfo e:
```

Output similar to the following displays:

```
Volume Name : Volume
Serial Number : 0xd0b634d9
Max Component Length : 255
File System Name : NTFS
```

```
Supports Named Streams
Is DAX Volume
```

To query drive F for NTFS-specific volume information, type:

```
fsutil fsinfo ntfsinfo f:
```

Output similar to the following displays:

```
NTFS Volume Serial Number : 0xe660d46a60d442cb
Number Sectors : 0x0000000010ea04f
Total Clusters : 0x000000000021d409
Mft Zone End : 0x0000000000004700
```

To query the file system's underlying hardware for sector information, type:

```
fsutil fsinfo sectorinfo d:
```

Output similar to the following displays:

```
D:\>fsutil fsinfo sectorinfo d:
LogicalBytesPerSector : 4096
PhysicalBytesPerSectorForAtomicity : 4096
Trim Not Supported
DAX capable
```

To query the file system statistics for drive E, type:

```
fsutil fsinfo statistics e:
```

Output similar to the following displays:

```
File System Type : NTFS
Version : 1
UserFileReads : 75021
UserFileReadBytes : 1305244512
LogFileWriteBytes : 180936704
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil hardlink

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Creates a hard link between an existing file and a new file. A hard link is a directory entry for a file. Every file can be considered to have at least one hard link.

On NTFS volumes, each file can have multiple hard links, so a single file can appear in many directories (or even in the same directory with different names). Because all of the links reference the same file, programs can open any of the links and modify the file. A file is deleted from the file system only after all links to it have been deleted. After you create a hard link, programs can use it like any other file name.

Syntax

```
fsutil hardlink create <newfilename> <existingfilename>
fsutil hardlink list <filename>
```

Parameters

Parameter	Description
create	Establishes an NTFS hard link between an existing file and a new file. (An NTFS hard link is similar to a POSIX hard link.)
<newfilename>	Specifies the file that you want to create a hard link to.
<existingfilename>	Specifies the file that you want to create a hard link from.
list	Lists the hard links to *filename*.

Related links

- Command-Line Syntax Key
- fsutil

fsutil objectid

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Manages object identifiers (OIDs), which are internal objects used by the Distributed Link Tracking (DLT) Client service and File Replication Service (FRS), to track other objects such as files, directories, and links. Object identifiers are invisible to most programs and should never be modified.

> **⚠ Warning**
>
> Don't delete, set, or otherwise modify an object identifier. Deleting or setting an object identifier can result in the loss of data from portions of a file, up to and including entire volumes of data. In addition, you might cause adverse behavior in the Distributed Link Tracking (DLT) Client service and File Replication Service (FRS).

Syntax

```
fsutil objectid [create] <filename>
fsutil objectid [delete] <filename>
fsutil objectid [query] <filename>
fsutil objectid [set] <objectID> <birthvolumeID> <birthobjectID> <domainID>
<filename>
```

Parameters

Parameter	Description
create	Creates an object identifier if the specified file does not already have one. If the file already has an object identifier, this subcommand is equivalent to the **query** subcommand.
delete	Deletes an object identifier.
query	Queries an object identifier.

Parameter	Description
set	Sets an object identifier.
`<objectID>`	Sets a file-specific 16 byte hexadecimal identifier that is guaranteed to be unique within a volume. The object identifier is used by the Distributed Link Tracking (DLT) Client service and the File Replication Service (FRS) to identify files.
`<birthvolumeID>`	Indicates the volume on which the file was located when it first obtained an object identifier. This value is a 16-byte hexadecimal identifier that is used by the DLT Client service.
`<birthobjectID>`	Indicates the file's original object identifier (The *objectID* may change when a file is moved). This value is a 16-byte hexadecimal identifier that is used by the DLT Client service.
`<domainID>`	16-byte hexadecimal domain identifier. This value isn't currently used and must be set to all zeros.
`<filename>`	Specifies the full path to the file including the file name and extension, for example *C:\documents\filename.txt*.

Remarks

- Any file that has an object identifier also has a birth volume identifier, a birth object identifier, and a domain identifier. When you move a file, the object identifier may change, but the birth volume and birth object identifiers remain the same. This behavior enables the Windows operating system to always find a file, no matter where it has been moved.

Examples

To create an object identifier, type:

```
fsutil objectid create c:\temp\sample.txt
```

To delete an object identifier, type:

```
fsutil objectid delete c:\temp\sample.txt
```

To query an object identifier, type:

```
fsutil objectid query c:\temp\sample.txt
```

To set an object identifier, type:

```
fsutil objectid set 40dff02fc9b4d4118f120090273fa9fc
f86ad6865fe8d21183910008c709d19e 40dff02fc9b4d4118f120090273fa9fc
00000000000000000000000000000000 c:\temp\sample.txt
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil quota

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Manages disk quotas on NTFS volumes to provide more precise control of network-based storage.

Syntax

```
fsutil quota [disable] <volumepath>
fsutil quota [enforce] <volumepath>
fsutil quota [modify] <volumepath> <threshold> <limit> <username>
fsutil quota [query] <volumepath>
fsutil quota [track] <volumepath>
fsutil quota [violations]
```

Parameters

Parameter	Description
disable	Disables quota tracking and enforcement on the specified volume.
enforce	Enforces quota usage on the specified volume.
modify	Modifies an existing disk quota or creates a new quota.
query	Lists existing disk quotas.
track	Tracks disk usage on the specified volume.
violations	Searches the system and application logs and displays a message to indicate that quota violations have been detected or that a user has reached a quota threshold or quota limit.
`<volumepath>`	Required. Specifies the drive name followed by a colon or the GUID in the format `volume{GUID}`.
`<threshold>`	Sets the limit (in bytes) at which warnings are issued. This parameter is required for the `fsutil quota modify` command.

Parameter	Description
`<limit>`	Sets the maximum allowed disk usage (in bytes). This parameter is required for the `fsutil quota modify` command.
`<username>`	Specifies the domain or user name. This parameter is required for the `fsutil quota modify` command.

Remarks

- Disk quotas are implemented on a per-volume basis, and they enable both hard and soft storage limits to be implemented on a per-user basis.
- You can use write scripts that use **fsutil quota** to set the quota limits every time you add a new user or to automatically track quota limits, compile them into a report, and automatically send them to the system administrator in e-mail.

Examples

To list existing disk quotas for a disk volume that is specified with the GUID, {928842df-5a01-11de-a85c-806e6f6e6963}, type:

```
fsutil quota query volume{928842df-5a01-11de-a85c-806e6f6e6963}
```

To list existing disk quotas for a disk volume that is specified with the drive letter, **C:**, type:

```
fsutil quota query C:
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil repair

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Administers and monitors NTFS self-healing repair operations. Self-healing NTFS attempts to correct corruptions of the NTFS file system online, without requiring **Chkdsk.exe** to be run. For more information, see Self-healing NTFS.

Syntax

```
fsutil repair [enumerate] <volumepath> [<logname>]
fsutil repair [initiate] <volumepath> <filereference>
fsutil repair [query] <volumepath>
fsutil repair [set] <volumepath> <flags>
fsutil repair [wait][<waittype>] <volumepath>
```

Parameters

Parameter	Description
enumerate	Enumerates the entires of a volume's corruption log.
`<logname>`	Can be `$corrupt`, the set of confirmed corruptions in the volume or `$verify`, a set of potential, unverified corruptions in the volume.
initiate	Initiates NTFS self-healing.
`<filereference>`	Specifies the NTFS volume-specific file ID (file reference number). The file reference includes the segment number of the file.
query	Queries the self-healing state of the NTFS volume.
set	Sets the self-healing state of the volume.

Parameter	Description
`<flags>`	Specifies the repair method to be used when setting the self-healing state of the volume. This parameter can be set to three values: • **0x01** - Enables general repair. • **0x09** - Warns about potential data loss without repair. • **0x00** - Disables NTFS self-healing repair operations.
state	Queries the corruption state of the system or for a given volume.
wait	Waits for repair(s) to complete. If NTFS has detected a problem on a volume on which it is performing repairs, this option allows the system to wait until the repair is complete before it runs any pending scripts.
`[waittype {0|1}]`	Indicates whether to wait for the current repair to complete or to wait for all repairs to complete. The *waittype* parameter can be set to the following values: • **0** - Waits for all repairs to complete. (default value) • **1** - Waits for the current repair to complete.

Examples

To enumerate the confirmed corruptions of a volume, type:

```
fsutil repair enumerate C: $Corrupt
```

To enable self-healing repair on drive C, type:

```
fsutil repair set c: 1
```

To disable self-healing repair on drive C, type:

```
fsutil repair set c: 0
```

Related links

- Command-Line Syntax Key
- fsutil
- Self-healing NTFS

fsutil reparsepoint

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Queries or deletes reparse points. The **fsutil reparsepoint** command is typically used by support professionals.

Reparse points are NTFS file system objects that have a definable attribute, which contains user-defined data. They're used to:

- Extend functionality in the input/output (I/O) subsystem.
- Act as directory junction points and volume mount points.
- Mark certain files as special to a file system filter driver.

Syntax

```
fsutil reparsepoint [query] <filename>
fsutil reparsepoint [delete] <filename>
```

Parameters

Parameter	Description
query	Retrieves the reparse point data that is associated with the file or directory identified by the specified handle.
delete	Deletes a reparse point from the file or directory that is identified by the specified handle, but does not delete the file or directory.
`<filename>`	Specifies the full path to the file including the file name and extension, for example *C:\documents\filename.txt*.

Remarks

- When a program sets a reparse point, it stores this data, plus a reparse tag, which uniquely identifies the data it is storing. When the file system opens a file with a reparse point, it attempts to find the associated file system filter. If the file system filter is found, the filter processes the file as directed by the reparse data. If no file system filter is found, the **File open** operation fails.

Examples

To retrieve reparse point data associated with *c:\server*, type:

```
fsutil reparsepoint query c:\server
```

To delete a reparse point from a specified file or directory, use the following format:

```
fsutil reparsepoint delete c:\server
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil resource

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Creates a Secondary Transactional Resource Manager, starts or stops a Transactional Resource Manager, or displays information about a Transactional Resource Manager, and modifies the following behavior:

- Whether a default Transactional Resource Manager cleans its transactional metadata at the next mount.
- The specified Transactional Resource Manager to prefer consistency over availability.
- The specified Transaction Resource Manager to prefer availability over consistency.
- The characteristics of a running Transactional Resource Manager.

Syntax

```
fsutil resource [create] <rmrootpathname>
fsutil resource [info] <rmrootpathname>
fsutil resource [setautoreset] {true|false} <Defaultrmrootpathname>
fsutil resource [setavailable] <rmrootpathname>
fsutil resource [setconsistent] <rmrootpathname>
fsutil resource [setlog] [growth {<containers> containers|<percent> percent}
<rmrootpathname>] [maxextents <containers> <rmrootpathname>] [minextents
<containers> <rmrootpathname>] [mode {full|undo} <rmrootpathname>] [rename
<rmrootpathname>] [shrink <percent> <rmrootpathname>] [size <containers>
<rmrootpathname>]
fsutil resource [start] <rmrootpathname> [<rmlogpathname> <tmlogpathname>
fsutil resource [stop] <rmrootpathname>
```

Parameters

Parameter	Description
create	Creates a secondary Transactional Resource Manager.

Parameter	Description
`<rmrootpathname>`	Specifies the full path to a Transactional Resource Manager root directory.
info	Displays the specified Transactional Resource Manager's information.
setautoreset	Specifies whether a default Transactional Resource Manager will clean the transactional metadata on the next mount. • **true** - Specifies that the Transaction Resource Manager will clean the transactional metadata on the next mount, by default. • **false** - Specifies that the Transaction Resource Manager will not clean the transactional metadata on the next mount, by default.
`<defaultrmrootpathname>`	Specifies the drive name followed by a colon.
setavailable	Specifies that a Transactional Resource Manager will prefer availability over consistency.
setconsistent	Specifies that a Transactional Resource Manager will prefer consistency over availability.
setlog	Changes the characteristics of a Transactional Resource Manager that is already running.
growth	Specifies the amount by which the Transactional Resource Manager log can grow. The growth parameter can be specified as follows: • Number of containers, using the format: `<containers> containers` • Percentage, using the format: `<percent> percent`
`<containers>`	Specifies the data objects that are used by the Transactional Resource Manager.
maxextent	Specifies the maximum number of containers for the specified Transactional Resource Manager.
minextent	Specifies the minimum number of containers for the specified Transactional Resource Manager.
mode `{full|undo}`	Specifies whether all transactions are logged (**full**) or only rolled back events are logged (**undo**).
rename	Changes the GUID for the Transactional Resource Manager.
shrink	Specifies percentage by which the Transactional Resource Manager log can automatically decrease.

Parameter	Description
size	Specifies the size of the Transactional Resource Manager as a specified number of *containers*.
start	Starts the specified Transactional Resource Manager.
stop	Stops the specified Transactional Resource Manager.

Examples

To set the log for the Transactional Resource Manager that is specified by *c:\test*, to have an automatic growth of five containers, type:

```
fsutil resource setlog growth 5 containers c:test
```

To set the log for the Transactional Resource Manager that is specified by *c:\test*, to have an automatic growth of two percent, type:

```
fsutil resource setlog growth 2 percent c:test
```

To specify that the default Transactional Resource Manager will clean the transactional metadata on the next mount on drive C, type:

```
fsutil resource setautoreset true c:\
```

Related links

- Command-Line Syntax Key
- fsutil
- Transactional NTFS

fsutil sparse

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Manages sparse files. A sparse file is a file with one or more regions of unallocated data in it.

A program sees these unallocated regions as containing bytes with a zero value and that there's no disk space representing these zeros. When a sparse file is read, allocated data is returned as stored, and unallocated data is returned, by default, as zeros, in accordance with the C2 security requirement specification. Sparse file support allows data to be deallocated from anywhere in the file.

Syntax

```
fsutil sparse [queryflag] <filename>
fsutil sparse [queryrange] <filename>
fsutil sparse [setflag] <filename>
fsutil sparse [setrange] <filename> <beginningoffset> <length>
```

Parameters

Parameter	Description
queryflag	Queries sparse.
queryrange	Scans a file and searches for ranges that may contain nonzero data.
setflag	Marks the indicated file as sparse.
setrange	Fills a specified range of a file with zeros.
`<filename>`	Specifies the full path to the file including the file name and extension, for example *C:\documents\filename.txt*.
`<beginningoffset>`	Specifies the offset within the file to mark as sparse.

Parameter	Description
`<length>`	Specifies the length of the region in the file to be marked as sparse (in bytes).

Remarks

- All meaningful or nonzero data is allocated, whereas all non-meaningful data (large strings of data that is composed of zeros) is not allocated.
- In a sparse file, large ranges of zeroes may not require disk allocation. Space for nonzero data is allocated as needed when the file is written.
- Only compressed or sparse files can have zeroed ranges known to the operating system.
- If the file is sparse or compressed, NTFS may de-allocate disk space within the file. This sets the range of bytes to zeroes without extending the file size.

Examples

To mark a file named *sample.txt* in the *c:\temp* directory as sparse, type:

```
fsutil sparse setflag c:\temp\sample.txt
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil tiering

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10

Enables management of storage tier functions, such as setting and disabling flags and listing of tiers.

Syntax

```
fsutil tiering [clearflags] <volume> <flags>
fsutil tiering [queryflags] <volume>
fsutil tiering [regionlist] <volume>
fsutil tiering [setflags] <volume> <flags>
fsutil tiering [tierlist] <volume>
```

Parameters

Parameter	Description
clearflags	Disables the tiering behavior flags of a volume.
`<volume>`	Specifies the volume.
/trnh	For volumes with tiered storage, causes Heat gathering to be disabled. Applies to NTFS and ReFS only.
queryflags	Queries the tiering behavior flags of a volume.
regionlist	Lists the tiered regions of a volume and their respective storage tiers.
setflags	Enables the tiering behavior flags of a volume.
tierlist	Lists the storage tiers associated with a volume.

Examples

To query the flags on volume C, type:

```
fsutil tiering queryflags C:
```

To set the flags on volume C, type:

```
fsutil tiering setflags C: /trnh
```

To clear the flags on volume C, type:

```
fsutil tiering clearflags C: /trnh
```

To list the regions of volume C and their respective storage tiers, type:

```
fsutil tiering regionlist C:
```

To list the tiers of volume C, type:

```
fsutil tiering tierlist C:
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil transaction

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Manages NTFS transactions.

Syntax

```
fsutil transaction [commit] <GUID>
fsutil transaction [fileinfo] <filename>
fsutil transaction [list]
fsutil transaction [query] [{files | all}] <GUID>
fsutil transaction [rollback] <GUID>
```

Parameters

Parameter	Description
commit	Marks the end of a successful implicit or explicit specified transaction.
`<GUID>`	Specifies the GUID value that represents a transaction.
fileinfo	Displays transaction information for the specified file.
`<filename>`	Specifies full path and file name.
list	Displays a list of currently running transactions.
query	Displays information for the specified transaction. • If `fsutil transaction query files` is specified, the file information is displayed only for the specified transaction. • If `fsutil transaction query all` is specified, all information for the transaction will be displayed.
rollback	Rolls back a specified transaction to the beginning.

Examples

To display transaction information for file *c:\test.txt*, type:

```
fsutil transaction fileinfo c:\test.txt
```

Related links

- Command-Line Syntax Key
- fsutil
- Transactional NTFS

fsutil usn

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Manages the update sequence number (USN) change journal. The USN change journal provides a persistent log of all changes made to files on the volume. As files, directories, and other NTFS objects are added, deleted, and modified, NTFS enters records into the USN change journal, one for each volume on the computer. Each record indicates the type of change and the object changed. New records are appended to the end of the stream.

Syntax

```
fsutil usn [createjournal] m=<maxsize> a=<allocationdelta> <volumepath>
fsutil usn [deletejournal] {/d | /n} <volumepath>
fsutil usn [enablerangetracking] <volumepath> [options]
fsutil usn [enumdata] <fileref> <lowUSN> <highUSN> <volumepath>
fsutil usn [queryjournal] <volumepath>
fsutil usn [readdata] <filename>
fsutil usn [readjournal] [c= <chunk-size> s=<file-size-threshold>]
<volumepath>
```

Parameters

Parameter	Description
createjournal	Creates a USN change journal.
m=`<maxsize>`	Specifies the maximum size, in bytes, that NTFS allocates for the change journal.
a=`<allocationdelta>`	Specifies the size, in bytes, of memory allocation that is added to the end and removed from the beginning of the change journal.
`<volumepath>`	Specifies the drive letter (followed by a colon).

Parameter	Description
deletejournal	Deletes or disables an active USN change journal. **CAUTION:** Deleting the change journal impacts the File Replication Service (FRS) and the Indexing Service, because it requires these services to perform a complete (and time-consuming) scan of the volume. This in turn negatively impacts FRS SYSVOL replication and replication between DFS link alternates while the volume is being rescanned.
/d	Disables an active USN change journal, and returns input/output (I/O) control while the change journal is being disabled.
/n	Disables an active USN change journal and returns I/O control only after the change journal is disabled.
enablerangetracking	Enables USN write range tracking for a volume.
c=`<chunk-size>`	Specifies the chunk size to track on a volume.
s=`<file-size-threshold>`	Specifies the file size threshold for range tracking.
enumdata	Enumerates and lists the change journal entries between two specified boundaries.
`<fileref>`	Specifies the ordinal position within the files on the volume at which the enumeration is to begin.
`<lowUSN>`	Specifies the lower boundary of the range of USN values used to filter the records that are returned. Only records whose last change journal USN is between or equal to the *lowUSN* and *highUSN* member values are returned.
`<highUSN>`	Specifies the upper boundary of the range of USN values used to filter the files that are returned.
queryjournal	Queries a volume's USN data to gather information about the current change journal, its records, and its capacity.
readdata	Reads the USN data for a file.
`<filename>`	Specifies the full path to the file, including the file name and extension For example: *C:\documents\filename.txt*.
readjournal	Reads the USN records in the USN journal.
minver=`<number>`	Minimum Major Version of USN_RECORD to return. Default = 2.
maxver=`<number>`	Maximum Major Version of USN_RECORD to return. Default = 4.
startusn=`<USN number>`	USN to start reading the USN journal from. Default = 0.

Remarks

- Programs can consult the USN change journal to determine all the modifications made to a set of files. The USN change journal is much more efficient than checking time stamps or registering for file notifications. The USN change journal is enabled and used by the Indexing Service, File Replication Service (FRS), Remote Installation Services (RIS), and Remote Storage.
- If a change journal already exists on a volume, the **createjournal** parameter updates the change journal's **maxsize** and **allocationdelta** parameters. This enables you to expand the number of records that an active journal maintains without having to disable it.
- The change journal can grow larger than this target value, but the change journal is truncated at the next NTFS checkpoint to less than this value. NTFS examines the change journal and trims it when its size exceeds the value of **maxsize** plus the value of **allocationdelta**. At NTFS checkpoints, the operating system writes records to the NTFS log file that enable NTFS to determine what processing is required to recover from a failure.
- The change journal can grow to more than the sum of the values of **maxsize** and **allocationdelta** before being trimmed.
- Deleting or disabling an active change journal is very time consuming, because the system must access all the records in the master file table (MFT) and set the last USN attribute to 0 (zero). This process can take several minutes, and it can continue after the system restarts, if a restart is necessary. During this process, the change journal is not considered active, nor is it disabled. While the system is disabling the journal, it cannot be accessed, and all journal operations return errors. You should use extreme care when disabling an active journal, because it adversely affects other applications that are using the journal.

Examples

To create a USN change journal on drive C, type:

```
fsutil usn createjournal m=1000 a=100 c:
```

To delete an active USN change journal on drive C, type:

```
fsutil usn deletejournal /d c:
```

To enable range tracking with a specified chunk-size and file-size-threshold, type:

```
fsutil usn enablerangetracking c=16384 s=67108864 C:
```

To enumerate and list the change journal entries between two specified boundaries on drive C, type:

```
fsutil usn enumdata 1 0 1 c:
```

To query USN data for a volume on drive C, type:

```
fsutil usn queryjournal c:
```

To read the USN data for a file in the \Temp folder on drive C, type:

```
fsutil usn readdata c:\temp\sample.txt
```

To read the USN journal with a specific start USN, type:

```
fsutil usn readjournal startusn=0xF00
```

Related links

- Command-Line Syntax Key
- fsutil

fsutil volume

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10, Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8

Dismounts a volume, or queries the hard disk drive to determine how much free space is currently available on the hard disk drive or which file is using a particular cluster.

Syntax

```
fsutil volume [allocationreport] <volumepath>
fsutil volume [diskfree] <volumepath>
fsutil volume [dismount] <volumepath>
fsutil volume [filelayout] <volumepath> <fileID>
fsutil volume [list]
fsutil volume [querycluster] <volumepath> <cluster> [<cluster>] … …
```

Parameters

Parameter	Description
allocationreport	Displays information about how storage is used on a given volume.
`<volumepath>`	Specifies the drive letter (followed by a colon).
diskfree	Queries the hard disk drive to determine the amount of free space on it.
dismount	Dismounts a volume.
filelayout	Displays NTFS metadata for the given file.
`<fileID>`	Specifies the file id.
list	Lists all of the volumes on the system.
querycluster	Finds which file is using a specified cluster. You can specify multiple clusters with the **querycluster** parameter.
`<cluster>`	Specifies the logical cluster number (LCN).

Examples

To display an allocated clusters report, type:

```
fsutil volume allocationreport C:
```

To dismount a volume on drive C, type:

```
fsutil volume dismount c:
```

To query the amount of free space of a volume on drive C, type:

```
fsutil volume diskfree c:
```

To display all the information about a specified file(s), type:

```
fsutil volume C: *
fsutil volume C:\Windows
fsutil volume C: 0x00040000000001bf
```

To list the volumes on disk, type:

```
fsutil volume list
```

To find the file(s) that are using the clusters, specified by the logical cluster numbers 50 and 0x2000, on drive C, type:

```
fsutil volume querycluster C: 50 0x2000
```

Related links

- Command-Line Syntax Key
- fsutil
- How NTFS Works

fsutil wim

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10

Provides functions to discover and manage Windows Image (WIM)-backed files.

Syntax

```
fsutil wim [enumfiles] <drive name> <data source>
fsutil wim [enumwims] <drive name>
fsutil wim [queryfile] <filename>
fsutil wim [removewim] <drive name> <data source>
```

Parameters

Parameter	Description
enumfiles	Enumerates WIM backed files.
`<drive name>`	Specifies the drive name.
`<data source>`	Specifies the data source.
enumwims	Enumerates backing WIM files.
queryfile	Queries if the file is backed by WIM, and if so, displays details about the WIM file.
`<filename>`	Specifies the filename.
removewim	Removes a WIM from backing files.

Examples

To enumerate the files for drive C: from data source 0, type:

```
fsutil wim enumfiles C: 0
```

To enumerate backing WIM files for drive C:, type:

```
fsutil wim enumwims C:
```

To see if a file is backed by WIM, type:

```
fsutil wim queryFile C:\Windows\Notepad.exe
```

To remove the WIM from backing files for volume C: and data source 2, type:

```
fsutil wim removewims C: 2
```

Related links

- Command-Line Syntax Key
- fsutil

ftp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Transfers files to and from a computer running a File Transfer Protocol (ftp) server service. This command can be used interactively or in batch mode by processing ASCII text files.

Syntax

```
ftp [-v] [-d] [-i] [-n] [-g] [-s:<filename>] [-a] [-A] [-x:<sendbuffer>] [-
r:<recvbuffer>] [-b:<asyncbuffers>][-w:<windowssize>][<host>] [-?]
```

Parameters

Parameter	Description
-v	Suppresses display of remote server responses.
-d	Enables debugging, displaying all commands passed between the FTP client and FTP server.
-i	Disables interactive prompting during multiple file transfers.
-n	Suppresses auto-login upon initial connection.
-g	Disables file name globbing. **Glob** permits the use of the asterisk (*) and question mark (?) as wildcard characters in local file and path names.
-s:`<filename>`	Specifies a text file that contains **ftp** commands. These commands run automatically after **ftp** starts. This parameter allows no spaces. Use this parameter instead of redirection (`<`). **Note:** In Windows 8 and Windows Server 2012 or later operating systems, the text file must be written in UTF-8.
-a	Specifies that any local interface can be used when binding the ftp data connection.
-A	Logs onto the ftp server as anonymous.
-x:`<sendbuffer>`	Overrides the default SO_SNDBUF size of 8192.

Parameter	Description
-r:`<recvbuffer>`	Overrides the default SO_RCVBUF size of 8192.
-b: `<asyncbuffers>`	Overrides the default async buffer count of 3.
-w:`<windowssize>`	Specifies the size of the transfer buffer. The default window size is 4096 bytes.
`<host>`	Specifies the computer name, IP address, or IPv6 address of the ftp server to which to connect. The host name or address, if specified, must be the last parameter on the line.
-?	Displays help at the command prompt.

Remarks

- The **ftp** command-line parameters are case-sensitive.
- This command is available only if the **Internet Protocol (TCP/IP)** protocol is installed as a component in the properties of a network adapter in Network Connections.
- The **ftp** command can be used interactively. After it is started, **ftp** creates a sub-environment in which you can use **ftp** commands. You can return to the command prompt by typing the **quit** command. When the **ftp** sub-environment is running, it is indicated by the `ftp >` command prompt. For more information, see the **ftp** commands.
- The **ftp** command supports the use of IPv6 when the IPv6 protocol is installed.

Examples

To log on to the ftp server named `ftp.example.microsoft.com`, type:

```
ftp ftp.example.microsoft.com
```

To log on to the ftp server named `ftp.example.microsoft.com` and run the **ftp** commands contained in a file named *resync.txt*, type:

```
ftp -s:resync.txt ftp.example.microsoft.com
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance
- IP version 6
- IPv6 applications

ftp append

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Appends a local file to a file on the remote computer using the current file type setting.

Syntax

```
append <localfile> [remotefile]
```

Parameters

Parameter	Description
`<localfile>`	Specifies the local file to add.
[remotefile]	Specifies the file on the remote computer to which `<localfile>` is added. If you don't use this parameter, the `<localfile>` name is used in place of the remote file name.

Examples

To append *file1.txt* to *file2.txt* on the remote computer, type:

```
append file1.txt file2.txt
```

To append the local *file1.txt* to a file named *file1.txt* on the remote computer.

```
append file1.txt
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp ascii

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets the file transfer type to ASCII. The **ftp** command supports both ASCII (default) and binary image file transfer types, but we recommend using ASCII when transferring text files. In ASCII mode, character conversions to and from the network standard character set are performed. For example, end-of-line characters are converted as necessary, based on the target operating system.

Syntax

```
ascii
```

Examples

To set the file transfer type to ASCII, type:

```
ascii
```

Related links

- Command-Line Syntax Key
- ftp binary command
- Additional FTP guidance

ftp bell

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Toggles an audible sound to occur after each file transfer command is completed. By default, this command is toggled off.

Syntax

```
bell
```

Examples

To toggle an audible sound to occur after each file transfer command is completed, type:

```
bell
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp binary

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets the file transfer type to binary. The **ftp** command supports both ASCII (default) and binary image file transfer types, but we recommend using binary when transferring executable files. In binary mode, files are transferred in one-byte units.

Syntax

```
binary
```

Examples

To set the file transfer type to binary, type:

```
binary
```

Related links

- Command-Line Syntax Key
- ftp ascii command
- Additional FTP guidance

ftp bye

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Ends the ftp session on the remote computer, and then exits.

> **Note**
>
> This command is the same as the **ftp quit command**.

Syntax

```
bye
```

Examples

To end the ftp session with the remote computer and exit, type:

```
bye
```

Related links

- Command-Line Syntax Key
- ftp quit command
- Additional FTP guidance

ftp cd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the working directory on the remote computer.

Syntax

```
cd <remotedirectory>
```

Parameters

Parameter	Description
`<remotedirectory>`	Specifies the directory on the remote computer to which you want to change.

Examples

To change the directory on the remote computer to *Docs*, type:

```
cd Docs
```

To change the directory on the remote computer to *May Videos*, type:

```
cd  May Videos
```

Related links

- Command-Line Syntax Key

- Additional FTP guidance

ftp close

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Ends the ftp session with the remote server and remains at the `ftp>` prompt.

Syntax

```
close
```

Examples

To end the ftp session with the remote server and remain at the `ftp>` prompt, type:

```
close
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp debug

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Toggles Debugging mode. By default, Debugging mode is turned off. If Debugging mode is turned on, you'll see each command sent to the remote computer, preceeded by the `>` character.

Syntax

```
debug
```

Examples

To toggle debug mode on and off, type:

```
debug
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp delete

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Deletes files on remote computers.

Syntax

```
delete <remotefile>
```

Parameters

Parameter	Description
`<remotefile>`	Specifies the file to delete.

Examples

To delete the *test.txt* file on the remote computer, type:

```
delete test.txt
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp dir

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays a list of directory files and subdirectories on a remote computer.

Syntax

```
dir [<remotedirectory>] [<localfile>]
```

Parameters

Parameter	Description
`[<remotedirectory>]`	Specifies the directory for which you want to see a listing. If no directory is specified, the current working directory on the remote computer is used.
`[<localfile>]`	Specifies a local file in which to store the directory listing. If a local file is not specified, results are displayed on the screen.

Examples

To display a directory listing for *dir1* on the remote computer, type:

```
dir dir1
```

To save a list of the current directory on the remote computer in the local file *dirlist.txt*, type:

```
dir . dirlist.txt
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp disconnect

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Disconnects from the remote computer and remains at the `ftp>` prompt.

Syntax

```
disconnect
```

Examples

To disconnect from the remote computer and remains at the `ftp>` prompt, type:

```
disconnect
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp get

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies a remote file to the local computer using the current file transfer type.

> **Note**
>
> This command is the same as the **ftp recv command**.

Syntax

```
get <remotefile> [<localfile>]
```

Parameters

Parameter	Description
`<remotefile>`	Specifies the remote file to copy.
`[<localfile>]`	Specifies the name of the file to use on the local computer. If *localfile* isn't specified, the file is given the name of the *remotefile*.

Examples

To copy *test.txt* to the local computer using the current file transfer, type:

```
get test.txt
```

To copy *test.txt* to the local computer as *test1.txt* using the current file transfer, type:

```
```

```
get test.txt test1.txt
```

Related links

- Command-Line Syntax Key
- ftp recv command
- ftp ascii command
- ftp binary command
- Additional FTP guidance

ftp glob

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Toggles allowing wildcard expansion for local file names. By default, globbing (wildcard expansion) is turned on. If globbing is turned on, you'll be able to use the asterisk (*) and question mark (?) as wildcard characters in local file or path names.

Syntax

```
glob
```

Examples

To toggle whether to allow wildcard expansion of local file names, type:

```
glob
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp hash

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Toggles number sign (#) printing for each transferred data block. By default, the hash command is turned off. The size of a data block is 2048 bytes.

Syntax

```
hash
```

Examples

To toggle number sign (#) printing for each data block that is transferred, type:

```
hash
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp lcd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the working directory on the local computer. By default, the working directory is the directory in which the **ftp** command was started.

Syntax

```
lcd [<directory>]
```

Parameters

Parameter	Description
`[<directory>]`	Specifies the directory on the local computer to which to change. If *directory* isn't specified, the current working directory is changed to the default directory.

Examples

To change the working directory on the local computer to *c:\dir1*, type:

```
lcd c:\dir1
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp literal

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sends verbatim arguments to the remote ftp server. A single ftp reply code is returned.

> **Note**
>
> This command is the same as the **ftp quote command**.

Syntax

```
literal <argument> [ ]
```

Parameters

Parameter	Description
`<argument>`	Specifies the argument to send to the ftp server.

Examples

To send a **quit** command to the remote ftp server, type:

```
literal quit
```

Related links

- Command-Line Syntax Key
- ftp quote command

- Additional FTP guidance

ftp ls

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays an abbreviated list of files and subdirectories from the remote computer.

Syntax

```
ls [<remotedirectory>] [<localfile>]
```

Parameters

Parameter	Description
`[<remotedirectory>]`	Specifies the directory for which you want to see a listing. If no directory is specified, the current working directory on the remote computer is used.
`[<localfile>]`	Specifies a local file in which to store the listing. If a local file is not specified, results are displayed on the screen.

Examples

To display an abbreviated list of files and subdirectories from the remote computer, type:

```
ls
```

To get an abbreviated directory listing of *dir1* on the remote computer and save it in a local file called *dirlist.txt*, type:

```
ls dir1 dirlist.txt
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp mget

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies remote files to the local computer using the current file transfer type.

Syntax

```
mget <remotefile>[ ]
```

Parameters

Parameter	Description
`<remotefile>`	Specifies the remote files to copy to the local computer.

Examples

To copy remote files *a.exe* and *b.exe* to the local computer using the current file transfer type, type:

```
mget a.exe b.exe
```

Related links

- Command-Line Syntax Key
- ftp ascii command
- ftp binary command
- Additional FTP guidance

ftp mkdir

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates a directory on the remote computer.

Syntax

```
mkdir <directory>
```

Parameters

Parameter	Description
`<directory>`	Specifies the name of the new remote directory.

Examples

To create a directory called *dir1* on the remote computer, type:

```
mkdir dir1
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp mls

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays an abbreviated list of files and subdirectories in a remote directory.

Syntax

```
mls <remotefile>[ ] <localfile>
```

Parameters

Parameter	Description
`<remotefile>`	Specifies the file for which you want to see a listing. When specifying *remotefiles*, use a hyphen to represent the current working directory on the remote computer.
`<localfile>`	Specifies a local file in which to store the listing. When specifying *localfile*, use a hyphen to display the listing on the screen.

Examples

To display an abbreviated list of files and subdirectories for *dir1* and *dir2*, type:

```
mls dir1 dir2 -
```

To save an abbreviated list of files and subdirectories for *dir1* and *dir2* in the local file *dirlist.txt*, type:

```
mls dir1 dir2 dirlist.txt
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp mput

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies local files to the remote computer using the current file transfer type.

Syntax

```
mput <localfile>[ ]
```

Parameters

Parameter	Description
`<localfile>`	Specifies the local file to copy to the remote computer.

Examples

To copy *Program1.exe* and *Program2.exe* to the remote computer using the current file transfer type, type:

```
mput Program1.exe Program2.exe
```

Related links

- Command-Line Syntax Key
- ftp ascii command
- ftp binary command
- Additional FTP guidance

ftp open

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Connects to the specified ftp server.

Syntax

```
open <computer> [<port>]
```

Parameters

Parameter	Description
`<computer>`	Specifies the remote computer to which you are trying to connect. You can use an IP address or computer name (in which case a DNS server or Hosts file must be available).
`[<port>]`	Specifies a TCP port number to use to connect to an ftp server. By default, TCP port 21 is used.

Examples

To connect to the ftp server at *ftp.microsoft.com*, type:

```
open ftp.microsoft.com
```

To connect to the ftp server at *ftp.microsoft.com* that is listening on TCP port *755*, type:

```
open ftp.microsoft.com 755
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp prompt

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Toggles Prompt mode on and off. By default, Prompt mode is turned on. If Prompt mode is turned on, the ftp command prompts during multiple file transfers to allow you to selectively retrieve or store files.

> **Note**
>
> You can use the **ftp mget** and **ftp mput** commands to transfer all files when Prompt mode is turned off.

Syntax

```
prompt
```

Examples

To toggle Prompt mode on and off, type:

```
prompt
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp put

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies a local file to the remote computer using the current file transfer type.

> **Note**
>
> This command is the same as the **ftp send command**.

Syntax

```
put <localfile> [<remotefile>]
```

Parameters

Parameter	Description
`<localfile>`	Specifies the local file to copy.
`[<remotefile>]`	Specifies the name to use on the remote computer. If you don't specify a *remotefile*, the file is give the *localfile* name.

Examples

To copy the local file *test.txt* and name it *test1.txt* on the remote computer, type:

```
put test.txt test1.txt
```

To copy the local file *program.exe* to the remote computer, type:

```
put program.exe
```

Related links

- Command-Line Syntax Key
- ftp ascii command
- ftp binary command
- Additional FTP guidance

ftp pwd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the current remote computer directory.

Syntax

```
pwd
```

Examples

To display the current remote computer directory, type:

```
pwd
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp quit

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Ends the ftp session with the remote computer, and then exits.

> **Note**
>
> This command is the same as the **ftp bye command**.

Syntax

```
quit
```

Examples

To end the ftp session with the remote computer and return to the operating system command prompt, type:

```
quit
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp quote

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sends verbatim arguments to the remote ftp server. A single ftp reply code is returned.

> **Note**
>
> This command is the same as the **ftp literal command**.

Syntax

```
quote <argument>[ ]
```

Parameters

Parameter	Description
`<argument>`	Specifies the argument to send to the ftp server.

Examples

To send a **quit** command to the remote ftp server, type:

```
quote quit
```

Related links

- Command-Line Syntax Key
- ftp literal command

- Additional FTP guidance

ftp recv

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies a remote file to the local computer using the current file transfer type.

> **Note**
>
> This command is the same as the **ftp get command**.

Syntax

```
recv <remotefile> [<localfile>]
```

Parameters

Parameter	Description
`<remotefile>`	Specifies the remote file to copy.
`[<localfile>]`	Specifies the name of the file to use on the local computer. If *localfile* isn't specified, the file is given the name of the *remotefile*.

Examples

To copy *test.txt* to the local computer using the current file transfer, type:

```
recv test.txt
```

To copy *test.txt* to the local computer as *test1.txt* using the current file transfer, type:

```
```

```
recv test.txt test1.txt
```

Related links

- Command-Line Syntax Key
- ftp get command
- ftp ascii command
- ftp binary command
- Additional FTP guidance

ftp remotehelp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays help for remote commands.

Syntax

```
remotehelp [<command>]
```

Parameters

Parameter	Description
`[<command>]`	Specifies the name of the command about which you want help. If `<command>` isn't specified, this command displays a list of all remote commands. You can also run remote commands using ftp quote or ftp literal.

Examples

To display a list of remote commands, type:

```
remotehelp
```

To display the syntax for the *feat* remote command, type:

```
remotehelp feat
```

Related links

- Command-Line Syntax Key

- ftp quote
- ftp literal
- Additional FTP guidance

ftp rename

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Renames remote files.

Syntax

```
rename <filename> <newfilename>
```

Parameters

Parameter	Description
`<filename>`	Specifies the file that you want to rename.
`<newfilename>`	Specifies the new file name.

Examples

To rename the remote file *example.txt* to *example1.txt*, type:

```
rename example.txt example1.txt
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp rmdir

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Deletes a remote directory.

Syntax

```
rmdir <directory>
```

Parameters

Parameter	Description
`<directory>`	Specifies the name of the remote directory to delete.

Examples

To delete the *pictures* remote directory, type:

```
rmdir pictures
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp send

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies a local file to the remote computer using the current file transfer type.

> **Note**
>
> This command is the same as the **ftp put command**.

Syntax

```
send <localfile> [<remotefile>]
```

Parameters

Parameter	Description
`<localfile>`	Specifies the local file to copy.
`<remotefile>`	Specifies the name to use on the remote computer. If you don't specify a *remotefile*, the file will get the *localfile* name.

Examples

To copy the local file *test.txt* and name it *test1.txt* on the remote computer, type:

```
send test.txt test1.txt
```

To copy the local file *program.exe* to the remote computer, type:

```
send program.exe
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp status

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the current status of ftp connections.

Syntax

```
status
```

Examples

To display the current status of ftp connections, type:

```
status
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp trace

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Toggles packet tracing. This command also displays the series of internal FTP function calls when running a **ftp** command.

Syntax

```
trace
```

Examples

Toggle tracing on and off, type:

```
trace
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp type

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets or displays the file transfer type. The **ftp** command supports both ASCII (default) and binary image file transfer types:

- We recommend using ASCII when transferring text files. In ASCII mode, character conversions to and from the network standard character set are performed. For example, end-of-line characters are converted as necessary, based on the target operating system.
- We recommend using binary when transferring executable files. In binary mode, files are transferred in one-byte units.

Syntax

```
type [<typename>]
```

Parameters

Parameter	Description
`[<typename>]`	Specifies the file transfer type. If you don't specify this parameter, the current type is displayed.

Examples

To set the file transfer type to ASCII, type:

```
type ascii
```

To set the transfer file type to binary, type:

```
type binary
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp user

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Specifies a user to the remote computer.

Syntax

```
user <username> [<password>] [<account>]
```

Parameters

Parameter	Description
`<username>`	Specifies a user name with which to log on to the remote computer.
`[<password>]`	Specifies the password for *username*. If a password is not specified but is required, the **ftp** command prompts for the password.
`[<account>]`	Specifies an account with which to log on to the remote computer. If an *account* isn't specified but is required, the **ftp** command prompts for the account.

Examples

To specify *User1* with the password *Password1*, type:

```
user User1 Password1
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp verbose

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Toggles Verbose mode. By default, Verbose mode is turned on. When Verbose mode is on, all **ftp** command responses are displayed. When a file transfer is completed, statistics regarding the efficiency of the transfer are also displayed.

Syntax

```
verbose
```

Examples

To toggle Verbose mode on and off, type:

```
verbose
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp mdelete

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Deletes files on the remote computer.

Syntax

```
mdelete <remotefile>[...]
```

Parameters

Parameter	Description
`<remotefile>`	Specifies the remote file to delete.

Examples

To delete remote files *a.exe* and *b.exe*, type:

```
mdelete a.exe b.exe
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftp mdir

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays a directory list of files and subdirectories in a remote directory.

Syntax

```
mdir <remotefile>[...] <localfile>
```

Parameters

Parameter	Description
`<remotefile>`	Specifies the directory or file for which you want to see a listing. You can specify multiple *remotefiles*. Type a hyphen (-) to use the current working directory on the remote computer.
`<localfile>`	Specifies a local file to store the listing. This parameter is required. Type a hyphen (-) to display the listing on the screen.

Examples

To display a directory listing of *dir1* and *dir2* on the screen, type:

```
mdir dir1 dir2 -
```

To save the combined directory listing of *dir1* and *dir2* in a local file called *dirlist.txt*, type:

```
mdir dir1 dir2 dirlist.txt
```

Related links

- Command-Line Syntax Key
- Additional FTP guidance

ftype

Article • 02/03/2023

Displays or modifies file types that are used in file name extension associations. If used without an assignment operator (=), this command displays the current open command string for the specified file type. If used without parameters, this command displays the file types that have open command strings defined.

> **Note**
>
> This command is only supported within cmd.exe and is not available from PowerShell. Though you can use `cmd /c ftype` as a workaround.

Syntax

```
ftype [<filetype>[=[<opencommandstring>]]]
```

Parameters

Parameter	Description
`<filetype>`	Specifies the file type to display or change.
`<opencommandstring>`	Specifies the open command string to use when opening files of the specified file type.
/?	Displays help at the command prompt.

Remarks

The following table describes how **ftype** substitutes variables within an open command string:

Variable	Replacement value
`%0` or `%1`	Gets substituted with the file name being launched through the association.

Variable	Replacement value
`%*`	Gets all of the parameters.
`%2`, `%3`, ...	Gets the first parameter (`%2`), the second parameter (`%3`), and so on.
`%~<n>`	Gets all of the remaining parameters starting with the *n*th parameter, where *n* can be any number from 2 to 9.

Examples

To display the current file types that have open command strings defined, type:

```
ftype
```

To display the current open command string for the *txtfile* file type, type:

```
ftype txtfile
```

This command produces output similar to the following:

`txtfile=%SystemRoot%\system32\NOTEPAD.EXE %1`

To delete the open command string for a file type called *example*, type:

```
ftype example=
```

To associate the .pl file name extension with the PerlScript file type and enable the PerlScript file type to run PERL.EXE, type the following commands:

```
assoc .pl=PerlScript
ftype PerlScript=perl.exe %1 %*
```

To eliminate the need to type the .pl file name extension when invoking a Perl script, type:

```
set PATHEXT=.pl;%PATHEXT%
```

Related links

- Command-Line Syntax Key

fveupdate

Article • 02/03/2023

FveUpdate is an internal tool, used by the setup program when a computer is upgraded. It updates the metadata associated with BitLocker to the latest version. This tool cannot be run independently.

Related links

- Command-Line Syntax Key

getmac

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network. This command is particularly useful either when you want to enter the MAC address into a network analyzer, or when you need to know what protocols are currently in use on each network adapter on a computer.

Syntax

```
getmac[.exe][/s <computer> [/u <domain\<user> [/p <password>]]][/fo {table | list | csv}][/nh][/v]
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
/u `<domain>\` `<user>`	Runs the command with the account permissions of the user specified by *user* or *domain**user*. The default is the permissions of the current logged on user on the computer issuing the command.
/p `<password>`	Specifies the password of the user account that is specified in the **/u** parameter.
/fo {table | list | csv}	Specifies the format to use for the query output. Valid values are **table**, **list**, and **csv**. The default format for output is **table**.
/nh	Suppresses column header in output. Valid when the **/fo** parameter is set to **table** or **csv**.
/v	Specifies that the output display verbose information.
/?	Displays help at the command prompt.

Examples

The following examples show how you can use the **getmac** command:

```
getmac /fo table /nh /v
```

```
getmac /s srvmain
```

```
getmac /s srvmain /u maindom\hiropln
```

```
getmac /s srvmain /u maindom\hiropln /p p@ssW23
```

```
getmac /s srvmain /u maindom\hiropln /p p@ssW23 /fo list /v
```

```
getmac /s srvmain /u maindom\hiropln /p p@ssW23 /fo table /nh
```

Related links

- Command-Line Syntax Key

gettype

Article • 05/22/2023

Applies to: Windows Server (All supported versions)

The `gettype` command is deprecated and may not be supported in future releases of Windows.

`gettype` is included in Windows Server 2003. For more information, see gettype.

Related links

- Command-Line Syntax Key

goto

Article • 02/03/2023

Directs cmd.exe to a labeled line in a batch program. Within a batch program, this command directs command processing to a line that is identified by a label. When the label is found, processing continues starting with the commands that begin on the next line.

Syntax

```
goto <label>
```

Parameters

Parameter	Description
`<label>`	Specifies a text string that is used as a label in the batch program.
/?	Displays help at the command prompt.

Remarks

- If command extensions are enabled (the default), and you use the **goto** command with a target label of **:EOF**, you transfer control to the end of the current batch script file and exit the batch script file without defining a label. When you use this command with the **:EOF** label, you must insert a colon before the label. For example: `goto:EOF`.

- You can use spaces in the *label* parameter, but you can't include other separators (for example, semicolons (;) or equal signs (=)).

- The *label* value that you specify must match a label in the batch program. The label within the batch program must begin with a colon (:). If a line begins with a colon, it's treated as a label and any commands on that line are ignored. If your batch program doesn't contain the label that you specify in the *label* parameter, then the batch program stops and displays the following message: `Label not found`.

- You can use **goto** with other commands to perform conditional operations. For more information about using **goto** for conditional operations, see the if command.

Examples

The following batch program formats a disk in drive A as a system disk. If the operation is successful, the **goto** command directs processing to the **:end** label:

```
echo off
format a: /s
if not errorlevel 1 goto end
echo An error occurred during formatting.
:end
echo End of batch program.
```

Related links

- Command-Line Syntax Key
- cmd command
- if command

gpfixup

Article • 02/03/2023

Fixes domain name dependencies in Group Policy Objects and Group Policy links after a domain rename operation. To use this command, you must install Group Policy Management as a feature through Server Manager.

Syntax

```
gpfixup [/v]
[/olddns:<olddnsname> /newdns:<newdnsname>]
[/oldnb:<oldflatname> /newnb:<newflatname>]
[/dc:<dcname>] [/sionly]
[/user:<username> [/pwd:{<password>|*}]] [/?]
```

Parameters

Parameter	Description
/v	Displays detailed status messages. If this parameter isn't used, only error messages or a summary status message stating, **SUCCESS** or **FAILURE** appears.
/olddns:`<olddnsname>`	Specifies the old DNS name of the renamed domain as `<olddnsname>` when the domain rename operation changes the DNS name of a domain. You can use this parameter only if you also use the **/newdns** parameter to specify a new domain DNS name.
/newdns:`<newdnsname>`	Specifies the new DNS name of the renamed domain as `<newdnsname>` when the domain rename operation changes the DNS name of a domain. You can use this parameter only if you also use the **/olddns** parameter to specify the old domain DNS name.
/oldnb:`<oldflatname>`	Specifies the old NetBIOS name of the renamed domain as `<oldflatname>` when the domain rename operation changes the NetBIOS name of a domain. You can use this parameter only if you use the **/newnb** parameter to specify a new domain NetBIOS name.
/newnb:`<newflatname>`	Specifies the new NetBIOS name of the renamed domain as `<newflatname>` when the domain rename operation changes the NetBIOS name of a domain. You can use this parameter only if you use the **/oldnb** parameter to specify the old domain NetBIOS name.

Parameter	Description
/dc:`<dcname>`	Connect to the domain controller named `<dcname>` (a DNS name or a NetBIOS name). `<dcname>` must host a writable replica of the domain directory partition as indicated by one of the following: • The DNS name `<newdnsname>` by using **/newdns** • The NetBIOS name `<newflatname>` by using **/newnb** If this parameter isn't used, you can connect to any domain controller in the renamed domain indicated by `<newdnsname>` or `<newflatname>`.
/sionly	Performs only the Group Policy fix that relates to managed software installation (the Software Installation extension for Group Policy). Skip the actions that fix Group Policy links and the SYSVOL paths in GPOs.
/user:`<username>`	Runs this command in the security context of the user `<username>`, where `<username>` is in the format domain\user. If this parameter isn't used, this command runs as the logged in user.
/pwd:`{<password> | *}`	Specifies the password for the user.
/?	Displays Help at the command prompt.

Examples

This example assumes that you have already performed a domain rename operation in which you changed the DNS name from **MyOldDnsName** to **MyNewDnsName**, and the NetBIOS name from **MyOldNetBIOSName** to **MyNewNetBIOSName**.

In this example, you use the **gpfixup** command to connect to the domain controller named **MyDcDnsName** and repair GPOs and Group Policy links by updating the old domain name embedded in the GPOs and links. Status and error output is saved to a file that is named **gpfixup.log**.

```
gpfixup /olddns: MyOldDnsName /newdns:MyNewDnsName /oldnb:MyOldNetBIOSName
/newnb:MyNewNetBIOSName /dc:MyDcDnsName 2>&1 >gpfixup.log
```

This example is the same as the previous one, except that it assumes the NetBIOS name of the domain was not changed during the domain rename operation.

```
gpfixup /olddns: MyOldDnsName /newdns:MyNewDnsName /dc:MyDcDnsName 2>&1
>gpfixup.log
```

Related links

- Command-Line Syntax Key
- Administering Active Directory Domain Rename

gpresult

Article • 09/29/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the Resultant Set of Policy (RSoP) information for a remote user and computer. To use RSoP reporting for remotely targeted computers through the firewall, you must have firewall rules that enable inbound network traffic on the ports.

Syntax

```
gpresult [/s <system> [/u <username> [/p [<password>]]]] [/user
[<targetdomain>\]<targetuser>] [/scope {user | computer}] {/r | /v | /z |
[/x | /h] <filename> [/f] | /?}
```

> **Note**
>
> Except when using **/?**, you must include an output option, **/r**, **/v**, **/z**, **/x**, or **/h**.

Parameters

Parameter	Description
/s `<system>`	Specifies the name or IP address of a remote computer. Don't use backslashes. The default is the local computer.
/u `<username>`	Uses the credentials of the specified user to run the command. The default user is the user who is signed in to the computer that issues the command.
/p `[<password>]`	Specifies the password of the user account that is provided in the **/u** parameter. If **/p** is omitted, **gpresult** prompts for the password. The **/p** parameter can't be used with **/x** or **/h**.
/user `[<targetdomain>\]<targetuser>]`	Specifies the remote user whose RSoP data is to be displayed.
/scope `{user | computer}`	Displays RSoP data for either the user or the computer. If **/scope** is omitted, **gpresult** displays RSoP data for both the user and the

Parameter	Description
computer.	
`[/x | /h] <filename>`	Saves the report in either XML (**/x**) or HTML (**/h**) format at the location and with the file name that is specified by the *filename* parameter. Can't be used with **/u**, **/p**, **/r**, **/v**, or **/z**.
/f	Forces **gpresult** to overwrite the file name that is specified in the **/x** or **/h** option.
/r	Displays RSoP summary data.
/v	Displays verbose policy information. This includes detailed settings that were applied with a precedence of 1.
/z	Displays all available information about Group Policy. This includes detailed settings that were applied with a precedence of 1 and higher.
/?	Displays help at the command prompt.

Remarks

- Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, Group Policy is applied to users or computers based on their membership in sites, domains, or organizational units.
- Because you can apply overlapping policy settings to any computer or user, the Group Policy feature generates a resulting set of policy settings when the user signs in. The **gpresult** command displays the resulting set of policy settings that were enforced on the computer for the specified user when the user signed in.
- Because **/v** and **/z** produce much information, it's useful to redirect output to a text file (for example, `gpresult/z >policy.txt`).
- On ARM64 versions of Windows, only the `gpresult` in SysWow64 works with the `/h` parameter.

Examples

To retrieve RSoP data for only the remote user *maindom\targetuser*, on the computer *srvmain*, enter:

```
```

```
gpresult /s srvmain /user maindom\targetuser /scope user /r
```

To save all available information about Group Policy to a file named *policy.txt* for only the remote user *maindom\targetuser*, on the computer *srvmain*, enter:

```
gpresult /s srvmain /user maindom\targetuser /z > policy.txt
```

To display RSoP data for the signed-in user, *maindom\hiropln* with the password *p@ssW23*, for the computer *srvmain*, enter:

```
gpresult /s srvmain /u maindom\hiropln /p p@ssW23 /r
```

Related links

- Command-Line Syntax Key

gpupdate

Article • 02/03/2023

Updates Group Policy settings.

Syntax

```
gpupdate [/target:{computer | user}] [/force] [/wait:<VALUE>] [/logoff]
[/boot] [/sync] [/?]
```

Parameters

Parameter	Description
/target:`{computer|user}`	Specifies that only User or only Computer policy settings are updated. By default, both User and Computer policy settings are updated.
/force	Reapplies all policy settings. By default, only policy settings that have changed are applied.
/wait:`<VALUE>`	Sets the number of seconds to wait for policy processing to finish before returning to the command prompt. When the time limit is exceeded, the command prompt appears, but policy processing continues. The default value is 600 seconds. The value **0** means not to wait. The value **-1** means to wait indefinitely. In a script, by using this command with a time limit specified, you can run **gpupdate** and continue with commands that do not depend upon the completion of **gpupdate**. Alternatively, you can use this command with no time limit specified to let **gpupdate** finish running before other commands that depend on it are run.
/logoff	Causes a logoff after the Group Policy settings are updated. This is required for those Group Policy client-side extensions that do not process policy on a background update cycle but do process policy when a user logs on. Examples include user-targeted Software Installation and Folder Redirection. This option has no effect if there are no extensions called that require a logoff.

Parameter	Description
/boot	Causes a computer restart after the Group Policy settings are applied. This is required for those Group Policy client-side extensions that do not process policy on a background update cycle but do process policy at computer startup. Examples include computer-targeted Software Installation. This option has no effect if there are no extensions called that require a restart.
/sync	Causes the next foreground policy application to be done synchronously. Foreground policy is applied at computer boot and user logon. You can specify this for the user, computer, or both, by using the **/target** parameter. The **/force** and **/wait** parameters are ignored if you specify them.
/?	Displays Help at the command prompt.

Examples

To force a background update of all Group Policy settings, regardless of whether they've changed, type:

```
gpupdate /force
```

Related links

- Command-Line Syntax Key

graftabl

Article • 02/03/2023

Enables Windows operating systems to display an extended character set in graphics mode. If used without parameters, **graftabl** displays the previous and the current code page.

> **ⓘ Important**
>
> The **graftabl** command is a legacy command, and therefore outdated. It is normally not installed in modern Windows versions. Please see the **chcp** page for codepage handling.

Syntax

```
graftabl <codepage>
graftabl /status
```

Parameters

Parameter	Description
`<codepage>`	Specifies a code page to define the appearance of extended characters in graphics mode. Valid code page identification numbers are: • **437** - United States • **850** - Multilingual (Latin I) • **852** - Slavic (Latin II) • **855** - Cyrillic (Russian) • **857** - Turkish • **860** - Portuguese • **861** - Icelandic • **863** - Canadian-French • **865** - Nordic • **866** - Russian • **869** - Modern Greek
/status	Displays the current code page being used by this command.
/?	Displays help at the command prompt.

Remarks

- The **graftabl** command affects only the monitor display of extended characters of the code page that you specify. It doesn't change the actual console input code page. To change the console input code page, use the mode or chcp command.
- Each exit code and a brief description of it:

Exit code	Description
0	Character set was loaded successfully. No previous code page was loaded.
1	An incorrect parameter was specified. No action was taken.
2	A file error occurred.

- You can use the ERRORLEVEL environment variable in a batch program to process exit codes that are returned by **graftabl**.

Examples

To view the current code page used by **graftabl**, type:

```
graftabl /status
```

To load the graphics character set for code page 437 (United States) into memory, type:

```
graftabl 437
```

To load the graphics character set for code page 850 (multilingual) into memory, type:

```
graftabl 850
```

Related links

- Command-Line Syntax Key
- freedisk command

- mode command
- chcp command

help

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays a list of the available commands or detailed help information on a specified command. If used without parameters, **help** lists and briefly describes every system command.

Syntax

```
help [<command>]
```

Parameters

Parameter	Description
`<command>`	Specifies the command for which to display detailed help information.

Examples

To view information about the **robocopy** command, type:

```
help robocopy
```

To display a list of all commands available in DiskPart, type:

```
help
```

To display detailed help information about how to use the **create partition primary** command in DiskPart, type:

```
```

```
help create partition primary
```

Related links

- Command-Line Syntax Key

helpctr

Article • 03/03/2021

The helpctr command has been deprecated, and isn't guaranteed to be supported in Windows.

This tool is included in Windows Server 2003. For more information, see Helpctr.

hostname

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the host name portion of the full computer name of the computer.

> **ⓘ Important**
>
> This command is available only if the Internet Protocol (TCP/IP) protocol is installed as a component in the properties of a network adapter in Network.

Syntax

```
hostname
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.

Any parameter different than `/?` produces an error message and sets the errorlevel to 1.

Notes

- Environment variable `%COMPUTERNAME%` usually will print the same string as `hostname`, but in uppercase.
- If environment variable `_CLUSTER_NETWORK_NAME_` is defined, `hostname` will print its value.

Examples

- To display the name of the computer, type:

```shell
hostname
```

- To display the name of the computer in uppercase:

```shell
echo %COMPUTERNAME%
```

- To alter the hostname output:

```shell
set "_CLUSTER_NETWORK_NAME_=Altered Computer Name"
hostname
```

Related links

- Command-Line Syntax Key

icacls

Article • 02/03/2023

Displays or modifies discretionary access control lists (DACLs) on specified files, and applies stored DACLs to files in specified directories.

> **Note**
>
> This command replaces the deprecated **cacls command**.

Syntax

```
icacls <filename> [/grant[:r] <sid>:<perm>[...]] [/deny <sid>:<perm>[...]]
[/remove[:g|:d]] <sid>[...]] [/t] [/c] [/l] [/q] [/setintegritylevel
<Level>:<policy>[...]]
icacls <directory> [/substitute <sidold> <sidnew> [...]] [/restore <aclfile>
[/c] [/l] [/q]]
```

Parameters

Parameter	Description
<filename>	Specifies the file for which to display or modify DACLs.
<directory>	Specifies the directory for which to display or modify DACLs.
/t	Performs the operation on all specified files in the current directory and its subdirectories.
/c	Continues the operation despite any file errors. Error messages will still be displayed.
/l	Performs the operation on a symbolic link instead of its destination.
/q	Suppresses success messages.
[/save <ACLfile> [/t] [/c] [/l] [/q]]	Stores DACLs for all matching files into an access control list (ACL) file for later use with **/restore**.
[/setowner <username> [/t] [/c] [/l] [/q]]	Changes the owner of all matching files to the specified user.

Parameter	Description
[/findsid <sid> [/t] [/c] [/l] [/q]]	Finds all matching files that contain a DACL explicitly mentioning the specified security identifier (SID).
[/verify [/t] [/c] [/l] [/q]]	Finds all files with ACLs that are not canonical or have lengths inconsistent with access control entry (ACE) counts.
[/reset [/t] [/c] [/l] [/q]]	Replaces ACLs with default inherited ACLs for all matching files.
[/grant[:r] <sid>:<perm>[...]]	Grants specified user access rights. Permissions replace previously granted explicit permissions. Not adding the **:r**, means that permissions are added to any previously granted explicit permissions.
[/deny <sid>:<perm>[...]]	Explicitly denies specified user access rights. An explicit deny ACE is added for the stated permissions and the same permissions in any explicit grant are removed.
[/remove[:g | :d]] <sid>[...] [/t] [/c] [/l] [/q]	Removes all occurrences of the specified SID from the DACL. This command can also use: • **:g** - Removes all occurrences of granted rights to the specified SID. • **:d** - Removes all occurrences of denied rights to the specified SID.
[/setintegritylevel [(CI)(OI)] <Level>:<Policy>[...]]	Explicitly adds an integrity ACE to all matching files. The level can be specified as: • **l** - Low • **m**- Medium • **h** - High Inheritance options for the integrity ACE may precede the level and are applied only to directories.
[/substitute <sidold><sidnew> [...]]	Replaces an existing SID (*sidold*) with a new SID (*sidnew*). Requires using with the `<directory>` parameter.
/restore <ACLfile> [/c] [/l] [/q]	Applies stored DACLs from `<ACLfile>` to files in the specified directory. Requires using with the `<directory>` parameter.
/inheritancelevel: [e | d | r]	Sets the inheritance level, which can be: • **e** - Enables inheritance • **d** - Disables inheritance and copies the ACEs • **r** - Disables inheritance and removes only inherited ACEs

Remarks

- SIDs may be in either numerical or friendly name form. If you use a numerical form, affix the wildcard character * to the beginning of the SID.
- This command preserves the canonical order of ACE entries as:
    - Explicit denials
    - Explicit grants
    - Inherited denials
    - Inherited grants
- The `<perm>` option is a permission mask that can be specified in one of the following forms:
    - A sequence of simple rights (basic permissions):
        - **F** - Full access
        - **M**- Modify access
        - **RX** - Read and execute access
        - **R** - Read-only access
        - **W** - Write-only access
    - A comma-separated list in parenthesis of specific rights (advanced permissions):
        - **D** - Delete
        - **RC** - Read control (read permissions)
        - **WDAC** - Write DAC (change permissions)
        - **WO** - Write owner (take ownership)
        - **S** - Synchronize
        - **AS** - Access system security
        - **MA** - Maximum allowed
        - **GR** - Generic read
        - **GW** - Generic write
        - **GE** - Generic execute

    - **GA** - Generic all
    - **RD** - Read data/list directory
    - **WD** - Write data/add file
    - **AD** - Append data/add subdirectory
    - **REA** - Read extended attributes
    - **WEA** - Write extended attributes
    - **X** - Execute/traverse
    - **DC** - Delete child
    - **RA** - Read attributes
    - **WA** - Write attributes
- Inheritance rights may precede either `<perm>` form:
    - **(I)** - Inherit. ACE inherited from the parent container.
    - **(OI)** - Object inherit. Objects in this container will inherit this ACE. Applies only to directories.
    - **(CI)** - Container inherit. Containers in this parent container will inherit this ACE. Applies only to directories.
    - **(IO)** - Inherit only. ACE inherited from the parent container, but does not apply to the object itself. Applies only to directories.
    - **(NP)** - Do not propagate inherit. ACE inherited by containers and objects from the parent container, but does not propagate to nested containers. Applies only to directories.

Examples

To save the DACLs for all files in the C:\Windows directory and its subdirectories to the ACLFile file, type:

```
icacls c:\windows\* /save aclfile /t
```

To restore the DACLs for every file within ACLFile that exists in the C:\Windows directory and its subdirectories, type:

```
icacls c:\windows\ /restore aclfile
```

To grant the user User1 Delete and Write DAC permissions to a file named Test1, type:

```
icacls test1 /grant User1:(d,wdac)
```

To grant the user defined by SID S-1-1-0 Delete and Write DAC permissions to a file, named Test2, type:

```
icacls test2 /grant *S-1-1-0:(d,wdac)
```

Related links

- Command-Line Syntax Key

if

Article • 02/03/2023

Performs conditional processing in batch programs.

Syntax

```
if [not] ERRORLEVEL <number> <command> [else <expression>]
if [not] <string1>==<string2> <command> [else <expression>]
if [not] exist <filename> <command> [else <expression>]
```

If command extensions are enabled, use the following syntax:

```
if [/i] <string1> <compareop> <string2> <command> [else <expression>]
if cmdextversion <number> <command> [else <expression>]
if defined <variable> <command> [else <expression>]
```

Parameters

Parameter	Description
not	Specifies that the command should be carried out only if the condition is false.
errorlevel `<number>`	Specifies a true condition only if the previous program run by Cmd.exe returned an exit code equal to or greater than *number*.
`<command>`	Specifies the command that should be carried out if the preceding condition is met.
`<string1>==<string2>`	Specifies a true condition only if *string1* and *string2* are the same. These values can be literal strings or batch variables (for example, `%1`). You do not need to enclose literal strings in quotation marks.
exist `<filename>`	Specifies a true condition if the specified file name exists.

Parameter	Description
`<compareop>`	Specifies a three-letter comparison operator, including: • **EQU** - Equal to • **NEQ** - Not equal to • **LSS** - Less than • **LEQ** - Less than or equal to • **GTR** - Greater than • **GEQ** - Greater than or equal to
/i	Forces string comparisons to ignore case. You can use **/i** on the `string1==string2` form of **if**. These comparisons are generic, in that if both *string1* and *string2* are comprised of numeric digits only, the strings are converted to numbers and a numeric comparison is performed.
cmdextversion `<number>`	Specifies a true condition only if the internal version number associated with the command extensions feature of Cmd.exe is equal to or greater than the number specified. The first version is 1. It increases by increments of one when significant enhancements are added to the command extensions. The **cmdextversion** conditional is never true when command extensions are disabled (by default, command extensions are enabled).
defined `<variable>`	Specifies a true condition if *variable* is defined.
`<expression>`	Specifies a command-line command and any parameters to be passed to the command in an **else** clause.
/?	Displays help at the command prompt.

Remarks

- If the condition specified in an **if** clause is true, the command that follows the condition is carried out. If the condition is false, the command in the **if** clause is ignored and the command executes any command that is specified in the **else** clause.

- When a program stops, it returns an exit code. To use exit codes as conditions, use the **errorlevel** parameter.

- If you use **defined**, the following three variables are added to the environment: **%errorlevel%**, **%cmdcmdline%**, and **%cmdextversion%**.

    - **%errorlevel%**: Expands into a string representation of the current value of the ERRORLEVEL environment variable. This variable assumes that there isn't already

an existing environment variable with the name ERRORLEVEL. If there is, you'll get that ERRORLEVEL value instead.

  - **%cmdcmdline%**: Expands into the original command line that was passed to Cmd.exe prior to any processing by Cmd.exe. This assumes that there isn't already an existing environment variable with the name CMDCMDLINE. If there is, you'll get that CMDCMDLINE value instead.

  - **%cmdextversion%**: Expands into the string representation of the current value of **cmdextversion**. This assumes that there isn't already an existing environment variable with the name CMDEXTVERSION. If there is, you'll get that CMDEXTVERSION value instead.

- You must use the **else** clause on the same line as the command after the **if**.

Examples

To display the message **Cannot find data file if the file Product.dat cannot be found**, type:

```
if not exist product.dat echo Cannot find data file
```

To format a disk in drive A and display an error message if an error occurs during the formatting process, type the following lines in a batch file:

```
:begin
@echo off
format a: /s
if not errorlevel 1 goto end
echo An error occurred during formatting.
:end
echo End of batch program.
```

To delete the file Product.dat from the current directory or display a message if Product.dat is not found, type the following lines in a batch file:

```
IF EXIST Product.dat (
del Product.dat
) ELSE (
```

```
echo The Product.dat file is missing.
)
```

> **Note**
>
> These lines can be combined into a single line as follows:
>
> ```
> IF EXIST Product.dat (del Product.dat) ELSE (echo The Product.dat file
> is missing.)
> ```

To echo the value of the ERRORLEVEL environment variable after running a batch file, type the following lines in the batch file:

```
goto answer%errorlevel%
:answer1
echo The program returned error level 1
goto end
:answer0
echo The program returned error level 0
goto end
:end
echo Done!
```

To go to the okay label if the value of the ERRORLEVEL environment variable is less than or equal to 1, type:

```
if %errorlevel% LEQ 1 goto okay
```

Related links

- Command-Line Syntax Key
- goto command

ipconfig

Article • 02/03/2023

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

Syntax

```
ipconfig [/allcompartments] [/all] [/renew [<adapter>]] [/release
[<adapter>]] [/renew6[<adapter>]] [/release6 [<adapter>]] [/flushdns]
[/displaydns] [/registerdns] [/showclassid <adapter>] [/setclassid <adapter>
[<classID>]]
```

Parameters

Parameter	Description
/all	Displays the full TCP/IP configuration for all adapters. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.
/displaydns	Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.
/flushdns	Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.
/registerdns	Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a failed DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

Parameter	Description
/release `[<adapter>]`	Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the *adapter* parameter is included. This parameter disables TCP/IP for adapters configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.
/release6`[<adapter>]`	Sends a DHCPRELEASE message to the DHCPv6 server to release the current DHCP configuration and discard the IPv6 address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the *adapter* parameter is included. This parameter disables TCP/IP for adapters configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.
/renew `[<adapter>]`	Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the *adapter* parameter is included. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.
/renew6 `[<adapter>]`	Renews DHCPv6 configuration for all adapters (if an adapter is not specified) or for a specific adapter if the *adapter* parameter is included. This parameter is available only on computers with adapters that are configured to obtain an IPv6 address automatically. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.
/setclassid `<adapter> [<classID>]`	Configures the DHCP class ID for a specified adapter. To set the DHCP class ID for all adapters, use the asterisk (*) wildcard character in place of *adapter*. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. If a DHCP class ID is not specified, the current class ID is removed.
/showclassid `<adapter>`	Displays the DHCP class ID for a specified adapter. To see the DHCP class ID for all adapters, use the asterisk (*) wildcard character in place of *adapter*. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically.
/?	Displays Help at the command prompt.

Remarks

- This command is most useful on computers that are configured to obtain an IP address automatically. This enables users to determine which TCP/IP configuration

values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.

- If the name you supply for *adapter* contains any spaces, use quotation marks around the adapter name (for example, "adapter name").
- For adapter names, **ipconfig** supports the use of the asterisk (*) wildcard character to specify either adapters with names that begin with a specified string or adapters with names that contain a specified string. For example, `Local*` matches all adapters that start with the string Local and `*Con*` matches all adapters that contain the string Con.

Examples

To display the basic TCP/IP configuration for all adapters, type:

```
ipconfig
```

To display the full TCP/IP configuration for all adapters, type:

```
ipconfig /all
```

To renew a DHCP-assigned IP address configuration for only the Local Area Connection adapter, type:

```
ipconfig /renew Local Area Connection
```

To flush the DNS resolver cache when troubleshooting DNS name resolution problems, type:

```
ipconfig /flushdns
```

To display the DHCP class ID for all adapters with names that start with Local, type:

```
```

```
ipconfig /showclassid Local*
```

To set the DHCP class ID for the Local Area Connection adapter to TEST, type:

```
ipconfig /setclassid Local Area Connection TEST
```

Related links

- Command-Line Syntax Key

ipxroute

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays and modifies information about the routing tables used by the IPX protocol. Used without parameters, **ipxroute** displays the default settings for packets that are sent to unknown, broadcast, and multicast addresses.

Syntax

```
ipxroute servers [/type=x]
ipxroute ripout <network>
ipxroute resolve {guid | name} {GUID | <adaptername>}
ipxroute board= N [def] [gbr] [mbr] [remove=xxxxxxxxxxxx]
ipxroute config
```

Parameters

Parameter	Description
servers `[/type=x]`	Displays the Service Access Point (SAP) table for the specified server type. **x** must be an integer. For example, `/type=4` displays all file servers. If you don't specify **/type**, `ipxroute servers` displays all types of servers, listing them by server name.
resolve `{GUID | name}` `{GUID | adaptername}`	Resolves the name of the GUID to its friendly name, or the friendly name to its GUID.
board= *n*	Specifies the network adapter for which to query or set parameters.
def	Sends packets to the ALL ROUTES broadcast. If a packet is transmitted to a unique Media Access Card (MAC) address that is not in the source routing table, **ipxroute** sends the packet to the SINGLE ROUTES broadcast by default.
gbr	Sends packets to the ALL ROUTES broadcast. If a packet is transmitted to the broadcast address (FFFFFFFFFFFF), **ipxroute** sends the packet to the SINGLE ROUTES broadcast by default.

Parameter	Description
mbr	Sends packets to the ALL ROUTES broadcast. If a packet is transmitted to a multicast address (C000xxxxxxxx), **ipxroute** sends the packet to the SINGLE ROUTES broadcast by default.
remove=*xxxxxxxxxxxx*	removes the given node address from the source routing table.
config	Displays information about all of the bindings for which IPX is configured.
/?	Displays help at the command prompt.

Examples

To display the network segments that the workstation is attached to, the workstation node address, and frame type being used, type:

```
ipxroute config
```

Related links

- Command-Line Syntax Key

irftp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sends files over an infrared link.

> **ⓘ Important**
>
> Make sure the devices intended to communicate over an infrared link have infrared functionality enabled and are working correctly. Also make sure an infrared link is established between the devices.

Syntax

```
irftp [<drive>:\] [[<path>] <filename>] [/h][/s]
```

Parameters

Parameter	Description
`<drive>:\`	Specifies the drive that contains the files that you want to send over an infrared link.
`[path] <filename>`	Specifies the location and name of the file or set of files that you want to send over an infrared link. If you specify a set of files, you must specify the full path for each file.
/h	Specifies hidden mode. When hidden mode is used, the files are sent without displaying the Wireless Link dialog box.
/s	Opens the **Wireless Link** dialog box, so that you can select the file or set of files that you want to send without using the command line to specify the drive, path, and file names. The **Wireless Link** dialog box also opens if you use this command without any parameters.

Examples

To send *c:\example.txt* over the infrared link, type:

```
irftp c:\example.txt
```

Related links

- Command-Line Syntax Key

jetpack

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Compacts a Windows Internet Name Service (WINS) or Dynamic Host Configuration Protocol (DHCP) database. We recommend you compact the WINS database whenever it approaches 30 MB.

Jetpack.exe compacts the database by:

1. Copying the database information to a temporary database file.
2. Deleting the original database file, either WINS or DHCP.
3. Renames the temporary database files to the original filename.

Syntax

```
jetpack.exe <database_name> <temp_database_name>
```

Parameters

Parameter	Description
`<database_name>`	Specifies the name of the original database file.
`<temp_database_name>`	Specifies the name of the temporary database file to be created by jetpack.exe. Note: This temporary file is removed when the compact process is complete. For this command to work properly, you must make sure your temp file name is unique and that a file with that name doesn't already exist.
/?	Displays help at the command prompt.

Examples

To compact the WINS database, where **Tmp.mdb** is a temporary database and **Wins.mdb** is the WINS database, type:

```
cd %SYSTEMROOT%\SYSTEM32\WINS
NET STOP WINS
jetpack Wins.mdb Tmp.mdb
NET start WINS
```

To compact the DHCP database, where **Tmp.mdb** is a temporary database and **Dhcp.mdb** is the DHCP database, type:

```
cd %SYSTEMROOT%\SYSTEM32\DHCP
NET STOP DHCPSERVER
jetpack Dhcp.mdb Tmp.mdb
NET start DHCPSERVER
```

Related links

- Command-Line Syntax Key

klist

Article • 02/03/2023

Displays a list of currently cached Kerberos tickets.

> **ⓘ Important**
>
> You must be at least a **Domain Admin**, or equivalent, to run all the parameters of this command.

Syntax

```
klist [-lh <logonID.highpart>] [-li <logonID.lowpart>] tickets | tgt | purge
| sessions | kcd_cache | get | add_bind | query_bind | purge_bind
```

Parameters

Parameter	Description
-lh	Denotes the high part of the user's locally unique identifier (LUID), expressed in hexadecimal. If neither **–lh** nor **–li** are present, the command defaults to the LUID of the user who is currently signed in.
-li	Denotes the low part of the user's locally unique identifier (LUID), expressed in hexadecimal. If neither **–lh** nor **–li** are present, the command defaults to the LUID of the user who is currently signed in.
tickets	Lists the currently cached ticket-granting-tickets (TGTs), and service tickets of the specified logon session. This is the default option.
tgt	Displays the initial Kerberos TGT.
purge	Allows you to delete all the tickets of the specified logon session.
sessions	Displays a list of logon sessions on this computer.
kcd_cache	Displays the Kerberos constrained delegation cache information.
get	Allows you to request a ticket to the target computer specified by the service principal name (SPN).
add_bind	Allows you to specify a preferred domain controller for Kerberos authentication.

Parameter	Description
query_bind	Displays a list of cached preferred domain controllers for each domain that Kerberos has contacted.
purge_bind	Removes the cached preferred domain controllers for the domains specified.
kdcoptions	Displays the Key Distribution Center (KDC) options specified in RFC 4120.
/?	Displays Help for this command.

Remarks

- If no parameters are provided, **klist** retrieves all the tickets for the currently logged on user.
- The parameters display the following information:
  - **tickets** - Lists the currently cached tickets of services that you have authenticated to since logon. Displays the following attributes of all cached tickets:
    - **LogonID:** The LUID.
    - **Client:** The concatenation of the client name and the domain name of the client.
    - **Server:** The concatenation of the service name and the domain name of the service.
    - **KerbTicket Encryption Type:** The encryption type that is used to encrypt the Kerberos ticket.
    - **Ticket Flags:** The Kerberos ticket flags.
    - **Start Time:** The time from which the ticket is valid.
    - **End Time:** The time the ticket becomes no longer valid. When a ticket is past this time, it can no longer be used to authenticate to a service or be used for renewal.
    - **Renew Time:** The time that a new initial authentication is required.
    - **Session Key Type:** The encryption algorithm that is used for the session key.
  - **tgt** - Lists the initial Kerberos TGT and the following attributes of the currently cached ticket:

    - **LogonID:** Identified in hexadecimal.
    - **ServiceName:** krbtgt
    - **TargetName `<SPN>`**: krbtgt
    - **DomainName:** Name of the domain that issues the TGT.
    - **TargetDomainName:** Domain that the TGT is issued to.
    - **AltTargetDomainName:** Domain that the TGT is issued to.
    - **Ticket Flags:** Address and target actions and type.
    - **Session Key:** Key length and encryption algorithm.
    - **StartTime:** Local computer time that the ticket was requested.
    - **EndTime:** Time the ticket becomes no longer valid. When a ticket is past this time, it can no longer be used to authenticate to a service.
    - **RenewUntil:** Deadline for ticket renewal.
    - **TimeSkew:** Time difference with the Key Distribution Center (KDC).
    - **EncodedTicket:** Encoded ticket.
- **purge** - Allows you to delete a specific ticket. Purging tickets destroys all tickets that you have cached, so use this attribute with caution. It might stop you from being able to authenticate to resources. If this happens, you'll have to log off and log on again.
    - **LogonID:** Identified in hexadecimal.
- **sessions** - Allows you to list and display the information for all logon sessions on this computer.
    - **LogonID:** If specified, displays the logon session only by the given value. If not specified, displays all the logon sessions on this computer.
- **kcd_cache** - Allows you to display the Kerberos constrained delegation cache information.
    - **LogonID:** If specified, displays the cache information for the logon session by the given value. If not specified, displays the cache information for the current user's logon session.
- **get** - Allows you to request a ticket to the target that is specified by the SPN.

    - **LogonID:** If specified, requests a ticket by using the logon session by the given value. If not specified, requests a ticket by using the current user's logon session.
    - **kdcoptions:** Requests a ticket with the given KDC options
- **add_bind** - Allows you to specify a preferred domain controller for Kerberos authentication.
- **query_bind** - Allows you to display cached, preferred domain controllers for the domains.
- **purge_bind** - Allows you to remove cached, preferred domain controllers for the domains.
- **kdcoptions** - For the current list of options and their explanations, see RFC 4120.

Examples

To query the Kerberos ticket cache to determine if any tickets are missing, if the target server or account is in error, or if the encryption type is not supported due to an Event ID 27 error, type:

```
klist
```

```
klist -li 0x3e7
```

To learn about the specifics of each ticket-granting-ticket that is cached on the computer for a logon session, type:

```
klist tgt
```

To purge the Kerberos ticket cache, log off, and then log back on, type:

```
klist purge
```

```
klist purge -li 0x3e7
```

To diagnose a logon session and to locate a logonID for a user or a service, type:

```
klist sessions
```

To diagnose Kerberos constrained delegation failure, and to find the last error that was encountered, type:

```
klist kcd_cache
```

To diagnose if a user or a service can get a ticket to a server, or to request a ticket for a specific SPN, type:

```
klist get host/%computername%
```

To diagnose replication issues across domain controllers, you typically need the client computer to target a specific domain controller. To target the client computer to the specific domain controller, type:

```
klist add_bind CONTOSO KDC.CONTOSO.COM
```

```
klist add_bind CONTOSO.COM KDC.CONTOSO.COM
```

To query which domain controllers were recently contacted by this computer, type:

```
klist query_bind
```

To rediscover domain controllers, or to flush the cache before creating new domain controller bindings with `klist add_bind`, type:

```
klist purge_bind
```

Related links

- Command-Line Syntax Key

ksetup

Article • 02/03/2023

Performs tasks related to setting up and maintaining Kerberos protocol and the Key Distribution Center (KDC) to support Kerberos realms. Specifically, this command is used to:

- Change the computer settings for locating Kerberos realms. In non-Microsoft, Kerberos–based implementations, this information is usually kept in the Krb5.conf file. In Windows Server operating systems, it's kept in the registry. You can use this tool to modify these settings. These settings are used by workstations to locate Kerberos realms and by domain controllers to locate Kerberos realms for cross-realm trust relationships.
- Initialize registry keys that the Kerberos Security Support Provider (SSP) uses to locate a KDC for the Kerberos realm, if the computer is isn't a member of a Windows domain. After configuration, the user of a client computer running the Windows operating system can log on to accounts in the Kerberos realm.
- Search the registry for the domain name of the user's realm and then resolves the name to an IP address by querying a DNS server. The Kerberos protocol can use DNS to locate KDCs by using only the realm name, but it must be specially configured to do so.

Syntax

```
ksetup
[/setrealm <DNSdomainname>]
[/mapuser <principal> <account>]
[/addkdc <realmname> <KDCname>]
[/delkdc <realmname> <KDCname>]
[/addkpasswd <realmname> <KDCPasswordName>]
[/delkpasswd <realmname> <KDCPasswordName>]
[/server <servername>]
[/setcomputerpassword <password>]
[/removerealm <realmname>]
[/domain <domainname>]
[/changepassword <oldpassword> <newpassword>]
[/listrealmflags]
[/setrealmflags <realmname> [sendaddress] [tcpsupported] [delegate]
[ncsupported] [rc4]]
[/addrealmflags <realmname> [sendaddress] [tcpsupported] [delegate]
[ncsupported] [rc4]]
```

```
[/delrealmflags [sendaddress] [tcpsupported] [delegate] [ncsupported] [rc4]]
[/dumpstate]
[/addhosttorealmmap] <hostname> <realmname>]
[/delhosttorealmmap] <hostname> <realmname>]
[/setenctypeattr] <domainname> {DES-CBC-CRC | DES-CBC-MD5 | RC4-HMAC-MD5 |
AES128-CTS-HMAC-SHA1-96 | AES256-CTS-HMAC-SHA1-96}
[/getenctypeattr] <domainname>
[/addenctypeattr] <domainname> {DES-CBC-CRC | DES-CBC-MD5 | RC4-HMAC-MD5 |
AES128-CTS-HMAC-SHA1-96 | AES256-CTS-HMAC-SHA1-96}
[/delenctypeattr] <domainname>
```

Parameters

Parameter	Description
ksetup setrealm	Makes this computer a member of a Kerberos realm.
ksetup addkdc	Defines a KDC entry for the given realm.
ksetup delkdc	Deletes a KDC entry for the realm.
ksetup addkpasswd	Adds a kpasswd server address for a realm.
ksetup delkpasswd	Deletes a kpasswd server address for a realm.
ksetup server	Allows you to specify the name of a Windows computer on which to apply the changes.
ksetup setcomputerpassword	Sets the password for the computer's domain account (or host principal).
ksetup removerealm	Deletes all information for the specified realm from the registry.
ksetup domain	Allows you to specify a domain (if the `<domainname>` hasn't already been set by the **/domain** parameter).
ksetup changepassword	Allows you to use the kpasswd to change the logged on user's password.
ksetup listrealmflags	Lists the available realm flags that **ksetup** can detect.
ksetup setrealmflags	Sets realm flags for a specific realm.
ksetup addrealmflags	Adds additional realm flags to a realm.
ksetup delrealmflags	Deletes realm flags from a realm.
ksetup dumpstate	Analyzes the Kerberos configuration on the given computer. Adds a host to realm mapping to the registry.

Parameter	Description
ksetup addhosttorealmmap	Adds a registry value to map the host to the Kerberos realm.
ksetup delhosttorealmmap	Deletes the registry value that mapped the host computer to the Kerberos realm.
ksetup setenctypeattr	Sets one or more encryption types trust attributes for the domain.
ksetup getenctypeattr	Gets the encryption types trust attribute for the domain.
ksetup addenctypeattr	Adds encryption types to the encryption types trust attribute for the domain.
ksetup delenctypeattr	Deletes the encryption types trust attribute for the domain.
/?	Displays Help at the command prompt.

Related links

- Command-Line Syntax Key

ksetup addenctypeattr

Article • 02/03/2023

Adds the encryption type attribute to the list of possible types for the domain. A status message is displayed upon successful or failed completion.

Syntax

```
ksetup /addenctypeattr <domainname> {DES-CBC-CRC | DES-CBC-MD5 | RC4-HMAC-MD5 | AES128-CTS-HMAC-SHA1-96 | AES256-CTS-HMAC-SHA1-96}
```

Parameters

Parameter	Description
`<domainname>`	Name of the domain to which you want to establish a connection. Use the fully qualified domain name or a simple form of the name, such as corp.contoso.com or contoso.
encryption type	Must be one of the following supported encryption types: • DES-CBC-CRC • DES-CBC-MD5 • RC4-HMAC-MD5 • AES128-CTS-HMAC-SHA1-96 • AES256-CTS-HMAC-SHA1-96

Remarks

- You can set or add multiple encryption types by separating the encryption types in the command with a space. However, you can only do so for one domain at a time.

Examples

To view the encryption type for the Kerberos ticket-granting ticket (TGT) and the session key, type:

```
klist
```

To set the domain to corp.contoso.com, type:

```
ksetup /domain corp.contoso.com
```

To add the encryption type *AES-256-CTS-HMAC-SHA1-96* to the list of possible types for the domain *corp.contoso.com*, type:

```
ksetup /addenctypeattr corp.contoso.com AES-256-CTS-HMAC-SHA1-96
```

To set the encryption type attribute to *AES-256-CTS-HMAC-SHA1-96* for the domain *corp.contoso.com*, type:

```
ksetup /setenctypeattr corp.contoso.com AES-256-CTS-HMAC-SHA1-96
```

To verify that the encryption type attribute was set as intended for the domain, type:

```
ksetup /getenctypeattr corp.contoso.com
```

Related links

- Command-Line Syntax Key
- klist command
- ksetup command
- ksetup domain command
- ksetup setenctypeattr command
- ksetup getenctypeattr command
- ksetup delenctypeattr command

ksetup addhosttorealmmap

Article • 08/31/2023

Adds a service principal name (SPN) mapping between the stated host and the realm. This command also allows you to map a host or multiple hosts that are sharing the same DNS suffix to the realm.

The mapping is stored in the registry, under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\HostToRealm**.

Syntax

```
ksetup /addhosttorealmmap <hostname> <realmname>
```

Parameters

Parameter	Description
`<hostname>`	The host name is the computer name, and it can be stated as the computer's fully qualified domain name.
`<realmname>`	The realm name is stated as an uppercase DNS name, such as CORP.CONTOSO.COM.

Examples

To map the host computer *IPops897* to the *CONTOSO* realm, type:

```
ksetup /addhosttorealmmap IPops897 CONTOSO
```

Check the registry to make sure the mapping occurred as intended.

Related links

- Command-Line Syntax Key

- ksetup command
- ksetup delhosttorealmmap command

ksetup addkdc

Article • 02/03/2023

Adds a Key Distribution Center (KDC) address for the given Kerberos realm

The mapping is stored in the registry, under **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\Kerberos\Domains** and the computer must be restarted before the new realm setting will be used.

> **Note**
>
> To deploy Kerberos realm configuration data to multiple computers, you must use the **Security Configuration Template** snap-in and policy distribution, explicitly on individual computers. You can't use this command.

Syntax

```
ksetup /addkdc <realmname> [<KDCname>]
```

Parameters

Parameter	Description
`<realmname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM. This value also appears as the default realm when **ksetup** is run, and is the realm to which you want to add the other KDC.
`<KDCname>`	Specifies the case-insensitive, fully-qualified domain name, such as mitkdc.contoso.com. If the KDC name is omitted, DNS will locate KDCs.

Examples

To configure a non-Windows KDC server and the realm that the workstation should use, type:

```
ksetup /addkdc CORP.CONTOSO.COM mitkdc.contoso.com
```

To set the local computer account password to p@sswrd1% on the same computer as in the previous example, and then to restart the computer, type:

```
ksetup /setcomputerpassword p@sswrd1%
```

To verify the default realm name for the computer or to verify that this command worked as intended, type:

```
ksetup
```

Check the registry to make sure the mapping occurred as intended.

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup setcomputerpassword command

ksetup addkpasswd

Article • 02/03/2023

Adds a Kerberos password (kpasswd) server address for a realm.

Syntax

```
ksetup /addkpasswd <realmname> [<kpasswdname>]
```

Parameters

Parameter	Description
`<realmname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM, and is listed as the default realm or **Realm=** when **ksetup** is run.
`<kpasswdname>`	Specifies the Kerberos password server. It's stated as a case-insensitive, fully-qualified domain name, such as mitkdc.contoso.com. If the KDC name is omitted, DNS might be used to locate KDCs.

Remarks

- If the Kerberos realm that the workstation will be authenticating to supports the Kerberos change password protocol, you can configure a client computer running the Windows operating system to use a Kerberos password server.
- You can add additional KDC names one at a time.

Examples

To configure the CORP.CONTOSO.COM realm to use the non-Windows KDC server, mitkdc.contoso.com, as the password server, type:

```
ksetup /addkpasswd CORP.CONTOSO.COM mitkdc.contoso.com
```

To verify the KDC name is set, type `ksetup` and then view the output, looking for the text, **kpasswd** =. If you don't see the text, it means the mapping hasn't been configured.

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup delkpasswd command

ksetup addrealmflags

Article • 05/03/2023

Applies to Windows Server (All supported versions)

The ksetup addrealmflags command adds other realm flags to a specified realm.

Syntax

```
ksetup /addrealmflags <realmname> [sendaddress] [tcpsupported] [delegate]
[ncsupported] [rc4]
```

Parameters

Parameter	Description
`<realmname>`	Specifies the uppercase DNS name, such as `CORP.CONTOSO.COM`.

Remarks

- Realm flags are stored in the registry under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Domains\<realmname>`. This entry doesn't exist in the registry by default. You can use the ksetup addrealmflags command to populate the registry.
- The realm flags specify other features of a Kerberos realm that aren't based on the Windows Server operating system. Computers running Windows Server can use a Kerberos server to administer authentication in the Kerberos realm instead of using a domain running a Windows Server operating system. This registry entry establishes the features of the realm and is as follows:

Value	Realm flag	Description
`0xF`	`All`	All realm flags are set.
`0x00`	`None`	No realm flags are set and no other features are enabled.
`0x01`	`sendaddress`	The IP address is included within the ticket-granting tickets.

Value	Realm flag	Description
`0x02`	`tcpsupported`	Both the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are supported in this realm.
`0x04`	`delegate`	Everyone in this realm is trusted for delegation.
`0x08`	`ncsupported`	This realm supports name canonicalization, which allows for DNS and Realm naming standards.
`0x80`	`rc4`	This realm supports RC4 encryption to enable cross-realm trust, which allows for the use of TLS.

- You can see the available and set realm flags by viewing the output of **ksetup** or `ksetup /dumpstate`.

Examples

To list the available realm flags for the realm CONTOSO, type:

```
ksetup /listrealmflags
```

To set two flags to the CONTOSO realm, type:

```
ksetup /setrealmflags CONTOSO ncsupported delegate
```

To add one more flag that isn't currently in the set, type:

```
ksetup /addrealmflags CONTOSO SendAddress
```

To verify the realm flag is set, type `ksetup` and then view the output, looking for the text, **Realm flags** =. If you don't see the text, it means that the flag hasn't been set.

Related links

- Command-Line Syntax Key
- ksetup command

- ksetup listrealmflags command
- ksetup setrealmflags command
- ksetup delrealmflags command
- ksetup dumpstate command

ksetup changepassword

Article • 02/03/2023

Uses the Key Distribution Center (KDC) password (kpasswd) value to change the password of the logged-on user. The output of the command informs you of the success or failure status.

You can check whether the **kpasswd** is set, by running the `ksetup /dumpstate` command and viewing the output.

Syntax

```
ksetup /changepassword <oldpassword> <newpassword>
```

Parameters

Parameter	Description
`<oldpassword>`	Specifies the logged-on user's existing password.
`<newpassword>`	Specifies the logged on user's new password. This password must meet all the password requirements set on this computer.

Remarks

- If the user account isn't found in the current domain, the system will ask you to supply the domain name where the user account resides.
- If you want to force a password change at next logon, this command allows the use of the asterisk (*) so the user will be prompted for a new password.
-

Examples

To change the password of a user who is currently logged on to this computer in this domain, type:

```
```

```
ksetup /changepassword Pas$w0rd Pa$$w0rd
```

To change the password of a user who is currently logged on in the Contoso domain, type:

```
ksetup /domain CONTOSO /changepassword Pas$w0rd Pa$$w0rd
```

To force the currently logged on user to change the password at the next logon, type:

```
ksetup /changepassword Pas$w0rd *
```

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup dumpstate command
- ksetup addkpasswd command
- ksetup delkpasswd command
- ksetup dumpstate command

ksetup delenctypeattr

Article • 02/03/2023

Removes the encryption type attribute for the domain. A status message is displayed upon successful or failed completion.

You can view the encryption type for the Kerberos ticket-granting ticket (TGT) and the session key, by running the **klist** command and viewing the output. You can set the domain to connect to and use, by running the `ksetup /domain <domainname>` command.

Syntax

```
ksetup /delenctypeattr <domainname>
```

Parameters

Parameter	Description
`<domainname>`	Name of the domain to which you want to establish a connection. You can use either the fully-qualified domain name or a simple form of the name, such as corp.contoso.com or contoso.

Examples

To determine the current encryption types that are set on this computer, type:

```
klist
```

To set the domain to mit.contoso.com, type:

```
ksetup /domain mit.contoso.com
```

To verify what the encryption type attribute is for the domain, type:

```
```

```
ksetup /getenctypeattr mit.contoso.com
```

To remove the set encryption type attribute for the domain mit.contoso.com, type:

```
ksetup /delenctypeattr mit.contoso.com
```

Related links

- Command-Line Syntax Key
- klist command
- ksetup command
- ksetup domain command
- ksetup addenctypeattr command
- ksetup setenctypeattr command

ksetup delhosttorealmmap

Article • 02/03/2023

Removes a service principal name (SPN) mapping between the stated host and the realm. This command also removes any mapping between a host to realm (or multiple hosts to realm).

The mapping is stored in the registry, under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentContolSet\Control\Lsa\Kerberos\HostToRealm`. After running this command, we recommend making sure the mapping appears in the registry.

Syntax

```
ksetup /delhosttorealmmap <hostname> <realmname>
```

Parameters

Parameter	Description
`<hostname>`	Specifies the fully-qualified domain name of the computer.
`<realmname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM.

Examples

To change the configuration of the realm CONTOSO, and to delete the mapping of the host computer IPops897 to the realm, type:

```
ksetup /delhosttorealmmap IPops897 CONTOSO
```

Related links

- Command-Line Syntax Key

- ksetup command
- ksetup addhosttorealmmap command

ksetup delkdc

Article • 02/03/2023

Deletes instances of Key Distribution Center (KDC) names for the Kerberos realm.

The mapping is stored in the registry, under `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\Kerberos\Domains`. After running this command, we recommend making sure the KDC was removed and no longer appears in the list.

> **Note**
>
> To remove realm configuration data from multiple computers, use the **Security Configuration Template** snap-in with policy distribution, instead of using the **ksetup** command explicitly on individual computers.

Syntax

```
ksetup /delkdc <realmname> <KDCname>
```

Parameters

Parameter	Description
`<realmname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM. This is the default realm that appears when you run the **ksetup** command, and it's the realm from which you want to delete the KDC.
`<KDCname>`	Specifies the case-sensitive, fully-qualified domain name, such as mitkdc.contoso.com.

Examples

To view all of the associations between the Windows realm and the non-Windows realm, and to determine which ones to remove, type:

```
ksetup
```

To remove the association, type:

```
ksetup /delkdc CORP.CONTOSO.COM mitkdc.contoso.com
```

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup addkdc command

ksetup delkpasswd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes a Kerberos password server (kpasswd) for a realm.

Syntax

```
ksetup /delkpasswd <realmname> <kpasswdname>
```

Parameters

Parameter	Description
`<realmname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM, and is listed as the default realm or **Realm=** when **ksetup** is run.
`<kpasswdname>`	Specifies the Kerberos password server. It's stated as a case-insensitive, fully-qualified domain name, such as mitkdc.contoso.com. If the KDC name is omitted, DNS might be used to locate KDCs.

Examples

To make sure the realm CORP.CONTOSO.COM uses the non-Windows KDC server mitkdc.contoso.com as the password server, type:

```
ksetup /delkpasswd CORP.CONTOSO.COM mitkdc.contoso.com
```

To make sure the realm CORP.CONTOSO.COM is not mapped to a Kerberos password server (the KDC name), type `ksetup` on the Windows computer and then view the output.

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup delkpasswd command

ksetup delrealmflags

Article • 02/03/2023

Removes realm flags from the specified realm.

Syntax

```
ksetup /delrealmflags <realmname> [sendaddress] [tcpsupported] [delegate]
[ncsupported] [rc4]
```

Parameters

Parameter	Description
`<realmname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM, and is listed as the default realm or **Realm=** when **ksetup** is run.

Remarks

- The realm flags specify additional features of a Kerberos realm that aren't based on the Windows Server operating system. Computers that are running Windows Server, can use a Kerberos server to administer authentication in the Kerberos realm, instead of using a domain running a Windows Server operating system. This entry establishes the features of the realm, and are as follows:

Value	Realm flag	Description
0xF	All	All realm flags are set.
0x00	None	No realm flags are set, and no additional features are enabled.
0x01	sendaddress	The IP address will be included within the ticket-granting tickets.
0x02	tcpsupported	Both the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are supported in this realm.
0x04	delegate	Everyone in this realm is trusted for delegation.
0x08	ncsupported	This realm supports name canonicalization, which allows for DNS and Realm naming standards.

Value	Realm flag	Description
0x80	rc4	This realm supports RC4 encryption to enable cross-realm trust, which allows for the use of TLS.

- Realm flags are stored in the registry under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Domains\<realmname>`. This entry doesn't exist in the registry by default. You can use the ksetup addrealmflags command to populate the registry.
- You can see the available and set realm flags by viewing the output of **ksetup** or `ksetup /dumpstate`.

Examples

To list the available realm flags for the realm CONTOSO, type:

```
ksetup /listrealmflags
```

To remove two flags currently in the set, type:

```
ksetup /delrealmflags CONTOSO ncsupported delegate
```

To verify the realm flags have been removed, type `ksetup` and then view the output, looking for the text, **Realm flags** =.

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup listrealmflags command
- ksetup setrealmflags command
- ksetup addrealmflags command
- ksetup dumpstate command

ksetup domain

Article • 02/03/2023

Sets the domain name for all Kerberos operations.

Syntax

```
ksetup /domain <domainname>
```

Parameters

Parameter	Description
`<domainname>`	Name of the domain to which you want to establish a connection. Use the fully-qualified domain name or a simple form of the name, such as contoso.com or contoso.

Examples

To establish a connection to a valid domain, such as Microsoft, by using the `ksetup /mapuser` subcommand, type:

```
ksetup /mapuser principal@realm domain-user /domain domain-name
```

After a successful connection, you'll receive a new TGT or an existing TGT will be refreshed.

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup mapuser command

ksetup dumpstate

Article • 02/03/2023

Displays the current state of realm settings for all realms that are defined on the computer. This command displays the same output as the **ksetup** command.

Syntax

```
ksetup /dumpstate
```

Remarks

- The output of this command includes the default realm (the domain that the computer is a member of) and all the realms that are defined on this computer. The following is included for each realm:
  - All the Key Distribution Centers (KDCs) that are associated with this realm.
  - All the **set realm** flags for this realm.
  - The KDC password.
- This command doesn't display the domain name specified by DNS detection or by the command `ksetup /domain`.
- This command doesn't display the computer password set by using the command `ksetup /setcomputerpassword`.

Examples

To locate the Kerberos realm configurations on a computer, type:

```
ksetup /dumpstate
```

Related links

- Command-Line Syntax Key
- ksetup command

ksetup getenctypeattr

Article • 02/03/2023

Retrieves the encryption type attribute for the domain. A status message is displayed upon successful or failed completion.

You can view the encryption type for the Kerberos ticket-granting ticket (TGT) and the session key, by running the **klist** command and viewing the output. You can set the domain to connect to and use, by running the `ksetup /domain <domainname>` command.

Syntax

```
ksetup /getenctypeattr <domainname>
```

Parameters

Parameter	Description
`<domainname>`	Name of the domain to which you want to establish a connection. Use the fully-qualified domain name or a simple form of the name, such as corp.contoso.com or contoso.

Examples

To verify the encryption type attribute for the domain, type:

```
ksetup /getenctypeattr mit.contoso.com
```

Related links

- Command-Line Syntax Key
- klist command
- ksetup command

- ksetup domain command
- ksetup addenctypeattr command
- ksetup setenctypeattr command
- ksetup delenctypeattr command

ksetup listrealmflags

Article • 02/03/2023

Lists the available realm flags that can be reported by **ksetup**.

Syntax

```
ksetup /listrealmflags
```

Remarks

- The realm flags specify additional features of a Kerberos realm that aren't based on the Windows Server operating system. Computers that are running Windows Server, can use a Kerberos server to administer authentication in the Kerberos realm, instead of using a domain running a Windows Server operating system. This entry establishes the features of the realm, and are as follows:

Value	Realm flag	Description
0xF	All	All realm flags are set.
0x00	None	No realm flags are set, and no additional features are enabled.
0x01	sendaddress	The IP address will be included within the ticket-granting tickets.
0x02	tcpsupported	Both the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are supported in this realm.
0x04	delegate	Everyone in this realm is trusted for delegation.
0x08	ncsupported	This realm supports name canonicalization, which allows for DNS and Realm naming standards.
0x80	rc4	This realm supports RC4 encryption to enable cross-realm trust, which allows for the use of TLS.

- Realm flags are stored in the registry under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Domains\<realmname>`. This entry doesn't exist in the registry by default. You can use the ksetup addrealmflags command to populate the registry.

Examples

To list the known realm flags on this computer, type:

```
ksetup /listrealmflags
```

To set the available realm flags that **ksetup** doesn't know, type:

```
ksetup /setrealmflags CORP.CONTOSO.COM sendaddress tcpsupported delete
ncsupported
```

-OR-

```
ksetup /setrealmflags CORP.CONTOSO.COM 0xF
```

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup addrealmflags command
- ksetup setrealmflags command
- ksetup delrealmflags command

ksetup mapuser

Article • 02/03/2023

Maps the name of a Kerberos principal to an account.

Syntax

```
ksetup /mapuser <principal> <account>
```

Parameters

Parameter	Description
`<principal>`	Specifies the fully-qualified domain name of any principal user. For example, mike@corp.CONTOSO.COM. If you don't specify an account parameter, mapping is deleted for the specified principal.
`<account>`	Specifies any account or security group name that exists on this computer, such as **Guest**, **Domain Users**, or **Administrator**. If this parameter is omitted, mapping is deleted for the specified principal.

Remarks

- An account can be specifically identified, such as **Domain Guests**, or you can use a wildcard character (*) to include all accounts.
- The computer only authenticates the principals of the given realm if they present valid Kerberos tickets.
- Whenever changes are made to the external Key Distribution Center (KDC) and the realm configuration, a restart of the computer where the setting was changed is required.

Examples

To see the current mapped settings and the default realm, type:

```
```

```
ksetup
```

To map Mike Danseglio's account within the Kerberos realm CONTOSO to the guest account on this computer, granting him all the privileges of a member of the built-in Guest account without having to authenticate to this computer, type:

```
ksetup /mapuser mike@corp.CONTOSO.COM guest
```

To remove the mapping of Mike Danseglio's account to the guest account on this computer to prevent him from authenticating to this computer with his credentials from CONTOSO, type:

```
ksetup /mapuser mike@corp.CONTOSO.COM
```

To map Mike Danseglio's account within the CONTOSO Kerberos realm to any existing account on this computer, type:

```
ksetup /mapuser mike@corp.CONTOSO.COM *
```

> **Note**
>
> If only the Standard User and Guest accounts are active on this computer, Mike's privileges are set to those.

To map all accounts within the CONTOSO Kerberos realm to any existing account of the same name on this computer, type:

```
ksetup /mapuser * *
```

Related links

- Command-Line Syntax Key

- ksetup command

ksetup removerealm

Article • 02/03/2023

Deletes all information for the specified realm from the registry.

The realm name is stored in the registry under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos` and `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\Kerberos`. This entry doesn't exist in the registry by default. You can use the ksetup addrealmflags command to populate the registry.

> **ⓘ Important**
>
> You can't remove the default realm name from the domain controller because this resets its DNS information, and removing it might make the domain controller unusable.

Syntax

```
ksetup /removerealm <realmname>
```

Parameters

Parameter	Description
`<realmname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM, and is listed as the default realm or **Realm=** when **ksetup** is run.

Examples

To remove an erroneous realm name (.CON instead of .COM) from the local computer, type:

```
ksetup /removerealm CORP.CONTOSO.CON
```

To verify the removal, you can run the **ksetup** command and review the output.

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup setrealm command

ksetup server

Article • 02/03/2023

Allows you to specify a name for a computer running the Windows operating system, so changes made by the **ksetup** command update the target computer.

The target server name is stored in the registry under `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\LSA\Kerberos`. This entry isn't reported when you run the **ksetup** command.

> **Important**
>
> There's no way to remove the targeted server name. Instead, you can change it back to the local computer name, which is the default.

Syntax

```
ksetup /server <servername>
```

Parameters

Parameter	Description
`<servername>`	Specifies the full computer name on which the configuration will be effective, such as *IPops897.corp.contoso.com*. If an incomplete fully-qualified domain computer name is specified, the command will fail.

Examples

To make your **ksetup** configurations effective on the *IPops897* computer, which is connected on the Contoso domain, type:

```
ksetup /server IPops897.corp.contoso.com
```

Related links

- Command-Line Syntax Key
- ksetup command

ksetup setcomputerpassword

Article • 02/03/2023

Sets the password for the local computer. This command affects the computer account only and requires a restart for the password change to take effect.

> **Important**
>
> The computer account password isn't displayed in the registry or as output from the **ksetup** command.

Syntax

```
ksetup /setcomputerpassword <password>
```

Parameters

Parameter	Description
`<password>`	Specifies the supplied password to set the computer account on the local computer. The password can only be set by using an account with administrative privileges, and the password must be from 1 to 156 alphanumeric or special characters.

Examples

To change the computer account password on the local computer from *IPops897* to *IPop$897!*, type:

```
ksetup /setcomputerpassword IPop$897!
```

Related links

- Command-Line Syntax Key

- ksetup command

ksetup setenctypeattr

Article • 02/03/2023

Sets the encryption type attribute for the domain. A status message is displayed upon successful or failed completion.

You can view the encryption type for the Kerberos ticket-granting ticket (TGT) and the session key, by running the **klist** command and viewing the output. You can set the domain to connect to and use, by running the `ksetup /domain <domainname>` command.

Syntax

```
ksetup /setenctypeattr <domainname> {DES-CBC-CRC | DES-CBC-MD5 | RC4-HMAC-MD5 | AES128-CTS-HMAC-SHA1-96 | AES256-CTS-HMAC-SHA1-96}
```

Parameters

Parameter	Description
`<domainname>`	Name of the domain to which you want to establish a connection. Use the fully qualified domain name or a simple form of the name, such as corp.contoso.com or contoso.
encryption type	Must be one of the following supported encryption types: • DES-CBC-CRC • DES-CBC-MD5 • RC4-HMAC-MD5 • AES128-CTS-HMAC-SHA1-96 • AES256-CTS-HMAC-SHA1-96

Remarks

- You can set or add multiple encryption types by separating the encryption types in the command with a space. However, you can only do so for one domain at a time.

Examples

To view the encryption type for the Kerberos ticket-granting ticket (TGT) and the session key, type:

```
klist
```

To set the domain to corp.contoso.com, type:

```
ksetup /domain corp.contoso.com
```

To set the encryption type attribute to AES-256-CTS-HMAC-SHA1-96 for the domain corp.contoso.com, type:

```
ksetup /setenctypeattr corp.contoso.com AES-256-CTS-HMAC-SHA1-96
```

To verify that the encryption type attribute was set as intended for the domain, type:

```
ksetup /getenctypeattr corp.contoso.com
```

Related links

- Command-Line Syntax Key
- klist command
- ksetup command
- ksetup domain command
- ksetup addenctypeattr command
- ksetup getenctypeattr command
- ksetup delenctypeattr command

ksetup setrealm

Article • 02/03/2023

Sets the name of a Kerberos realm.

> **ⓘ Important**
>
> Setting the Kerberos realm on a domain controller isn't supported. Attempting to do so causes a warning and a command failure.

Syntax

```
ksetup /setrealm <DNSdomainname>
```

Parameters

Parameter	Description
`<DNSdomainname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM. You can use the fully-qualified domain name or a simple form of the name. If you don't use uppercase for the DNS name, you'll be asked for verification to continue.

Examples

To set the realm of this computer to a specific domain name, and to restrict access by a non-domain controller just to the CONTOSO Kerberos realm, type:

```
ksetup /setrealm CONTOSO
```

Related links

- Command-Line Syntax Key
- ksetup command

- ksetup removerealm

ksetup setrealmflags

Article • 02/03/2023

Sets realm flags for the specified realm.

Syntax

```
ksetup /setrealmflags <realmname> [sendaddress] [tcpsupported] [delegate]
[ncsupported] [rc4]
```

Parameters

Parameter	Description
`<realmname>`	Specifies the uppercase DNS name, such as CORP.CONTOSO.COM.

Remarks

- The realm flags specify additional features of a Kerberos realm that aren't based on the Windows Server operating system. Computers that are running Windows Server, can use a Kerberos server to administer authentication in the Kerberos realm, instead of using a domain running a Windows Server operating system. This entry establishes the features of the realm, and are as follows:

Value	Realm flag	Description
0xF	All	All realm flags are set.
0x00	None	No realm flags are set, and no additional features are enabled.
0x01	sendaddress	The IP address will be included within the ticket-granting tickets.
0x02	tcpsupported	Both the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are supported in this realm.
0x04	delegate	Everyone in this realm is trusted for delegation.
0x08	ncsupported	This realm supports name canonicalization, which allows for DNS and Realm naming standards.

Value	Realm flag	Description
0x80	rc4	This realm supports RC4 encryption to enable cross-realm trust, which allows for the use of TLS.

- Realm flags are stored in the registry under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Domains\<realmname>`. This entry doesn't exist in the registry by default. You can use the ksetup addrealmflags command to populate the registry.
- You can see the available and set realm flags by viewing the output of **ksetup** or `ksetup /dumpstate`.

Examples

To list the available, and to set realm flags for the realm CONTOSO, type:

```
ksetup
```

To set two flags that aren't currently set, type:

```
ksetup /setrealmflags CONTOSO ncsupported delegate
```

To verify the realm flag is set, type `ksetup` and then view the output, looking for the text, **Realm flags** =. If you don't see the text, it means that the flag hasn't been set.

Related links

- Command-Line Syntax Key
- ksetup command
- ksetup listrealmflags command
- ksetup addrealmflags command
- ksetup delrealmflags command
- ksetup dumpstate command

ktmutil

Article • 02/03/2023

Starts the Kernel Transaction Manager utility. If used without parameters, **ktmutil** displays available subcommands.

Syntax

```
ktmutil list tms
ktmutil list transactions [{TmGUID}]
ktmutil resolve complete {TmGUID} {RmGUID} {EnGUID}
ktmutil resolve commit {TxGUID}
ktmutil resolve rollback {TxGUID}
ktmutil force commit {GUID}
ktmutil force rollback {GUID}
ktmutil forget
```

Examples

To force an Indoubt transaction with GUID 311a9209-03f4-11dc-918f-00188b8f707b to commit, type:

```
ktmutil force commit {311a9209-03f4-11dc-918f-00188b8f707b}
```

Related links

- Command-Line Syntax Key

ktpass

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configures the server principal name for the host or service in Active Directory Domain Services (AD DS) and generates a .keytab file that contains the shared secret key of the service. The .keytab file is based on the Massachusetts Institute of Technology (MIT) implementation of the Kerberos authentication protocol. The ktpass command-line tool allows non-Windows services that support Kerberos authentication to use the interoperability features provided by the Kerberos Key Distribution Center (KDC) service.

Syntax

```
ktpass
[/out <filename>]
[/princ <principalname>]
[/mapuser <useraccount>]
[/mapop {add|set}] [{-|+}desonly] [/in <filename>]
[/pass {password|*|{-|+}rndpass}]
[/minpass]
[/maxpass]
[/crypto {DES-CBC-CRC|DES-CBC-MD5|RC4-HMAC-NT|AES256-SHA1|AES128-SHA1|All}]
[/itercount]
[/ptype {KRB5_NT_PRINCIPAL|KRB5_NT_SRV_INST|KRB5_NT_SRV_HST}]
[/kvno <keyversionnum>]
[/answer {-|+}]
[/target]
[/rawsalt] [{-|+}dumpsalt] [{-|+}setupn] [{-|+}setpass <password>]  [/?
|/h|/help]
```

Parameters

Parameter	Description

Parameter	Description
/out `<filename>`	Specifies the name of the Kerberos version 5 .keytab file to generate. **Note:** This is the .keytab file you transfer to a computer that isn't running the Windows operating system, and then replace or merge with your existing .keytab file, */Etc/Krb5.keytab*.
/princ `<principalname>`	Specifies the principal name in the form host/computer.contoso.com@CONTOSO.COM. **Warning:** This parameter is case-sensitive.
/mapuser `<useraccount>`	Maps the name of the Kerberos principal, which is specified by the **princ** parameter, to the specified domain account.
/mapop `{add|set}`	Specifies how the mapping attribute is set. • **Add** - Adds the value of the specified local user name. This is the default. • **Set** - Sets the value for Data Encryption Standard (DES)-only encryption for the specified local user name.
`{-|+}`desonly	DES-only encryption is set by default. • + Sets an account for DES-only encryption. • - Releases restriction on an account for DES-only encryption. **Important:** Windows doesn't support DES by default.
/in `<filename>`	Specifies the .keytab file to read from a host computer that is not running the Windows operating system.
/pass `{password|*|{-|+}rndpass}`	Specifies a password for the principal user name that is specified by the **princ** parameter. Use `*` to prompt for a password.
/minpass	Sets the minimum length of the random password to 15 characters.
/maxpass	Sets the maximum length of the random password to 256 characters.

Parameter	Description
/crypto `{DES-CBC-CRC|DES-CBC-MD5|RC4-HMAC-NT|AES256-SHA1|AES128-SHA1|All}`	Specifies the keys that are generated in the keytab file: • **DES-CBC-CRC** - Used for compatibility. • **DES-CBC-MD5** - Adheres more closely to the MIT implementation and is used for compatibility. • **RC4-HMAC-NT** - Employs 128-bit encryption. • **AES256-SHA1** - Employs AES256-CTS-HMAC-SHA1-96 encryption. • **AES128-SHA1** - Employs AES128-CTS-HMAC-SHA1-96 encryption. • **All** - States that all supported cryptographic types can be used. **Note:** Because the default settings are based on older MIT versions, you should always use the `/crypto` parameter.
/itercount	Specifies the iteration count that is used for AES encryption. The default ignores **itercount** for non-AES encryption and sets AES encryption to 4,096.
/ptype `{KRB5_NT_PRINCIPAL|KRB5_NT_SRV_INST|KRB5_NT_SRV_HST}`	Specifies the principal type. • **KRB5_NT_PRINCIPAL** - The general principal type (recommended). • **KRB5_NT_SRV_INST** - The user service instance • **KRB5_NT_SRV_HST** - The host service instance
/kvno `<keyversionnum>`	Specifies the key version number. The default value is 1.
/answer `{-|+}`	Sets the background answer mode: • **-** Answers reset password prompts automatically with **NO**. • **+** Answers reset password prompts automatically with **YES**.

Parameter	Description
/target	Sets which domain controller to use. The default is for the domain controller to be detected, based on the principal name. If the domain controller name doesn't resolve, a dialog box will prompt for a valid domain controller.
/rawsalt	forces ktpass to use the rawsalt algorithm when generating the key. This parameter is optional.
`{-|+}dumpsalt`	The output of this parameter shows the MIT salt algorithm that is being used to generate the key.
`{-|+}setupn`	Sets the user principal name (UPN) in addition to the service principal name (SPN). The default is to set both in the .keytab file.
`{-|+}setpass <password>`	Sets the user's password when supplied. If rndpass is used, a random password is generated instead.
/?	Displays Help for this command.

Remarks

- Services running on systems that aren't running the Windows operating system can be configured with service instance accounts in AD DS. This allows any Kerberos client to authenticate to services that are not running the Windows operating system by using Windows KDCs.
- The **/princ** parameter isn't evaluated by ktpass and is used as provided. There's no check to see if the parameter matches the exact case of the **userPrincipalName** attribute value when generating the Keytab file. Case-sensitive Kerberos distributions using this Keytab file might have problems if there's no exact case match, and could even fail during pre-authentication. To check and retrieve the correct **userPrincipalName** attribute value from a LDifDE export file. For example:

```
ldifde /f keytab_user.ldf /d CN=Keytab
User,OU=UserAccounts,DC=contoso,DC=corp,DC=microsoft,DC=com /p base /l
samaccountname,userprincipalname
```

Examples

To create a Kerberos .keytab file for a host computer that isn't running the Windows operating system, you must map the principal to the account and set the host principal password.

1. Use the active directory **User and computers** snap-in to create a user account for a service on a computer that is not running the Windows operating system. For example, create an account with the name *User1*.

2. Use the **ktpass** command to set up an identity mapping for the user account by typing:

   ```
   ktpass /princ host/User1.contoso.com@CONTOSO.COM /mapuser User1 /pass
   MyPas$w0rd /out machine.keytab /crypto all /ptype KRB5_NT_PRINCIPAL
   /mapop set
   ```

   > **Note**
   >
   > You cannot map multiple service instances to the same user account.

3. Merge the .keytab file with the */Etc/Krb5.keytab* file on a host computer that isn't running the Windows operating system.

Related links

- Command-Line Syntax Key

label

Article • 02/03/2023

Creates, changes, or deletes the volume label (that is, the name) of a disk. If used without parameters, the **label** command changes the current volume label or deletes the existing label.

Syntax

```
label [/mp] [<volume>] [<label>]
```

Parameters

Parameter	Description
/mp	Specifies that the volume should be treated as a mount point or volume name.
`<volume>`	Specifies a drive letter (followed by a colon), mount point, or volume name. If a volume name is specified, the **/mp** parameter is unnecessary.
`<label>`	Specifies the label for the volume.
/?	Displays help at the command prompt.

Remarks

- Windows displays the volume label and serial number (if it has one) as part of the directory listing.
- An NTFS volume label can be up to 32 characters in length, including spaces. NTFS volume labels retain and display the case that was used when the label was created.

Examples

To label a disk in drive A that contains sales information for July, type:

```
label a:sales-july
```

To view and delete the current label for drive C, follow these steps:

1. At the command prompt, type:

   ```
   label
   ```

   Output similar to the following should be displayed:

   ```
   Volume in drive C: is Main Disk
   Volume Serial Number is 6789-ABCD
   Volume label (32 characters, ENTER for none)?
   ```

2. Press ENTER. The following prompt should be displayed:

   ```
   Delete current volume label (Y/N)?
   ```

3. Press **Y** to delete the current label, or **N** if you want to keep the existing label.

Related links

- Command-Line Syntax Key

lodctr

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Allows you to register or save performance counter name and registry settings in a file and designate trusted services.

Syntax

```
lodctr <filename> [/s:<filename>] [/r:<filename>] [/t:<servicename>]
```

Parameters

Parameter	Description
`<filename>`	Specifies the name of the initialization file that registers the performance counter name settings and explanatory text.
/s:`<filename>`	Specifies the name of the file to which the performance counter registry settings and explanatory text are saved.
/r	Restores counter registry settings and explanatory text from current registry settings and cached performance files related to the registry.
/r:`<filename>`	Specifies the name of the file that restores the performance counter registry settings and explanatory text. **Warning:** If you use this command, you'll overwrite all performance counter registry settings and explanatory text, replacing them with the configuration defined in the specified file.
/t:`<servicename>`	Indicates that service `<servicename>` is trusted.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces, use quotation marks around the text (for example, "file name 1").

Examples

To save the current performance registry settings and explanatory text to file "*perf backup1.txt*", type:

```
lodctr /s:"perf backup1.txt"
```

Related links

- Command-Line Syntax Key

logman

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates and manages Event Trace Session and Performance logs and supports many functions of Performance Monitor from the command line.

Syntax

```
logman [create | query | start | stop | delete| update | import | export |
/?] [options]
```

Parameters

Parameter	Description
logman create	Creates a counter, trace, configuration data collector, or API.
logman query	Queries data collector properties.
logman start | stop	Starts or stops data collection.
logman delete	Deletes an existing data collector.
logman update	Updates the properties of an existing data collector.
logman import | export	Imports a data collector set from an XML file or export a data collector set to an XML file.

Related links

- Command-Line Syntax Key

logman create

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates a counter, trace, configuration data collector, or API.

Syntax

```
logman create <counter | trace | alert | cfg | api> <[-n] <name>> [options]
```

Parameters

Parameter	Description
logman create counter	Creates a counter data collector.
logman create trace	Creates a trace data collector.
logman create alert	Creates an alert data collector.
logman create cfg	Creates a configuration data collector.
logman create api	Creates an API tracing data collector.

Related links

- Command-Line Syntax Key
- logman command

logman create alert

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates an alert data collector.

Syntax

```
logman create alert <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Perform the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering an `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changes to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Runs the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begins collecting data at the specified time.
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	Ends data collection at the specified time.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval for performance counter data collectors.
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.

Parameter	Description
-[-]r	Repeats the data collector daily at the specified begin and end times.
-[-]a	Appends an existing log file.
-[-]ow	Overwrites an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Runs the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, creates a new file when the specified time has elapsed. When time is not specified, creates a new file when the maximum size is exceeded.
-y	Answers yes to all questions without prompting.
-cf `<filename>`	Specifies the file listing performance counters to collect. The file should contain one performance counter name per line.
-[-]el	Enables or disables Event Log reporting.
-th `<threshold [threshold [...]]>`	Specify counters and their threshold values for an alert.
-[-]rdcs `<name>`	Specifies the Data Collector Set to start when an alert fires.
-[-]tn `<task>`	Specifies the task to run when an alert fires.
-[-]targ `<argument>`	Specifies the task arguments to be used with the task specified using -tn.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To create a new alert called, *new_alert*, which fires when the performance counter % Processor time in the Processor(_Total) counter group exceeds the counter value of 50, type:

```
```

```
logman create alert new_alert -th \Processor(_Total)\% Processor time>50
```

> **Note**
>
> The defined threshold value is based on the value collected by the counter, so in this example, the value of 50 equates to 50% Processor time.

Related links

- Command-Line Syntax Key
- logman update alert command
- logman command

logman create api

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates an API tracing data collector.

Syntax

```
logman create api <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Performs the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-f `<bin|bincirc>`	Specifies the log format for the data collector.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering a `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changed to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Run the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begin collecting data at the specified time.
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	End data collection at the specified time.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval for performance counter data collectors.

Parameter	Description
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.
-[-]r	Repeat the data collector daily at the specified begin and end times.
-[-]a	Append an existing log file.
-[-]ow	Overwrite an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Run the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, creates a new file when the specified time has elapsed. When time is not specified, creates a new file when the maximum size is exceeded.
-y	Answer yes to all questions without prompting.
-mods `<path [path [...]]>`	Specifies the list of modules to log API calls from.
-inapis `<module!api [module!api [...]]>`	Specifies the list of API calls to include in logging.
-exapis `<module!api [module!api [...]]>`	Specifies the list of API calls to exclude from logging.
-[-]ano	Log (-ano) API names only, or do not log only (-ano) API names.
-[-]recursive	Log (-recursive) or do not log (-recursive) APIs recursively beyond the first layer.
-exe `<value>`	Specifies the full path to an executable for API Tracing.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To create an API trace counter called trace_notepad, for the executable file c:\windows\notepad.exe, and putting the results in the file c:\notepad.etl, type:

```
logman create api trace_notepad -exe c:\windows\notepad.exe -o
c:\notepad.etl
```

To create an API trace counter called trace_notepad, for the executable file c:\windows\notepad.exe, collecting values produced by the module at c:\windows\system32\advapi32.dll, type:

```
logman create api trace_notepad -exe c:\windows\notepad.exe -mods
c:\windows\system32\advapi32.dll
```

To create an API trace counter called trace_notepad, for the executable file c:\windows\notepad.exe, excluding the API call TlsGetValue produced by the module kernel32.dll, type:

```
logman create api trace_notepad -exe c:\windows\notepad.exe -exapis
kernel32.dll!TlsGetValue
```

Related links

- Command-Line Syntax Key
- logman update api command
- logman command

logman create cfg

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates a configuration data collector.

Syntax

```
logman create cfg <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Performs the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering a * for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changes to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Runs the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begins collecting data at the specified time.
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	Ends data collection at the specified time.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval for performance counter data collectors.
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.

Parameter	Description
-[-]r	Repeats the data collector daily at the specified begin and end times.
-[-]a	Appends an existing log file.
-[-]ow	Overwrites an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Runs the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, creates a new file when the specified time has elapsed. When time is not specified, creates a new file when the maximum size is exceeded.
-y	Answers yes to all questions without prompting.
-[-]ni	Enables (-ni) or disable (-ni) network interface query.
-reg `<path [path [...]]>`	Specifies registry value(s) to collect.
-mgt `<query [query [...]]>`	Specifies WMI object(s) to collect using SQL query language.
-ftc `<path [path [...]]>`	Specifies the full path to the file(s) to collect.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To create a configuration data collector called cfg_log, using the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentverion\`, type:

```
logman create cfg cfg_log -reg HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\Currentverion\\
```

To create a configuration data collector called cfg_log, which records all WMI objects from `root\wmi` in the database column `MSNdis_Vendordriverversion`, type:

```
logman create cfg cfg_log -mgt root\wmi:select * FROM
MSNdis_Vendordriverversion
```

Related links

- Command-Line Syntax Key
- logman update cfg command
- logman command

logman create counter

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates a counter data collector.

Syntax

```
logman create counter <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Perform the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-f `<bin|bincirc|csv|tsv|sql>`	Specifies the log format for the data collector. The maximum log file size will be limited to 2 GB if `csv` is specified
-[-]u `<user [password]>`	Specifies the user to Run As. Entering an `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changes to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Runs the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begins collecting data at the specified time.
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	Ends data collection at the specified time.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval for performance counter data collectors.

Parameter	Description
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.
-[-]r	Repeats the data collector daily at the specified begin and end times.
-[-]a	Appends an existing log file.
-[-]ow	Overwrites an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Runs the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, create a new file when the specified time has elapsed. When time is not specified, create a new file when the maximum size is exceeded.
-y	Answers yes to all questions without prompting.
-cf `<filename>`	Specifies the file listing performance counters to collect. The file should contain one performance counter name per line.
-c `<path [path [ ]]>`	Specifies performance counter(s) to collect.
-sc `<value>`	Specifies the maximum number of samples to collect with a performance counter data collector.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To create a counter called *perf_log* using the % Processor time counter from the Processor(_Total) counter category, type:

```
logman create counter perf_log -c \Processor(_Total)\% Processor time
```

To create a counter called *perf_log* using the % Processor time counter from the Processor(_Total) counter category, creating a log file with a maximum size of 10 MB, and collecting data for 1 minute and 0 seconds, type:

```
logman create counter perf_log -c \Processor(_Total)\% Processor time -max
10 -rf 01:00
```

Related links

- Command-Line Syntax Key
- logman update counter command
- logman command

logman create trace

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Create an event trace data collector.

Syntax

```
logman create trace <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Performs the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
-ets	Sends commands to Event Trace Sessions directly without saving or scheduling.
[-n] `<name>`	Name of the target object.
-f `<bin|bincirc>`	Specifies the log format for the data collector.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering an `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changes to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Runs the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begins collecting data at the specified time.

Parameter	Description
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	Ends data collection at the specified time.
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.
-[-]r	Repeats the data collector daily at the specified begin and end times.
-[-]a	Appends an existing log file.
-[-]ow	Overwrites an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Runs the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, creates a new file when the specified time has elapsed. When time is not specified, creates a new file when the maximum size is exceeded.
-y	Answers yes to all questions without prompting.
-ct `<perf|system|cycle>`	Specifies the Event Trace Session clock type.
-ln `<logger_name>`	Specifies the logger name for Event Trace Sessions.
-ft `<[[hh:]mm:]ss>`	Specifies the Event Trace Session flush timer.
-[-]p `<provider [flags [level]]>`	Specifies a single Event Trace provider to enable.
-pf `<filename>`	Specifies a file listing multiple Event Trace providers to enable. The file should be a text file containing one provider per line.
-[-]rt	Runs the Event Trace Session in real-time mode.
-[-]ul	Runs the Event Trace Session in user.
-bs `<value>`	Specifies the Event Trace Session buffer size in kb.
-nb `<min max>`	Specifies the number of Event Trace Session buffers.

Parameter	Description
-mode `<globalsequence|localsequence|pagedmemory>`	Specifies the event trace session logger mode, including: • **Globalsequence** - Specifies that the event tracer add a sequence number to every event it receives irrespective of which trace session received the event. • **Localsequence** - Specifies that the event tracer add sequence numbers for events received at a specific trace session. When this option is used, duplicate sequence numbers can exist across all sessions but will be unique within each trace session. • **Pagedmemory** - Specifies that the event tracer use paged memory rather than the default non-paged memory pool for its internal buffer allocations.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To create an event trace data collector called *trace_log*, using no fewer than 16 and no more than 256 buffers, with each buffer being 64kb in size, putting the results in c:\logfile, type:

```
logman create trace trace_log -nb 16 256 -bs 64 -o c:\logfile
```

Related links

- Command-Line Syntax Key
- logman update trace command
- logman command

logman delete

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Deletes an existing data collector.

Syntax

```
logman delete <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Performs the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-ets	Sends commands to Event Trace Sessions directly without saving or scheduling.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering a * for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
/?	Displays context-sensitive help.

Examples

To delete the data collector *perf_log*, type:

```
logman delete perf_log
```

Related links

- Command-Line Syntax Key
- logman command

logman import and logman export

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Imports a Data Collector Set from an XML file, or exports a Data Collector Set to an XML file.

Syntax

```
logman import <[-n] <name> <-xml <name> [options]
logman export <[-n] <name> <-xml <name> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Perform the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-xml `<name>`	Name of the XML file to import or export.
-ets	Sends commands to Event Trace Sessions directly without saving or scheduling.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering an `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-y	Answers yes to all questions without prompting.
/?	Displays context-sensitive help.

Examples

To import the XML file *c:\windows\perf_log.xml* from the computer *server_1* as a data collector set called *perf_log*, type:

```
logman import perf_log -s server_1 -xml c:\windows\perf_log.xml
```

Related links

- Command-Line Syntax Key
- logman command

logman query

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Queries data collector or data collector set properties.

Syntax

```
logman query [providers|Data Collector Set name] [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Perform the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-ets	Sends commands to Event Trace Sessions directly without saving or scheduling.
/?	Displays context-sensitive help.

Examples

To list all Data Collector Sets configured on the target system, type:

```
logman query
```

To list the data collectors contained in the Data Collector Set named *perf_log*, type:

```
```

```
logman query perf_log
```

To list all available providers of data collectors on the target system, type:

```
logman query providers
```

Related links

- Command-Line Syntax Key
- logman command

logman start and logman stop

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

The **logman start** command starts a data collector and sets the begin time to manual. The **logman stop** command stops a Data Collector Set and sets the end time to manual.

Syntax

```
logman start <[-n] <name>> [options]
logman stop <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Perform the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Specifies the name of the target object.
-ets	Sends commands to Event Trace Sessions directly, without saving or scheduling.
-as	Performs the requested operation asynchronously.
-?	Displays context-sensitive help.

Examples

To start the data collector *perf_log*, on the remote computer *server_1*, type:

```
logman start perf_log -s server_1
```

Related links

- Command-Line Syntax Key
- logman command

logman update

Article • 02/03/2023

Updates an existing data collector.

Syntax

```
logman update <counter | trace | alert | cfg | api> <[-n] <name>> [options]
```

Parameters

Parameter	Description
logman update counter	Updates a counter data collector.
logman update alert	Updates an alert data collector.
logman update cfg	Updates a configuration data collector.
logman update api	Updates an API tracing data collector.

Related links

- Command-Line Syntax Key
- logman command

logman update alert

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Updates the properties of an existing alert data collector.

Syntax

```
logman update alert <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Perform the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering an `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changes to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Runs the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begins collecting data at the specified time.
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	Ends data collection at the specified time.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval for performance counter data collectors.
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.

Parameter	Description
-[-]r	Repeats the data collector daily at the specified begin and end times.
-[-]a	Appends an existing log file.
-[-]ow	Overwrites an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Runs the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, creates a new file when the specified time has elapsed. When time is not specified, creates a new file when the maximum size is exceeded.
-y	Answers yes to all questions without prompting.
-cf `<filename>`	Specifies the file listing performance counters to collect. The file should contain one performance counter name per line.
-[-]el	Enables or disables Event Log reporting.
-th `<threshold [threshold [...]]>`	Specify counters and their threshold values for an alert.
-[-]rdcs `<name>`	Specifies the Data Collector Set to start when an alert fires.
-[-]tn `<task>`	Specifies the task to run when an alert fires.
-[-]targ `<argument>`	Specifies the task arguments to be used with the task specified using -tn.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To update the existing alert called *new_alert*, setting the threshold value for the counter % Processor time in the Processor(_Total) counter group to 40%, type:

```
```

```
logman update alert new_alert -th \Processor(_Total)\% Processor time>40
```

Related links

- Command-Line Syntax Key
- logman create alert command
- logman command

logman update api

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Updates the properties of an existing API tracing data collector.

Syntax

```
logman update api <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Performs the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-f `<bin|bincirc>`	Specifies the log format for the data collector.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering a `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changed to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Run the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begin collecting data at the specified time.
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	End data collection at the specified time.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval for performance counter data collectors.

Parameter	Description
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.
-[-]r	Repeat the data collector daily at the specified begin and end times.
-[-]a	Append an existing log file.
-[-]ow	Overwrite an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Run the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, creates a new file when the specified time has elapsed. When time is not specified, creates a new file when the maximum size is exceeded.
-y	Answer yes to all questions without prompting.
-mods `<path [path [...]]>`	Specifies the list of modules to log API calls from.
-inapis `<module!api [module!api [...]]>`	Specifies the list of API calls to include in logging.
-exapis `<module!api [module!api [...]]>`	Specifies the list of API calls to exclude from logging.
-[-]ano	Log (-ano) API names only, or do not log only (-ano) API names.
-[-]recursive	Log (-recursive) or do not log (-recursive) APIs recursively beyond the first layer.
-exe `<value>`	Specifies the full path to an executable for API Tracing.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To update an existing API trace counter called *trace_notepad*, for the executable file c:\windows\notepad.exe, by excluding the API call TlsGetValue produced by the module kernel32.dll, type:

```
logman update api trace_notepad -exe c:\windows\notepad.exe -exapis
kernel32.dll!TlsGetValue
```

Related links

- Command-Line Syntax Key
- logman create api command
- logman command

logman update cfg

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Updates the properties of an existing configuration data collector.

Syntax

```
logman update cfg <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Performs the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering a * for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changes to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Runs the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begins collecting data at the specified time.
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	Ends data collection at the specified time.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval for performance counter data collectors.
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.

Parameter	Description
-[-]r	Repeats the data collector daily at the specified begin and end times.
-[-]a	Appends an existing log file.
-[-]ow	Overwrites an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Runs the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, creates a new file when the specified time has elapsed. When time is not specified, creates a new file when the maximum size is exceeded.
-y	Answers yes to all questions without prompting.
-[-]ni	Enables (-ni) or disable (-ni) network interface query.
-reg `<path [path [...]]>`	Specifies registry value(s) to collect.
-mgt `<query [query [...]]>`	Specifies WMI object(s) to collect using SQL query language.
-ftc `<path [path [...]]>`	Specifies the full path to the file(s) to collect.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To update a configuration data collector called *cfg_log*, to collect the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentverion\`, type:

```
logman update cfg cfg_log -reg HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\Currentverion\
```

Related links

- Command-Line Syntax Key
- logman create cfg command
- logman command

logman update counter

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Updates an existing counter data collector's properties.

Syntax

```
logman update counter <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Perform the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
[-n] `<name>`	Name of the target object.
-f `<bin|bincirc>`	Specifies the log format for the data collector.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering an `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changes to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Runs the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begins collecting data at the specified time.
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	Ends data collection at the specified time.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval for performance counter data collectors.

Parameter	Description
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.
-[-]r	Repeats the data collector daily at the specified begin and end times.
-[-]a	Appends an existing log file.
-[-]ow	Overwrites an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Runs the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, create a new file when the specified time has elapsed. When time is not specified, create a new file when the maximum size is exceeded.
-y	Answers yes to all questions without prompting.
-cf `<filename>`	Specifies the file listing performance counters to collect. The file should contain one performance counter name per line.
-c `<path [path [ ]]>`	Specifies performance counter(s) to collect.
-sc `<value>`	Specifies the maximum number of samples to collect with a performance counter data collector.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To create a counter called *perf_log* using the % Processor time counter from the Processor(_Total) counter category, type:

```
logman create counter perf_log -c \Processor(_Total)\% Processor time
```

To update an existing counter called *perf_log*, changing the sample interval to 10, the log format to CSV, and adding versioning to the log file name in the format mmddhhmm, type:

```
logman update counter perf_log -si 10 -f csv -v mmddhhmm
```

Related links

- Command-Line Syntax Key
- logman create counter command
- logman command

logman update trace

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Updates the properties of an existing event trace data collector.

Syntax

```
logman update trace <[-n] <name>> [options]
```

Parameters

Parameter	Description
-s `<computer name>`	Performs the command on the specified remote computer.
-config `<value>`	Specifies the settings file containing command options.
-ets	Sends commands to Event Trace Sessions directly without saving or scheduling.
[-n] `<name>`	Name of the target object.
-f `<bin|bincirc>`	Specifies the log format for the data collector.
-[-]u `<user [password]>`	Specifies the user to Run As. Entering an `*` for the password produces a prompt for the password. The password is not displayed when you type it at the password prompt.
-m `<[start] [stop] [[start] [stop] [...]]>`	Changes to manual start or stop instead of a scheduled begin or end time.
-rf `<[[hh:]mm:]ss>`	Runs the data collector for the specified period of time.
-b `<M/d/yyyy h:mm:ss[AM|PM]>`	Begins collecting data at the specified time.

Parameter	Description
-e `<M/d/yyyy h:mm:ss[AM|PM]>`	Ends data collection at the specified time.
-o `<path|dsn!log>`	Specifies the output log file or the DSN and log set name in a SQL database.
-[-]r	Repeats the data collector daily at the specified begin and end times.
-[-]a	Appends an existing log file.
-[-]ow	Overwrites an existing log file.
-[-]v `<nnnnnn|mmddhhmm>`	Attaches file versioning information to the end of the log file name.
-[-]rc `<task>`	Runs the command specified each time the log is closed.
-[-]max `<value>`	Maximum log file size in MB or maximum number of records for SQL logs.
-[-]cnf `<[[hh:]mm:]ss>`	When time is specified, creates a new file when the specified time has elapsed. When time is not specified, creates a new file when the maximum size is exceeded.
-y	Answers yes to all questions without prompting.
-ct `<perf|system|cycle>`	Specifies the Event Trace Session clock type.
-ln `<logger_name>`	Specifies the logger name for Event Trace Sessions.
-ft `<[[hh:]mm:]ss>`	Specifies the Event Trace Session flush timer.
-[-]p `<provider [flags [level]]>`	Specifies a single Event Trace provider to enable.
-pf `<filename>`	Specifies a file listing multiple Event Trace providers to enable. The file should be a text file containing one provider per line.
-[-]rt	Runs the Event Trace Session in real-time mode.
-[-]ul	Runs the Event Trace Session in user.
-bs `<value>`	Specifies the Event Trace Session buffer size in kb.
-nb `<min max>`	Specifies the number of Event Trace Session buffers.

Parameter	Description
-mode `<globalsequence|localsequence|pagedmemory>`	Specifies the event trace session logger mode, including: • **Globalsequence** - Specifies that the event tracer add a sequence number to every event it receives irrespective of which trace session received the event. • **Localsequence** - Specifies that the event tracer add sequence numbers for events received at a specific trace session. When this option is used, duplicate sequence numbers can exist across all sessions but will be unique within each trace session. • **Pagedmemory** - Specifies that the event tracer use paged memory rather than the default non-paged memory pool for its internal buffer allocations.
/?	Displays context-sensitive help.

Remarks

- Where [-] is listed, adding an extra hyphen (-) negates the option.

Examples

To update an existing event trace data collector called *trace_log*, changing the maximum log size to 10 MB, updating the log file format to CSV, and appending file versioning in the format mmddhhmm, type:

```
logman update trace trace_log -max 10 -f csv -v mmddhhmm
```

Related links

- Command-Line Syntax Key
- logman create trace command
- logman command

logoff

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Logs off a user from a session on a Remote Desktop Session Host server and deletes the session.

Syntax

```
logoff [<sessionname> | <sessionID>] [/server:<servername>] [/v]
```

Parameters

Parameter	Description
`<sessionname>`	Specifies the name of the session. This must be an active session.
`<sessionID>`	Specifies the numeric ID which identifies the session to the server.
/server:`<servername>`	Specifies the Remote Desktop Session Host server that contains the session whose user you want to log off. If unspecified, the server on which you are currently active is used.
/v	Displays information about the actions being performed.
/?	Displays help at the command prompt.

Remarks

- You can always log off yourself from the session to which you are currently logged on. You must, however, have **Full Control** permission to log off users from other sessions.
- Logging off a user from a session without warning can result in loss of data at the user's session. You should send a message to the user by using the **msg** command to warn the user before taking this action.

- If `<sessionID>` or `<sessionname>` isn't specified, **logoff** logs the user off from the current session.
- After you log off a user, all processes end and the session is deleted from the server.
- You can't log off a user from the console session.

Examples

To log off a user from the current session, type:

```
logoff
```

To log off a user from a session by using the session's ID, for example *session 12*, type:

```
logoff 12
```

To log off a user from a session by using the name of the session and server, for example session *TERM04* on *Server1*, type:

```
logoff TERM04 /server:Server1
```

Related links

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

lpq

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the status of a print queue on a computer running Line printer Daemon (LPD).

Syntax

```
lpq -S <servername> -P <printername> [-l]
```

Parameters

Parameter	Description
-S `<servername>`	Specifies (by name or IP address) the computer or printer sharing device that hosts the LPD print queue with a status that you want to display. This parameter is required and must be capitalized.
-P `<Printername>`	Specifies (by name) the printer for the print queue with a status that you want to display. This parameter is required and must be capitalized.
-l	Specifies that you want to display details about the status of the print queue.
/?	Displays help at the command prompt.

Examples

To display the status of the *Laserprinter1* printer queue on an LPD host at *10.0.0.45*, type:

```
lpq -S 10.0.0.45 -P Laserprinter1
```

Related links

- Command-Line Syntax Key

- Print Command Reference

lpr

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sends a file to a computer or printer sharing device running the Line printer Daemon (LPD) service in preparation for printing.

Syntax

```
lpr [-S <servername>] -P <printername> [-C <bannercontent>] [-J <jobname>]
[-o | -o l] [-x] [-d] <filename>
```

Parameters

Parameter	Description
-S `<servername>`	Specifies (by name or IP address) the computer or printer sharing device that hosts the LPD print queue with a status that you want to display. This parameter is required and must be capitalized.
-P `<printername>`	Specifies (by name) the printer for the print queue with a status that you want to display. To find the name of the printer, open the **Printers** folder. This parameter is required and must be capitalized.
-C `<bannercontent>`	Specifies the content to print on the banner page of the print job. If you don't include this parameter, the name of the computer from which the print job was sent appears on the banner page. This parameter must be capitalized.
-J `<jobname>`	Specifies the print job name that will be printed on the banner page. If you don't include this parameter, the name of the file being printed appears on the banner page. This parameter must be capitalized.
`[-o | -o l]`	Specifies the type of file that you want to print. The parameter **-o** specifies that you want to print a text file. The parameter **-o l** specifies that you want to print a binary file (for example, a PostScript file).
-d	Specifies that the data file must be sent before the control file. Use this parameter if your printer requires the data file to be sent first. For more information, see your printer documentation.

Parameter	Description
-x	Specifies that the **lpr** command must be compatible with the Sun Microsystems operating system (referred to as SunOS) for releases up to and including 4.1.4_u1.
`<filename>`	Specifies (by name) the file to be printed. This parameter is required.
/?	Displays help at the command prompt.

Examples

To print the *Document.txt* text file to the *Laserprinter1* printer queue on an LPD host at *10.0.0.45*, type:

```
lpr -S 10.0.0.45 -P Laserprinter1 -o Document.txt
```

To print the *PostScript_file.ps* Adobe PostScript file to the *Laserprinter1* printer queue on an LPD host at *10.0.0.45*, type:

```
lpr -S 10.0.0.45 -P Laserprinter1 -o l PostScript_file.ps
```

Related links

- Command-Line Syntax Key
- Print Command Reference

macfile

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Manages File Server for Macintosh servers, volumes, directories, and files. You can automate administrative tasks by including a series of commands in batch files and starting them manually or at predetermined times.

Modify directories in Macintosh-accessible volumes

To change the directory name, location, owner, group, and permissions for Macintosh-accessible volumes.

Syntax

```
macfile directory[/server:\\<computername>] /path:<directory> [/owner:
<ownername>] [/group:<groupname>] [/permissions:<permissions>]
```

Parameters

Parameter	Description
/server:`\\<computername>`	Specifies the server on which to change a directory. If omitted, the operation is performed on the local computer.
/path:`<directory>`	Specifies the path to the directory that you want to change. This parameter is required. **Note:** The directory must exist, using **macfile directory** won't create directories.
/owner:`<ownername>`	Changes the owner of the directory. If omitted, the owner name won't change.
/group:`<groupname>`	Specifies or changes the Macintosh primary group that is associated with the directory. If omitted, the primary group remains unchanged.

Parameter	Description
/permissions:`<permissions>`	Sets permissions on the directory for the owner, primary group, and world (everyone). This must be an 11-digit number, where the number 1 grants permission and 0 revokes permission (for example, 11111011000). If this parameter is omitted, permissions remain unchanged.
/?	Displays help at the command prompt.

Position of permissions digit

The position of the permissions digit determines which permission is set, including:

Position	Sets Permission
First	OwnerSeeFiles
Second	OwnerSeeFolders
Third	OwnerMakechanges
Fourth	GroupSeeFiles
Fifth	GroupSeeFolders
Sixth	GroupMakechanges
Seventh	WorldSeeFiles
Eighth	WorldSeeFolders
Ninth	WorldMakechanges
Tenth	The directory can't be renamed, moved, or deleted.
Eleventh	The changes apply to the current directory and all subdirectories.

Remarks

- If the information that you supply contains spaces or special characters, use quotation marks around the text (for example, "`<computer name>`").
- Use **macfile directory** to make an existing directory in a Macintosh-accessible volume available to Macintosh users. The **macfile directory** command doesn't create directories.

- Use File Manager, the command prompt, or the **macintosh new folder** command to create a directory in a Macintosh-accessible volume before you use the **macfile directory** command.

Examples

To assign *See Files*, *See Folders*, and *Make changes* permissions to the owner, to set *See Folder* permissions to all other users, and to prevent the directory from being renamed, moved, or deleted, type:

```
macfile directory /path:e:\statistics\may sales /permissions:11111011000
```

Where the subdirectory is *May sales*, located in the Macintosh-accessible volume *Statistics*, on the E:\ drive of the local server.

Join a Macintosh file's data and resource forks

To specify the server on which to join files, who created the file, the type of file, where the data fork is located, where the resource fork is located, and where the output file should be located.

Syntax

```
macfile forkize[/server:\\<computername>] [/creator:<creatorname>] [/type:
<typename>]  [/datafork:<filepath>] [/resourcefork:<filepath>] /targetfile:
<filepath>
```

Parameters

Parameter	Description
/server:`\\<computername>`	Specifies the server on which to join files. If omitted, the operation is performed on the local computer.
/creator:`<creatorname>`	Specifies the creator of the file. The Macintosh finder uses the **/creator** command-line option to determine the application that created the file.

Parameter	Description
/type:`<typename>`	Specifies the type of file. The Macintosh finder uses the **/type** command-line option to determine the file type within the application that created the file.
/datafork:`<filepath>`	Specifies the location of the data fork that is to be joined. You can specify a remote path.
/resourcefork:`<filepath>`	Specifies the location of the resource fork that is to be joined. You can specify a remote path.
/targetfile:`<filepath>`	Specifies the location of the file that's created by joining a data fork and a resource fork, or specifies the location of the file whose type or creator you are changing. The file must be on the specified server. This parameter is required.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces or special characters, use quotation marks around the text (for example, "`<computer name>`").

Examples

To create the file *tree_app* on the Macintosh-accessible volume *D:\Release*, using the resource fork *C:\Cross\Mac\Appcode*, and to make this new file appear to Macintosh clients as an application (Macintosh applications use the type *APPL*) with the creator (signature) set to *MAGNOLIA*, type:

```
macfile forkize /resourcefork:c:\cross\mac\appcode /type:APPL
/creator:MAGNOLIA /targetfile:D:\Release\tree_app
```

To change the file creator to *Microsoft Word 5.1*, for the file *Word.txt* in the directory *D:\Word documents\Group files*, on the server *\ServerA*, type:

```
macfile forkize /server:\\ServerA /creator:MSWD /type:TEXT
/targetfile:d:\Word documents\Group files\Word.txt
```

Change the sign-in message and limit sessions

To change the sign on message that appears when a user signs in to the File Server for Macintosh server and to limit the number of users who can simultaneously use File and print Servers for Macintosh.

Syntax

```
macfile server [/server:\\<computername>] [/maxsessions:{number | unlimited}] [/loginmessage:<message>]
```

Parameters

Parameter	Description
/server:`\\<computername>`	Specifies the server on which to change parameters. If omitted, the operation is performed on the local computer.
/maxsessions:`{number | unlimited}`	Specifies the maximum number of users who can simultaneously use File and print Servers for Macintosh. If omitted, the **maxsessions** setting for the server remains unchanged.
/loginmessage:`<message>`	Changes the message Macintosh users see when signing in to the File Server for Macintosh server. The maximum number of characters for the sign-in message is 199. If omitted, the **loginmessage** message for the server remains unchanged. To remove an existing sign-in message, include the **/loginmessage** parameter, but leave the *message* variable blank.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces or special characters, use quotation marks around the text (for example, "`<computer name>`").

Examples

To change the number of permitted File and print Server for Macintosh sessions on the local server to five sessions, and to add the sign-in message "Sign off from Server for Macintosh when you are finished", type:

```
macfile server /maxsessions:5 /loginmessage:Sign off from Server for
Macintosh when you are finished
```

Add, change, or remove Macintosh-accessible volumes

To add, change, or remove a Macintosh-accessible volume.

Syntax

```
macfile volume {/add|/set} [/server:\\<computername>] /name:
<volumename>/path:<directory>[/readonly:{true | false}] [/guestsallowed:
{true | false}] [/password:<password>] [/maxusers:{<number>>|unlimited}]
macfile volume /remove[/server:\\<computername>] /name:<volumename>
```

Parameters

Parameter	Description
`{/add | /set}`	Required when adding or changing a Macintosh-accessible volume. Adds or changes the specified volume.
/server:`\\ <computername>`	Specifies the server on which to add, change, or remove a volume. If omitted, the operation is performed on the local computer.
/name:`<volumename>`	Required. Specifies the volume name to be added, changed, or removed.
/path:`<directory>`	Required and valid only when you are adding a volume. Specifies the path to the root directory of the volume to be added.
/readonly:`{true | false}`	Specifies whether users can change files in the volume. Use **True** to specify that users can't change files in the volume. Use **False** to specify that users can change files in the volume. If omitted when adding a volume, changes to files are allowed. If omitted when changing a volume, the **readonly** setting for the volume remains unchanged.

Parameter	Description
/guestsallowed:`{true | false}`	Specifies whether users who log on as guests can use the volume. Use **True** to specify that guests can use the volume. Use **False** to specify that guests can't use the volume. If omitted when adding a volume, guests can use the volume. If omitted when changing a volume, the **guestsallowed** setting for the volume remains unchanged.
/password:`<password>`	Specifies a password that will be required to access the volume. If omitted when adding a volume, no password is created. If omitted when changing a volume, the password remains unchanged.
/maxusers:`{<number>> | unlimited}`	Specifies the maximum number of users who can simultaneously use the files on the volume. If omitted when adding a volume, an unlimited number of users can use the volume. If omitted when changing a volume, the **maxusers** value remains unchanged.
/remove	Required when you are removing a Macintosh-accessible volume. removes the specified volume.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces or special characters, use quotation marks around the text (for example, "`<computer name>`").

Examples

To create a volume called *US Marketing Statistics* on the local server, using the *Stats* directory in the E drive, and to specify that the volume cannot be accessed by guests, type:

```
macfile volume /add /name:US Marketing Statistics /guestsallowed:false
/path:e:\Stats
```

To change the volume created above to be read-only, to require a password, and to set the number of maximum users to five, type:

```
macfile volume /set /name:US Marketing Statistics /readonly:true
/password:saturn /maxusers:5
```

To add a volume called *Landscape Design*, on the server *Magnolia*, using the *trees* directory in the E drive, and to specify that the volume can be accessed by guests, type:

```
macfile volume /add /server:\\Magnolia /name:Landscape Design /path:e:\trees
```

To remove the volume called *Sales Reports* on the local server, type:

```
macfile volume /remove /name:Sales Reports
```

Related links

- Command-Line Syntax Key

makecab

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Package existing files into a cabinet (.cab) file.

> **Note**
>
> This command is the same as the **diantz command**.

Syntax

```
makecab [/v[n]] [/d var=<value> ...] [/l <dir>] <source> [<destination>]
makecab [/v[<n>]] [/d var=<value> ...] /f <directives_file> [...]
```

Parameters

Parameter	Description
`<source>`	File to compress.
`<destination>`	File name to give compressed file. If omitted, the last character of the source file name is replaced with an underscore (_) and used as the destination.
/f `<directives_file>`	A file with **makecab** directives (may be repeated).
/d var=`<value>`	Defines variable with specified value.
/l `<dir>`	Location to place destination (default is current directory).
/v[`<n>`]	Set debugging verbosity level (0=none,...,3=full).
/?	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- diantz command
- Microsoft Cabinet format

manage-bde

Article • 02/03/2023

Turns on or turns off BitLocker, specifies unlock mechanisms, updates recovery methods, and unlocks BitLocker-protected data drives.

> **Note**
>
> This command-line tool can be used in place of the **BitLocker Drive Encryption** Control Panel item.

Syntax

```
manage-bde [-status] [-on] [-off] [-pause] [-resume] [-lock] [-unlock] [-
autounlock] [-protectors] [-tpm]
[-setidentifier] [-forcerecovery] [-changepassword] [-changepin] [-
changekey] [-keypackage] [-upgrade] [-wipefreespace] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
manage-bde status	Provides information about all drives on the computer, whether or not they are BitLocker-protected.
manage-bde on	Encrypts the drive and turns on BitLocker.
manage-bde off	Decrypts the drive and turns off BitLocker. All key protectors are removed when decryption is complete.
manage-bde pause	Pauses encryption or decryption.
manage-bde resume	Resumes encryption or decryption.
manage-bde lock	Prevents access to BitLocker-protected data.
manage-bde unlock	Allows access to BitLocker-protected data with a recovery password or a recovery key.

Parameter	Description
manage-bde autounlock	Manages automatic unlocking of data drives.
manage-bde protectors	Manages protection methods for the encryption key.
manage-bde tpm	Configures the computer's Trusted Platform Module (TPM). This command isn't supported on computers running Windows 8 or **win8_server_2**. To manage the TPM on these computers, use either the TPM Management MMC snap-in or the TPM Management cmdlets for Windows PowerShell.
manage-bde setidentifier	Sets the drive identifier field on the drive to the value specified in the **Provide the unique identifiers for your organization** Group Policy setting.
manage-bde ForceRecovery	Forces a BitLocker-protected drive into recovery mode on restart. This command deletes all TPM-related key protectors from the drive. When the computer restarts, only a recovery password or recovery key can be used to unlock the drive.
manage-bde changepassword	Modifies the password for a data drive.
manage-bde changepin	Modifies the PIN for an operating system drive.
manage-bde changekey	Modifies the startup key for an operating system drive.
manage-bde KeyPackage	Generates a key package for a drive.
manage-bde upgrade	Upgrades the BitLocker version.
manage-bde WipeFreeSpace	Wipes the free space on a drive.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Related links

- Command-Line Syntax Key
- Enabling BitLocker by Using the Command Line

manage-bde status

Article • 02/03/2023

Provides information about all drives on the computer; whether or not they are BitLocker-protected, including:

- Size
- BitLocker version
- Conversion status
- Percentage encrypted
- Encryption method
- Protection status
- Lock status
- Identification field
- Key protectors

Syntax

```
manage-bde -status [<drive>] [-protectionaserrorlevel] [-computername
<name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-protectionaserrorlevel	Causes the manage-bde command-line tool to send the return code of **0** if the volume is protected and **1** if the volume is unprotected; most commonly used for batch scripts to determine if a drive is BitLocker-protected. You can also use **-p** as an abbreviated version of this command.

Parameter	Description
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To display the status of drive C, type:

```
manage-bde –status C:
```

Related links

- Command-Line Syntax Key
- manage-bde command

manage-bde on

Article • 02/03/2023

Encrypts the drive and turns on BitLocker.

Syntax

```
manage-bde –on <drive> {[-recoverypassword <numericalpassword>]|[-
recoverykey <pathtoexternaldirectory>]|[-startupkey
<pathtoexternalkeydirectory>]|[-certificate]|
[-tpmandpin]|[-tpmandpinandstartupkey <pathtoexternalkeydirectory>]|[-
tpmandstartupkey <pathtoexternalkeydirectory>]|[-password]|[-
ADaccountorgroup <domain\account>]}
[-usedspaceonly][-encryptionmethod
{aes128_diffuser|aes256_diffuser|aes128|aes256}] [-skiphardwaretest] [-
discoveryvolumetype <filesystemtype>] [-forceencryptiontype <type>] [-
removevolumeshadowcopies][-computername <name>]
[{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-recoverypassword	Adds a numerical password protector. You can also use **-rp** as an abbreviated version of this command.
`<numericalpassword>`	Represents the recovery password.
-recoverykey	Adds an external key protector for recovery. You can also use **-rk** as an abbreviated version of this command.
`<pathtoexternaldirectory>`	Represents the directory path to the recovery key.
-startupkey	Adds an external key protector for startup. You can also use **-sk** as an abbreviated version of this command.
`<pathtoexternalkeydirectory>`	Represents the directory path to the startup key.
-certificate	Adds a public key protector for a data drive. You can also use **-cert** as an abbreviated version of this command.

Parameter	Description
-tpmandpin	Adds a Trusted Platform Module (TPM) and personal identification number (PIN) protector for the operating system drive. You can also use **-tp** as an abbreviated version of this command.
-tpmandstartupkey	Adds a TPM and startup key protector for the operating system drive. You can also use **-tsk** as an abbreviated version of this command.
-tpmandpinandstartupkey	Adds a TPM, PIN, and startup key protector for the operating system drive. You can also use **-tpsk** as an abbreviated version of this command.
-password	Adds a password key protector for the data drive. You can also use **-pw** as an abbreviated version of this command.
-ADaccountorgroup	Adds a SID-based identity protector for the volume. The volume will automatically unlock if the user or computer has the proper credentials. When specifying a computer account, append a **$** to the computer name and specify **–service** to indicate that the unlock should happen in the content of the BitLocker server instead of the user. You can also use **-sid** as an abbreviated version of this command.
-usedspaceonly	Sets the encryption mode to Used Space Only encryption. The sections of the volume containing used space will be encrypted but the free space will not. If this option is not specified, all used space and free space on the volume will be encrypted. You can also use **-used** as an abbreviated version of this command.
-encryptionMethod	Configures the encryption algorithm and key size. You can also use **-em** as an abbreviated version of this command.
-skiphardwaretest	Begins encryption without a hardware test. You can also use **-s** as an abbreviated version of this command.
-discoveryvolumetype	Specifies the file system to use for the discovery data drive. The discovery data drive is a hidden drive added to a FAT-formatted, BitLocker-protected removable data drive that contains the BitLocker To Go Reader.
-forceencryptiontype	Forces BitLocker to use either software or hardware encryption. You can specify either **Hardware** or **Software** as the encryption type. If the **hardware** parameter is selected, but the drive doesn't support hardware encryption, manage-bde returns an error. If Group Policy settings forbids the specified encryption type, manage-bde returns an error. You can also use **-fet** as an abbreviated version of this command.

Parameter	Description
-removevolumeshadowcopies	Force deletion of Volume Shadow Copies for the volume. You won't be able to restore this volume using previous system restore points after running this command. You can also use **-rvsc** as an abbreviated version of this command.
`<filesystemtype>`	Specifies which file systems can be used with discovery data drives: FAT32, default, or none.
-computername	Specifies that manage-bde is being used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To turn on BitLocker for drive C, and to add a recovery password to the drive, type:

```
manage-bde –on C: -recoverypassword
```

To turn on BitLocker for drive C, add a recovery password to the drive, and to save a recovery key to drive E, type:

```
manage-bde –on C: -recoverykey E:\ -recoverypassword
```

To turn on BitLocker for drive C, using an external key protector (such as a USB key) to unlock the operating system drive, type:

```
manage-bde -on C: -startupkey E:\
```

ⓘ Important

This method is required if you are using BitLocker with computers that don't have a TPM.

To turn on BitLocker for data drive E, and to add a password key protector, type:

```
manage-bde –on E: -pw
```

To turn on BitLocker for operating system drive C, and to use hardware-based encryption, type:

```
manage-bde –on C: -fet hardware
```

Related links

- Command-Line Syntax Key
- manage-bde off command
- manage-bde pause command
- manage-bde resume command
- manage-bde command

manage-bde off

Article • 02/03/2023

Decrypts the drive and turns off BitLocker. All key protectors are removed when decryption is complete.

Syntax

```
manage-bde -off [<volume>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<volume>`	Specifies a drive letter followed by a colon, a volume GUID path, or a mounted volume.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To turn off BitLocker on drive C, type:

```
manage-bde –off C:
```

Related links

- Command-Line Syntax Key
- manage-bde on command
- manage-bde pause command
- manage-bde resume command
- manage-bde command

manage-bde -pause

Article • 02/03/2023

Pauses BitLocker encryption or decryption.

Syntax

```
manage-bde -pause [<volume>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<volume>`	Specifies a drive letter followed by a colon, a volume GUID path, or a mounted volume.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To pause BitLocker encryption on drive C, type:

Output

```
manage-bde -pause C:
```

Related links

- Command-Line Syntax Key

- manage-bde on command
- manage-bde off command
- manage-bde resume command
- manage-bde command

manage-bde resume

Article • 02/03/2023

Resumes BitLocker encryption or decryption after it has been paused.

Syntax

```
manage-bde -resume [<drive>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To resume BitLocker encryption on drive C, type:

```
manage-bde –resume C:
```

Related links

- Command-Line Syntax Key

- manage-bde on command
- manage-bde off command
- manage-bde pause command
- manage-bde command

manage-bde lock

Article • 02/03/2023

Locks a BitLocker-protected drive to prevent access to it unless the unlock key is provided.

Syntax

```
manage-bde -lock [<drive>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To lock data drive D, type:

```
manage-bde -lock D:
```

Related links

- Command-Line Syntax Key

- manage-bde command

manage-bde unlock

Article • 02/03/2023

Unlocks a BitLocker-protected drive by using a recovery password or a recovery key.

Syntax

```
manage-bde -unlock {-recoverypassword -password | -recoverykey
<pathtoexternalkeyfile>} <drive> [-certificate {-cf pathtocertificatefile |
-ct certificatethumbprint} {-pin}] [-password] [-computername <name>] [{-?
|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
-recoverypassword	Specifies that a recovery password will be used to unlock the drive. You can also use **-rp** as an abbreviated version of this command. This is the recovery key that's saved to a text file and must be written exactly as shown including dashes.
-password	Represents the recovery password that can be used to unlock the drive that either you or your administrator has set.
-recoverykey	Specifies that an external recovery key file will be used to unlock the drive. You can also use **-rk** as an abbreviated version of this command. This method searches for the **.bek** recovery key file that is saved to a USB drive.
`<pathtoexternalkeyfile>`	Represents the external recovery key file that can be used to unlock the drive.
`<drive>`	Represents a drive letter followed by a colon.
-certificate	The local user certificate for a BitLocker certificate to unlock the volume is located in the local user certificate store. You can also use **-cert** as an abbreviated version of this command.
-cf `<pathtocertificatefile>`	Path to the certificate file.
-ct `<certificatethumbprint>`	Certificate thumbprint which may optionally include the PIN (-pin).

Parameter	Description
-password	Presents a prompt for the password to unlock the volume. You can also use **-pw** as an abbreviated version of this command.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To unlock drive E with a password, type:

Windows Command Prompt

```
manage-bde -unlock E: -password
```

To unlock drive E with a recovery password, type:

Windows Command Prompt

```
manage-bde -unlock E: -recoverypassword xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx-
xxxxxx-xxxxxx-xxxxxx
```

To unlock drive E with a recovery key file that's been saved to a backup folder on another drive, type:

Windows Command Prompt

```
manage-bde -unlock E: -recoverykey F:\Backupkeys\recoverykey.bek
```

Related links

- Command-Line Syntax Key
- manage-bde command

manage-bde autounlock

Article • 02/03/2023

Manages the automatic unlocking of BitLocker-protected data drives.

Syntax

```
manage-bde -autounlock [{-enable|-disable|-clearallkeys}] <drive> [-
computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
-enable	Enables automatic unlocking for a data drive.
-disable	Disables automatic unlocking for a data drive.
-clearallkeys	Removes all stored external keys on the operating system drive.
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To enable automatic unlocking of data drive E, type:

```
manage-bde –autounlock -enable E:
```

Related links

- Command-Line Syntax Key
- manage-bde command

manage-bde protectors

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

Manages the protection methods used for the BitLocker encryption key.

Syntax

```
manage-bde -protectors [{-get|-add|-delete|-disable|-enable|-adbackup|-
aadbackup}] <drive> [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
-get	Displays all the key protection methods enabled on the drive and provides their type and identifier (ID).
-add	Adds key protection methods as specified by using additional **-add** parameters.
-delete	Deletes key protection methods used by BitLocker. All key protectors will be removed from a drive unless the optional **-delete** parameters are used to specify which protectors to delete. When the last protector on a drive is deleted, BitLocker protection of the drive is disabled to ensure that access to data is not lost inadvertently.
-disable	Disables protection, which will allow anyone to access encrypted data by making the encryption key available unsecured on drive. No key protectors are removed. Protection will be resumed the next time Windows is booted unless the optional **-disable** parameters are used to specify the reboot count.
-enable	Enables protection by removing the unsecured encryption key from the drive. All configured key protectors on the drive will be enforced.
-adbackup	Backs up recovery information for the drive specified to Active Directory Domain Services (AD DS). Append the **-id** parameter and specify the ID of a specific recovery key to back up. The **-id** parameter is required.
-aadbackup	Backs up all recovery information for the drive specified to Azure Active Directory (Azure AD). Append the **-id** parameter and specify the ID of a specific recovery key to back up. The **-id** parameter is required.

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief help at the command prompt.
-help or -h	Displays complete help at the command prompt.

Additional -add parameters

The -add parameter can also use these valid additional parameters.

```
manage-bde -protectors -add [<drive>] [-forceupgrade] [-recoverypassword
<numericalpassword>] [-recoverykey <pathtoexternalkeydirectory>]
[-startupkey <pathtoexternalkeydirectory>] [-certificate {-cf
<pathtocertificatefile>|-ct <certificatethumbprint>}] [-tpm] [-tpmandpin]
[-tpmandstartupkey <pathtoexternalkeydirectory>] [-tpmandpinandstartupkey
<pathtoexternalkeydirectory>] [-password][-adaccountorgroup
<securityidentifier> [-computername <name>]
[{-?|/?}] [{-help|-h}]
```

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-recoverypassword	Adds a numerical password protector. You can also use **-rp** as an abbreviated version of this command.
`<numericalpassword>`	Represents the recovery password.
-recoverykey	Adds an external key protector for recovery. You can also use **-rk** as an abbreviated version of this command.
`<pathtoexternalkeydirectory>`	Represents the directory path to the recovery key.
-startupkey	Adds an external key protector for startup. You can also use **-sk** as an abbreviated version of this command.
`<pathtoexternalkeydirectory>`	Represents the directory path to the startup key.

Parameter	Description
-certificate	Adds a public key protector for a data drive. You can also use **-cert** as an abbreviated version of this command.
-cf	Specifies that a certificate file will be used to provide the public key certificate.
`<pathtocertificatefile>`	Represents the directory path to the certificate file.
-ct	Specifies that a certificate thumbprint will be used to identify the public key certificate
`<certificatethumbprint>`	Specifies the value of the thumbprint property of the certificate you want to use. For example, a certificate thumbprint value of a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b should be specified as a909502dd82ae41433e6f83886b00d4277a32a7b.
-tpmandpin	Adds a Trusted Platform Module (TPM) and personal identification number (PIN) protector for the operating system drive. You can also use **-tp** as an abbreviated version of this command.
-tpmandstartupkey	Adds a TPM and startup key protector for the operating system drive. You can also use **-tsk** as an abbreviated version of this command.
-tpmandpinandstartupkey	Adds a TPM, PIN, and startup key protector for the operating system drive. You can also use **-tpsk** as an abbreviated version of this command.
-password	Adds a password key protector for the data drive. You can also use **-pw** as an abbreviated version of this command.
-adaccountorgroup	Adds a security identifier(SID)-based identity protector for the volume. You can also use **-sid** as an abbreviated version of this command. **IMPORTANT:** By default, you can't add an ADaccountorgroup protector remotely using either WMI or manage-bde. If your deployment requires the ability to add this protector remotely, you must enable constrained delegation.
-computername	Specifies that manage-bde is being used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief help at the command prompt.

Parameter	Description
-help or -h	Displays complete help at the command prompt.

Additional -delete parameters

```
manage-bde -protectors -delete <drive> [-type
{recoverypassword|externalkey|certificate|tpm|tpmandstartupkey|tpmandpin|tpm
andpinandstartupkey|Password|Identity}]
[-id <keyprotectorID>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-type	Identifies the key protector to delete. You can also use **-t** as an abbreviated version of this command.
recoverypassword	Specifies that any recovery password key protectors should be deleted.
externalkey	Specifies that any external key protectors associated with the drive should be deleted.
certificate	Specifies that any certificate key protectors associated with the drive should be deleted.
tpm	Specifies that any TPM-only key protectors associated with the drive should be deleted.
tpmandstartupkey	Specifies that any TPM and startup key based key protectors associated with the drive should be deleted.
tpmandpin	Specifies that any TPM and PIN based key protectors associated with the drive should be deleted.
tpmandpinandstartupkey	Specifies that any TPM, PIN, and startup key based key protectors associated with the drive should be deleted.
password	Specifies that any password key protectors associated with the drive should be deleted.
identity	Specifies that any identity key protectors associated with the drive should be deleted.
-ID	Identifies the key protector to delete by using the key identifier. This parameter is an alternative option to the **-type** parameter.

Parameter	Description
`<keyprotectorID>`	Identifies an individual key protector on the drive to delete. Key protector IDs can be displayed by using the **manage-bde -protectors -get** command.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief help at the command prompt.
-help or -h	Displays complete help at the command prompt.

Additional -disable parameters

```
manage-bde -protectors -disable <drive> [-rebootcount <integer 0 - 15>] [-
computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
rebootcount	Specifies that protection of the operating system volume has been suspended and will resume after Windows has been restarted the number of times specified in the **rebootcount** parameter. Specify **0** to suspend protection indefinitely. If this parameter isn't specified, BitLocker protection automatically resumes after Windows is restarted. You can also use **-rc** as an abbreviated version of this command.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief help at the command prompt.
-help or -h	Displays complete help at the command prompt.

Examples

To add a certificate key protector, identified by a certificate file, to drive E, type:

```
manage-bde -protectors -add E: -certificate -cf c:\File Folder\Filename.cer
```

To add an **adaccountorgroup** key protector, identified by domain and user name, to drive E, type:

```
manage-bde -protectors -add E: -sid DOMAIN\user
```

To disable protection until the computer has rebooted 3 times, type:

```
manage-bde -protectors -disable C: -rc 3
```

To delete all TPM and startup keys-based key protectors on drive C, type:

```
manage-bde -protectors -delete C: -type tpmandstartupkey
```

To list all key protectors for drive C, type:

```
manage-bde -protectors -get C:
```

To back up all recovery information for drive C to AD DS, type (where `-id` is the ID of the specific key protector to back up):

```
manage-bde -protectors -adbackup C: -id '{00000000-0000-0000-0000-
000000000000}'
```

Related links

- Command-Line Syntax Key
- manage-bde command

manage-bde tpm

Article • 08/30/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configures the computer's Trusted Platform Module (TPM).

Syntax

```
manage-bde -tpm [-turnon] [-takeownership <ownerpassword>] [-computername
<name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
-turnon	Enables and activates the TPM, allowing the TPM owner password to be set. You can also use **-t** as an abbreviated version of this command.
-takeownership	Takes ownership of the TPM by setting an owner password. You can also use **-o** as an abbreviated version of this command.
`<ownerpassword>`	Represents the owner password that you specify for the TPM.
-computername	Specifies that manage-bde.exe is used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To turn on the TPM, type:

```
manage-bde -tpm -turnon
```

To take ownership of the TPM and set the owner password to *0wnerP@ss*, type:

```
manage-bde -tpm -takeownership 0wnerP@ss
```

Related links

- Command-Line Syntax Key
- TPM Management cmdlets for Windows PowerShell
- manage-bde command

manage-bde setidentifier

Article • 02/03/2023

Sets the drive identifier field on the drive to the value specified in the **Provide the unique identifiers for your organization** Group Policy setting.

Syntax

```
manage-bde –setidentifier <drive> [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To set BitLocker drive identifier field for C, type:

```
manage-bde –setidentifier C:
```

Related links

- Command-Line Syntax Key
- manage-bde command
- BitLocker Recovery Guide

manage-bde forcerecovery

Article • 02/03/2023

Forces a BitLocker-protected drive into recovery mode on restart. This command deletes all Trusted Platform Module (TPM)-related key protectors from the drive. When the computer restarts, only a recovery password or recovery key can be used to unlock the drive.

Syntax

```
manage-bde –forcerecovery <drive> [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To cause BitLocker to start in recovery mode on drive C, type:

```
manage-bde –forcerecovery C:
```

Related links

- Command-Line Syntax Key
- manage-bde command

manage-bde changepassword

Article • 02/03/2023

Modifies the password for a data drive. The user is prompted for a new password.

Syntax

```
manage-bde -changepassword [<drive>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To change the password used to unlock BitLocker on data drive D, type:

```
manage-bde –changepassword D:
```

Related links

- Command-Line Syntax Key

- manage-bde command

manage-bde changepin

Article • 02/03/2023

Modifies the PIN for an operating system drive. The user is prompted to enter a new PIN.

Syntax

```
manage-bde -changepin [<drive>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To change the PIN used with BitLocker on drive C, type:

```
manage-bde –changepin C:
```

Related links

- Command-Line Syntax Key
- manage-bde command

manage-bde changekey

Article • 02/03/2023

Modifies the startup key for an operating system drive.

Syntax

```
manage-bde -changekey [<drive>] [<pathtoexternalkeydirectory>] [-
computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To create a new startup key on drive E, to use with BitLocker encryption on drive C, type:

```
manage-bde -changekey C: E:\
```

Related links

- Command-Line Syntax Key

- manage-bde command

manage-bde keypackage

Article • 02/03/2023

Generates a key package for a drive. The key package can be used in conjunction with the repair tool to repair corrupted drives.

Syntax

```
manage-bde -keypackage [<drive>] [-ID <keyprotectoryID>] [-path
<pathtoexternalkeydirectory>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-ID	Creates a key package using the key protector with the identifier specified by this ID value. **Tip:** Use the **manage-bde –protectors –get** command, along with the drive letter that you want to create a key package for, to get a list of available GUIDs to use as the ID value.
-path	Specifies the location to save the created key package.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To create a key package for drive C, based on the key protector identified by the GUID, and to save the key package to F:\Folder, type:

```
manage-bde -keypackage C: -id {84E151C1...7A62067A512} -path f:\Folder
```

Related links

- Command-Line Syntax Key
- manage-bde command

manage-bde upgrade

Article • 02/03/2023

Upgrades the BitLocker version.

Syntax

```
manage-bde -upgrade [<drive>] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To upgrade BitLocker encryption on drive C, type:

```
manage-bde –upgrade C:
```

Related links

- Command-Line Syntax Key

- manage-bde command

manage-bde wipefreespace

Article • 02/03/2023

Wipes the free space on the volume, removing any data fragments that may have existed in the space. Running this command on a volume encrypted using the **Used Space Only** encryption method provides the same level of protection as the **Full Volume Encryption** encryption method.

Syntax

```
manage-bde -wipefreespace|-w [<drive>] [-cancel] [-computername <name>] [{-?|/?}] [{-help|-h}]
```

Parameters

Parameter	Description
`<drive>`	Represents a drive letter followed by a colon.
-cancel	Cancels a wipe of free space that is in process.
-computername	Specifies that manage-bde.exe will be used to modify BitLocker protection on a different computer. You can also use **-cn** as an abbreviated version of this command.
`<name>`	Represents the name of the computer on which to modify BitLocker protection. Accepted values include the computer's NetBIOS name and the computer's IP address.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Examples

To wipe the free space on drive C, type either:

```
manage-bde -w C:
```

```
manage-bde -wipefreespace C:
```

To cancel the wipe of tje free space on drive C, type either:

```
manage-bde -w -cancel C:
```

```
manage-bde -wipefreespace -cancel C:
```

Related links

- Command-Line Syntax Key
- manage-bde command

mapadmin

Article • 02/03/2023

The **mapadmin** command-line utility administers User Name Mapping on the local or remote computer running Microsoft Services for Network File System. If you are logged on with an account that does not have administrative credentials, you can specify a user name and password of an account that does.

Syntax

```
mapadmin [<computer>] [-u <user> [-p <password>]]
mapadmin [<computer>] [-u <user> [-p <password>]] {start | stop}
mapadmin [<computer>] [-u <user> [-p <password>]] config <option[...]>
mapadmin [<computer>] [-u <user> [-p <password>]] add -wu <windowsuser> -uu
<UNIXuser> [-setprimary]
mapadmin [<computer>] [-u <user> [-p <password>]] add -wg <windowsgroup> -ug
<UNIXgroup> [-setprimary]
mapadmin [<computer>] [-u <user> [-p <password>]] setprimary -wu
<Windowsuser> [-uu <UNIXuser>]
mapadmin [<computer>] [-u <user> [-p <password>]] setprimary -wg
<Windowsgroup> [-ug <UNIXgroup>]
mapadmin [<computer>] [-u <user> [-p <password>]] delete <option[...]>
mapadmin [<computer>] [-u <user> [-p <password>]] list <option[...]>
mapadmin [<computer>] [-u <user> [-p <password>]] backup <filename>
mapadmin [<computer>] [-u <user> [-p <password>]] restore <filename>
mapadmin [<computer>] [-u <user> [-p <password>]] adddomainmap -d
<Windowsdomain> {-y <<NISdomain>> | -f <path>}
mapadmin [<computer>] [-u <user> [-p <password>]] removedomainmap -d
<Windowsdomain> -y <<NISdomain>>
mapadmin [<computer>] [-u <user> [-p <password>]] removedomainmap -all
mapadmin [<computer>] [-u <user> [-p <password>]] listdomainmaps
```

Parameters

Parameter	Description
`<computer>`	Specifies the remote computer running the User Name Mapping service that you want to administer. You can specify the computer using a Windows Internet Name Service (WINS) name or a Domain Name System (DNS) name, or by Internet Protocol (IP) address.

Parameter	Description
-u `<user>`	Specifies the user name of the user whose credentials are to be used. It might be necessary to add the domain name to the user name in the form *domain**username*.
-p `<password>`	Specifies the password of the user. If you specify the **-u** option but omit the **-p** option, you are prompted for the user's password.
`start | stop`	Starts or stops the User Name Mapping service.
config	Specifies general settings for User Name Mapping. The following options are available with this parameter: • **-r** `<dddd>:<hh>:<mm>`: Specifies the refresh interval for updating from the Windows and NIS databases in days, hours, and minutes. The minimum interval is 5 minutes. • **-i** `{yes | no}`: Turns simple mapping on (**yes**) or off (**no**). By default, mapping is turned on.
add	Creates a new mapping for a user or group. The following options are available with this parameter: • **-wu** `<name>`: Specifies the name of the Windows user for which a new mapping is being created. • **-uu** `<name>`: Specifies the name of the UNIX user for which a new mapping is being created. • **-wg** `<group>`: Specifies the name of the Windows group for which a new mapping is being created. • **-ug** `<group>`: Specifies the name of the UNIX group for which a new mapping is being created. • **-setprimary:** Specifies that the new mapping is the primary mapping.
setprimary	Specifies which mapping is the primary mapping for a UNIX user or group with multiple mappings. The following options are available with this parameter: • **-wu** `<name>`: Specifies the Windows user of the primary mapping. If more than one mapping for the user exists, use the **-uu** option to specify the primary mapping. • **-uu** `<name>`: Specifies the UNIX user of the primary mapping. • **-wg** `<group>`: Specifies the Windows group of the primary mapping. If more than one mapping for the group exists, use the **-ug** option to specify the primary mapping. • **-ug** `<group>`: Specifies the UNIX group of the primary mapping.

Parameter	Description
delete	Removes the mapping for a user or group. The following options are available for this parameter: • **-wu** `<user>`: Specifies the Windows user for which the mapping will be deleted, specified as `<windowsdomain>\<username>`. You must specify either the **-wu** or the **-uu** option, or both. If you specify both options, the particular mapping identified by the two options will be deleted. If you specify only the **-wu** option, all mappings for the specified user will be deleted. • **-uu** `<user>`: Specifies the UNIX user for whom the mapping will be deleted, specified as `<username>`. You must specify either the **-wu** or the **-uu** option, or both. If you specify both options, the particular mapping identified by the two options will be deleted. If you specify only the **-uu** option, all mappings for the specified user will be deleted. • **-wg** `<group>`: Specifies the Windows group for which the mapping will be deleted, specified as `<windowsdomain>\<username>`. You must specify either the **-wg** or the **-ug** option, or both. If you specify both options, the particular mapping identified by the two options will be deleted. If you specify only the **-wg** option, all mappings for the specified group will be deleted. • **-ug** `<group>`: Specifies the UNIX group for which the mapping will be deleted, specified as `<groupname>`. You must specify either the **-wg** or the **-ug** option, or both. If you specify both options, the particular mapping identified by the two options will be deleted. If you specify only the **-ug** option, all mappings for the specified group will be deleted.
list	Displays information about user and group mappings. The following options are available with this parameter: • **-all:** Lists both simple and advanced mappings for users and groups. • **-simple:** Lists all simple mapped users and groups. • **-advanced:** Lists all advanced mapped users and groups. Maps are listed in the order in which they are evaluated. Primary maps, marked with an asterisk (*), are listed first, followed by secondary maps, which are marked with a carat `(^)`. • **-wu** `<name>`: Lists the mapping for a specified Windows user. • **-wg** `<group>`: Lists the mapping for a Windows group. • **-uu** `<name>`: Lists the mapping for a UNIX user. • **-ug** `<group>`: Lists the mapping for a UNIX group.
backup	Saves User Name Mapping configuration and mapping data to the file specified by `<filename>`.

Parameter	Description
restore	Replaces configuration and mapping data with data from the file (specified by `<filename>`) that was created using the **backup** parameter.
adddomainmap	Adds a simple map between a Windows domain and an NIS domain or password and group files. The following options are available for this parameter: • **-d** `<windowsdomain>`: Specifies the Windows domain to be mapped. • **-y** `<NISdomain>`: Specifies the NIS domain to be mapped. You must use the **-n** `<NISserver>` parameter to specify the NIS server for the NIS domain specified by the **-y** option. • **-f** `<path>`: Specifies the fully-qualified path of directory containing the password and group files to be mapped. The files must be located on the computer being managed, and you can't use **mapadmin** to manage a remote computer to set up maps based on password and group files.
removedomainmap	Removes a simple map between a Windows domain and an NIS domain. The following options and argument are available for this parameter: • **-d** `<windowsdomain>`: Specifies the Windows domain of the map to be removed. • **-y** `<NISdomain>`: Specifies the NIS domain of the map to be removed. • **-all**: Specifies that all simple maps between Windows and NIS domains are to be removed. This will also remove any simple map between a Windows domain and password and group files.
listdomainmaps	Lists the Windows domains that are mapped to NIS domains or password and group files.

Remarks

- If you don't specify any paramters, the **mapadmin** command displays the current settings for User Name Mapping.
- For all options that specify a user or group name, the following formats can be used:
  - For Windows users, use the formats: `<domain>\<username>`, `\\<computer>\<username>`, `\<computer>\<username>`, or `<computer>\<username>`
  - For Windows groups, use the formats: `<domain>\<groupname>`, `\\<computer>\<groupname>`, `\<computer>\<groupname>`, or `<computer>\<groupname>`

- For UNIX users, use the formats: `<NISdomain>\<username>`, `<username>@<NISdomain>`, `<username>@PCNFS`, or `PCNFS\<username>`
- For UNIX groups, use the formats: `<NISdomain>\<groupname>`, `<groupname>@<NISdomain>`, `<groupname>@PCNFS`, or `PCNFS\<groupname>`

Related links

- Command-Line Syntax Key

md

Article • 02/03/2023

Creates a directory or subdirectory. Command extensions, which are enabled by default, allow you to use a single **md** command to create intermediate directories in a specified path.

> ⓘ **Note**
>
> This command is the same as the **mkdir command**.

Syntax

```
md [<drive>:]<path>
```

Parameters

Parameter	Description
`<drive>`:	Specifies the drive on which you want to create the new directory.
`<path>`	Specifies the name and location of the new directory. The maximum length of any single path is determined by the file system. This is a required parameter.
/?	Displays help at the command prompt.

Examples

To create a directory named *Directory1* within the current directory, type:

```
md Directory1
```

To create the directory tree *Taxes\Property\Current* within the root directory, with command extensions enabled, type:

```
md \Taxes\Property\Current
```

To create the directory tree *Taxes**Property**Current* within the root directory as in the previous example, but with command extensions disabled, type the following sequence of commands:

```

md \Taxes
md \Taxes\Property
md \Taxes\Property\Current
```

Related links

- Command-Line Syntax Key
- mkdir command

mkdir

Article • 02/03/2023

Creates a directory or subdirectory. Command extensions, which are enabled by default, allow you to use a single **mkdir** command to create intermediate directories in a specified path.

> **Note**
>
> This command is the same as the **md command**.

Syntax

```
mkdir [<drive>:]<path>
```

Parameters

Parameter	Description
`<drive>`:	Specifies the drive on which you want to create the new directory.
`<path>`	Specifies the name and location of the new directory. The maximum length of any single path is determined by the file system. This is a required parameter.
/?	Displays help at the command prompt.

Examples

To create a directory named *Directory1* within the current directory, type:

```
mkdir Directory1
```

To create the directory tree *Taxes\Property\Current* within the root directory, with command extensions enabled, type:

```
mkdir \Taxes\Property\Current
```

To create the directory tree *Taxes**Property**Current* within the root directory as in the previous example, but with command extensions disabled, type the following sequence of commands:

```

mkdir \Taxes
mkdir \Taxes\Property
mkdir \Taxes\Property\Current
```

Related links

- Command-Line Syntax Key
- md command

mklink

Article • 02/03/2023

Creates a directory or file symbolic or hard link.

Syntax

```
mklink [[/d] | [/h] | [/j]] <link> <target>
```

Parameters

Parameter	Description
/d	Creates a directory symbolic link. By default, this command creates a file symbolic link.
/h	Creates a hard link instead of a symbolic link.
/j	Creates a Directory Junction.
`<link>`	Specifies the name of the symbolic link being created.
`<target>`	Specifies the path (relative or absolute) that the new symbolic link refers to.
/?	Displays help at the command prompt.

Examples

To create and remove a symbolic link named MyFolder from the root directory to the \Users\User1\Documents directory, and a hard link named Myfile.file to the example.file file located within the directory, type:

```
mklink /d \MyFolder \Users\User1\Documents
mklink /h \MyFile.file \User1\Documents\example.file
rd \MyFolder
del \MyFile.file
```

Related links

- Command-Line Syntax Key
- del command
- rd command
- New-Item in Windows PowerShell

mmc

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Using mmc command-line options, you can open a specific **mmc** console, open **mmc** in author mode, or specify that the 32-bit or 64-bit version of **mmc** is opened.

Syntax

```
mmc <path>\<filename>.msc [/a] [/64] [/32]
```

Parameters

Parameter	Description
`<path>\<filename>.msc`	starts **mmc** and opens a saved console. You need to specify the complete path and file name for the saved console file. If you do not specify a console file, **mmc** opens a new console.
/a	Opens a saved console in author mode. Used to make changes to saved consoles.
/64	Opens the 64-bit version of **mmc** (mmc64). Use this option only if you are running a Microsoft 64-bit operating system and want to use a 64-bit snap-in.
/32	Opens the 32-bit version of **mmc** (mmc32). When running a Microsoft 64-bit operating system, you can run 32-bit snap-ins by opening mmc with this command-line option when you have 32-bit only snap-ins.

Remarks

- You can use environment variables to create command lines or shortcuts that don't depend on the explicit location of console files. For instance, if the path to a console file is in the system folder (for example, **mmc c:\winnt\system32\console_name.msc**), you can use the expandable data string **%systemroot%** to specify the location (**mmc%systemroot%\system32\console_name.msc**). This may be useful if you're

delegating tasks to people in your organization who are working on different computers.

- When consoles are opened using the **/a** option, they're opened in author mode, regardless of their default mode. This doesn't permanently change the default mode setting for files; when you omit this option, mmc opens console files according to their default mode settings.
- After you open **mmc** or a console file in author mode, you can open any existing console by clicking **Open** on the **Console** menu.
- You can use the command line to create shortcuts for opening **mmc** and saved consoles. A command-line command works with the **Run** command on the **Start** menu, in any command-prompt window, in shortcuts, or in any batch file or program that calls the command.

Related links

- Command-Line Syntax Key

mode

Article • 02/03/2023

Displays system status, changes system settings, or reconfigures ports or devices. If used without parameters, **mode** displays all the controllable attributes of the console and the available COM devices.

Serial port

Configures a serial communications port and sets the output handshake.

Syntax

```
mode com<m>[:] [baud=<b>] [parity=<p>] [data=<d>] [stop=<s>] [to={on|off}]
[xon={on|off}] [odsr={on|off}] [octs={on|off}] [dtr={on|off|hs}] [rts=
{on|off|hs|tg}] [idsr={on|off}]
```

Parameters

Parameter	Description
`com<m>[:]`	Specifies the number of the async Prncnfg.vbshronous communications port.
`baud=<b>`	Specifies the transmission rate in bits per second. The valid values include: • **11** - 110 baud • **15** - 150 baud • **30** - 300 baud • **60** - 600 baud • **12** - 1200 baud • **24** - 2400 baud • **48** - 4800 baud • **96** - 9600 baud • **19** - 19,200 baud

Parameter	Description
`parity=<p>`	Specifies how the system uses the parity bit to check for transmission errors. The valid values include: • **n** - none • **e** - even (default value) • **o** - odd • **m** - mark • **s** - space Not all devices support using the **m** or **s** parameters.
`data=<d>`	Specifies the number of data bits in a character. Valid values range from **5** through **8**. The default value is **7**. Not all devices support the values **5** and **6**.
`stop=<s>`	Specifies the number of stop bits that define the end of a character: **1**, **1.5**, or **2**. If the baud rate is **110**, the default value is **2**. Otherwise, the default value is **1**. Not all devices support the value **1.5**.
`to={on | off}`	Specifies whether the device uses infinite time out processing. The default value is **off**. Turning this option **on** means that the device will never stop waiting to receive a response from a host or client computer.
`xon={on | off}`	Specifies whether the system allows the XON/XOFF protocol. This protocol provides flow control for serial communications, enhancing reliability, but reducing performance.
`odsr={on | off}`	Specifies whether the system turns on the Data Set Ready (DSR) output handshake.
`octs={on | off}`	Specifies whether the system turns on the Clear to Send (CTS) output handshake.
`dtr={on | off | hs}`	Specifies whether the system turns on the Data Terminal Ready (DTR) output handshake. Setting this value to **on** mode, provides a constant signal to show the terminal is ready to send data. Setting this value to **hs** mode provides a handshake signal between the two terminals.
`rts={on | off | hs | tg}`	Specifies whether the system turns on the Request to Send (RTS) output handshake. Setting this value to **on** mode, provides a constant signal to show the terminal is ready to send data. Setting this value to **hs** mode provides a handshake signal between the two terminals. Setting this value to **tg** mode provides a way to toggle between ready and not ready states.
`idsr={on | off}`	Specifies whether the system turns on the DSR sensitivity. You must turn this option on to use DSR handshaking.
/?	Displays help at the command prompt.

Device status

Displays the status of a specified device. If used without parameters, **mode** displays the status of all devices installed on your system.

Syntax

```
mode [<device>] [/status]
```

Parameters

Parameter	Description
`<device>`	Specifies the name of the device for which you want to display the status. Standard names include, LPT1: through LPT3:, COM1: through COM9:, and CON.
/status	Requests the status of any redirected parallel printers. You can also use **/sta** as an abbreviated version of this command.
/?	Displays help at the command prompt.

Redirect printing

Redirects printer output. You must be a member of the Administrators group to redirect printing.

> ⓘ Note

To set up your system so that it sends parallel printer output to a serial printer, you must use the **mode** command twice. The first time, you must use **mode** to configure the serial port. The second time, you must use **mode** to redirect parallel printer output to the serial port you specified in the first **mode** command.

Syntax

```
mode LPT<n>[:]=COM<m>[:]
```

Parameters

Parameter	Description
LPT`<n>`[:]	Specifies the number of the LPT to configure. Typically, this means providing a value from **LTP1: through LTP3:**, unless your system includes special parallel port support. This parameter is required.
COM`<m>`[:]	Specifies the COM port to configure. Typically, this means providing a value from **COM1: through COM9:**, unless your system has special hardware for additional COM ports. This parameter is required.
/?	Displays help at the command prompt.

Examples

To redirect a serial printer that operates at 4800 baud with even parity, and is connected to the COM1 port (the first serial connection on your computer), type:

```
mode com1 48,e,,,b
mode lpt1=com1
```

To redirect parallel printer output from LPT1 to COM1, and then to print a file using LPT1, type the following command before you print the file:

```
mode lpt1
```

This command prevents the redirection the file from LPT1 to COM1.

Select code page

Configures or queries the code page info for a selected device.

Syntax

```
mode <device> codepage select=<yyy>
mode <device> codepage [/status]
```

Parameters

Parameter	Description
`<device>`	Specifies the device for which you want to select a code page. CON is the only valid name for a device. This parameter is required.
codepage	Specifies which code page to use with the specified device. You can also use **cp** as an abbreviated version of this command. This parameter is required.
select=`<yyy>`	Specifies the number of the code page to use with the device. The supported code pages, by country/region or language, include: • **437:** United States • **850:** Multilingual (Latin I) • **852:** Slavic (Latin II) • **855:** Cyrillic (Russian) • **857:** Turkish • **860:** Portuguese • **861:** Icelandic • **863:** Canadian-French • **865:** Nordic • **866:** Russian • **869:** Modern Greek This parameter is required.
/status	Displays the numbers of the current code pages selected for the specified device. You can also use **/sta** as an abbreviated version of this command. Regardless whether you specify **/status**, the **mode codepage** command will display the numbers of the code pages that are selected for the specified device.
/?	Displays help at the command prompt.

Display mode

Changes the size of the command prompt screen buffer

Syntax

```
mode con[:] [cols=<c>] [lines=<n>]
```

Parameters

Parameter	Description
con[:]	Indicates that the change applies to the Command Prompt window. This parameter is required.
cols=`<c>`	Specifies the number of columns in the command prompt screen buffer. The default setting is 80 columns, but you can set this to any value. If you don't use the default, typical values are 40 and 135 columns. Using non-standard values can result in the command prompt app problems.
lines=`<n>`	Specifies the number of lines in the command prompt screen buffer. The default value is 25, but you can set this to any value. If you don't use the default, the other typical value is 50 lines.
/?	Displays help at the command prompt.

Typematic rate

Sets the keyboard typematic rate. The typematic rate is the speed at which Windows can repeat a character when you press the key on a keyboard.

> ⓘ Note
>
> Some keyboards don't recognize this command.

Syntax

```
mode con[:] [rate=<r> delay=<d>]
```

Parameters

Parameter	Description
con[:]	Specifies the keyboard. This parameter is required.
rate=`<r>`	Specifies the rate at which a character is repeated on the screen when you hold down a key. The default value is 20 characters per second for IBM AT-compatible keyboards, and 21 for IBM PS/2-compatible keyboards, but you can use any value from 1 through 32. If you set this parameter, you must also set the **delay** parameter.

Parameter	Description
delay=`<d>`	Specifies the amount of time that will elapse after you press and hold down a key before the character output repeats. The default value is 2 (.50 seconds), but you can also use 1 (.25 seconds), 3 (.75 seconds), or 4 (1 second). If you set this parameter, you must also set the **rate** parameter.
/?	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

more

Article • 02/03/2023

Displays one screen of output at a time.

> **Note**
>
> The **more** command, with different parameters, is also available from the Recovery Console.

Syntax

```
<command> | more [/c] [/p] [/s] [/t<n>] [+<n>]
more [[/c] [/p] [/s] [/t<n>] [+<n>]] < [<drive>:][<path>]<filename>
more [/c] [/p] [/s] [/t<n>] [+<n>] [<files>]
```

Parameters

Parameter	Description
`<command>`	Specifies a command for which you want to display the output.
/c	Clears the screen before displaying a page.
/p	Expands form-feed characters.
/s	Displays multiple blank lines as a single blank line.
/t`<n>`	Displays tabs as the number of spaces specified by *n*.
+`<n>`	Displays the first file, beginning at the line specified by *n*.
`[<drive>:][<path>]<filename>`	Specifies the location and name of a file to display.
`<files>`	Specifies a list of files to display. Files must be separated using spaces.
/?	Displays help at the command prompt.

Remarks

- The following subcommands are accepted at the **more** prompt (`-- More --`), including:

Key	Action
SPACEBAR	Press the **SPACEBAR** to display the next screen.
ENTER	Press **ENTER** to display the file one line at a time.
f	Press **F** to display the next file listed on the command line.
q	Press **Q** to quit the **more** command.
=	Shows the line number.
p `<n>`	Press **P** to display the next *n* lines.
s `<n>`	Press **S** to skip the next *n* lines.
?	Press **?** to show the commands that are available at the **more** prompt.

- If you use the redirection character (`<`), you must also specify a file name as the source.
- If you use the pipe (`|`), you can use such commands as **dir**, **sort**, and **type**.

Examples

To view the first screen of information of a file named *Clients.new*, type one of the following commands:

```
more < clients.new
type clients.new | more
```

The **more** command displays the first screen of information from Clients.new, and you can press the SPACEBAR to see the next screen of information.

To clear the screen and remove all extra blank lines before displaying the file *Clients.new*, type one of the following commands:

```
more /c /s < clients.new
type clients.new | more /c /s
```

To display the current line number at the **more** prompt, type:

```
more =
```

The current line number is added to the **more** prompt, as `-- More [Line: 24] --`

To display a specific number of lines at the **more** prompt, type:

```
more p
```

The **more** prompt asks you for the number of lines to display, as follows: `-- More -- Lines:`. Type the number of lines to display, and then press ENTER. The screen changes to show only that number of lines.

To skip a specific number of lines at the **more** prompt, type:

```
more s
```

The **more** prompt asks you for the number of lines to skip, as follows: `-- More -- Lines:`. Type the number of lines to skip, and then press ENTER. The screen changes to show that those lines are skipped.

Related links

- Command-Line Syntax Key
- Windows Recovery Environment (WinRE)

mount

Article • 09/28/2023

A command-line utility that mounts Network File System (NFS) network shares. When used without options or arguments, **mount** displays information about all mounted NFS file systems.

> **Note**
>
> This utility is available only if **Client for NFS** is installed.

Syntax

```
mount [-o <option>[...]] [-u:<username>] [-p:{<password> | *}] {\\
<computername>\<sharename> | <computername>:/<sharename>} {<devicename> | *}
```

Parameters

Parameter	Description
-o rsize=`<buffersize>`	Sets the size in kilobytes of the read buffer. Acceptable values are 1, 2, 4, 8, 16, and 32; the default is 32 KB.
-o wsize=`<buffersize>`	Sets the size in kilobytes of the write buffer. Acceptable values are 1, 2, 4, 8, 16, and 32; the default is 32 KB.
-o timeout=`<seconds>`	Sets the time-out value in seconds for a remote procedure call (RPC). Acceptable values are 0.8, 0.9, and any integer in the range 1-60; the default is 0.8.
-o retry=`<number>`	Sets the number of retries for a soft mount. Acceptable values are integers in the range 1-10; the default is 1.
-o mtype=`{soft|hard}`	Sets the mount type for your NFS share. By default, Windows uses a soft mount. Soft mounts time out more easily when there are connection issues; however, to reduce I/O disruption during NFS server reboots, we recommend using a hard mount.
-o lang=`{euc-jp|euc-tw|euc-kr|shift-`	Specifies the language encoding to configure on an NFS share. You can use only one language on the share. This value

Parameter	Description
`jis|Big5|Ksc5601|Gb2312-80|Ansi}`	can include any of the following values: • **euc-jp:** Japanese • **euc-tw:** Chinese • **euc-kr:** Korean • **shift-jis:** Japanese • **Big5:** Chinese • **Ksc5601:** Korean • **Gb2312-80:** Simplified Chinese • **Ansi:** ANSI-encoded
-o fileaccess=`<mode>`	Specifies the default permission mode of new files created on the NFS share. Specify *mode* as a three-digit number in the form *ogw*, where *o*, *g*, and *w* are each a digit representing the access granted the file's owner, group, and the world, respectively. The digits must be in the range 0-7, including: • **0:** No access • **1:** x (execute access) • **2:** w (write access) • **3:** wx (write and execute access) • **4:** r (read access) • **5:** rx (read and execute access) • **6:** rw (read and write access) • **7:** rwx (read, write, and execute access)
-o anon	Mounts as an anonymous user.
-o nolock	Disables locking (default is **enabled**).
-o casesensitive	Forces file lookups on the server to be case sensitive.
-o sec=`{sys|krb5|krb5i|krb5p}`	Specifies the security mechanism for mounting an NFS share. This value can include any of the following: • **sec=sys:** No authentication or security checks are performed. Data transfers aren't encrypted. • **sec=krb5:** Specifies Kerberos authentication for mounting the NFS share. • **sec=krb5i:** Extends Kerberos security by adding data integrity checks between the client and server hasn't been tampered. • **sec=krb5p:** Enhances Kerberos security by enabling data privacy, which encrypts data exchanged between the client and server.
-u:`<username>`	Specifies the user name to use for mounting the share. If *username* isn't preceded by a backslash (****), it's treated as a

Parameter	Description
	UNIX user name.
-p:`<password>`	The password to use for mounting the share. If you use an asterisk (*), you're prompted for the password.
`<computername>`	Specifies the name of the NFS server.
`<sharename>`	Specifies the name of the file system.
`<devicename>`	Specifies the drive letter and name of the device. If you use an asterisk (*) this value represents the first available driver letter.

Examples

To mount the NFS share anonymously on network drive Z, type:

Windows Command Prompt

```
mount -o anon \\ServerIP\ShareName Z:
```

> **Note**
>
> In order for this parameter to function as intended, the NFS server must allow anonymous access.

To mount the NFS share and disable file locking for network drive Z, type:

Windows Command Prompt

```
mount -o nolock \\ServerIP\ShareName Z:
```

To mount the NFS share with permissions for the *ogw* set as rwx, rw, r, and to continuously reconnect to the NFS server if the connection is lost for network drive Z, type:

Windows Command Prompt

```
mount -o fileaccess=764 mtype=hard \\ServerIP\ShareName Z:
```

Related links

- Command-Line Syntax Key

mountvol

Article • 02/03/2023

Creates, deletes, or lists a volume mount point. You can also link volumes without requiring a drive letter.

Syntax

```
mountvol [<drive>:]<path volumename>
mountvol [<drive>:]<path> /d
mountvol [<drive>:]<path> /l
mountvol [<drive>:]<path> /p
mountvol /r
mountvol [/n|/e]
mountvol <drive>: /s
```

Parameters

Parameter	Description
`[<drive>:]<path>`	Specifies the existing NTFS directory where the mount point will reside.
`<volumename>`	Specifies the volume name that is the target of the mount point. The volume name uses the following syntax, where *GUID* is a globally unique identifier: `\\?\volume\{GUID}\`. The brackets `{ }` are required.
/d	Removes the volume mount point from the specified folder.
/l	Lists the mounted volume name for the specified folder.
/p	Removes the volume mount point from the specified directory, dismounts the basic volume, and takes the basic volume offline, making it unmountable. If other processes are using the volume, **mountvol** closes any open handles before dismounting the volume.
/r	Removes volume mount point directories and registry settings for volumes that are no longer in the system, preventing them from being automatically mounted and given their former volume mount point(s) when added back to the system.
/n	Disables automatic mounting of new basic volumes. New volumes are not mounted automatically when added to the system.

Parameter	Description
/e	Re-enables automatic mounting of new basic volumes.
/s	Mounts the EFI system partition on the specified drive.
/?	Displays help at the command prompt.

Remarks

- If you dismount your volume while using the **/p** parameter, the volume list will show the volume as not mounted until a volume mount point is created.
- If your volume has more than one mount point, use **/d** to remove the additional mount points before using **/p**. You can make the basic volume mountable again by assigning a volume mount point.
- If you need to expand your volume space without reformatting or replacing a hard drive, you can add a mount path to another volume. The benefit of using one volume with several mount paths is that you can access all local volumes by using a single drive letter (such as `C:`). You don't need to remember which volume corresponds to which drive letter—although you can still mount local volumes and assign them drive letters.

Examples

To create a mount point, type:

```
mountvol \sysmount \\?\volume\{2eca078d-5cbc-43d3-aff8-7e8511f60d0e}\
```

Related links

- Command-Line Syntax Key

move

Article • 02/03/2023

Moves one or more files from one directory to another directory.

> **ⓘ Important**
>
> Moving encrypted files to a volume that doesn't support Encrypting File System (EFS) results will result in an error. You must first decrypt the files or move them to a volume that supports EFS.

Syntax

```
move [{/y|-y}] [<source>] [<target>]
```

Parameters

Parameter	Description
/y	Stops prompting for confirmation that you want to overwrite an existing destination file. This parameter might be preset in the COPYCMD environment variable. You can override this preset by using the **-y** parameter. The default is to prompt before overwriting files, unless the command is run from within a batch script.
-y	Starts prompting for confirmation that you want to overwrite an existing destination file.
`<source>`	Specifies the path and name of the file(s) to move. To move or rename a directory, the *source* should be the current directory path and name.
`<target>`	Specifies the path and name to move files to. To move or rename a directory, the *target* should be the desired directory path and name.
/?	Displays help at the command prompt.

Examples

To move all files with the .xls extension from the *\Data* directory to the *\Second_Q\Reports* directory, type:

```
move \data\*.xls \second_q\reports\
```

Related links

- Command-Line Syntax Key

mqbkup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Backs up MSMQ message files and registry settings to a storage device and restores previously-stored messages and settings.

Both the backup and the restore operations stop the local MSMQ service. If the MSMQ service was started beforehand, the utility will attempt to restart the MSMQ service at the end of the backup or the restore operation. If the service was already stopped before running the utility, no attempt to restart the service is made.

Before using the MSMQ Message Backup/Restore utility you must close all local applications that are using MSMQ.

Syntax

```
mqbkup {/b | /r} <folder path_to_storage_device>
```

Parameters

Parameter	Description
/b	Specifies backup operation.
/r	Specifies restore operation.
`<folder path_to_storage_device>`	Specifies the path where the MSMQ message files and registry settings are stored.
/?	Displays help at the command prompt.

Remarks

- If a specified folder doesn't exist while performing either the backup or restore operation, the folder is automatically created by the utility.

- If you choose to specify an existing folder, it must be empty. If you specify a non-empty folder, the utility deletes every file and subfolder contained within it. In this case, you'll be prompted to give permission to delete existing files and subfolders. You can use the **/y** parameter to indicate that you agree beforehand to the deletion of all existing files and subfolders in the specified folder.

- The locations of folders used to store MSMQ message files are stored in the registry. Therefore, the utility restores MSMQ message files to the folders specified in the registry and not to the storage folders used before the restore operation.

Examples

To backup all MSMQ message files and registry settings, and to store them in the *msmqbkup* folder on your C: drive, type:

```
mqbkup /b c:\msmqbkup
```

To delete all existing files and subfolders in the *oldbkup* folder on your C: drive, and then to store MSMQ message files and registry settings in the folder, type:

```
mqbkup /b /y c:\oldbkup
```

To restore MSMQ messages and registry settings, type:

```
mqbkup /r c:\msmqbkup
```

Related links

- Command-Line Syntax Key
- MSMQ Powershell Reference

mqsvc

Article • 02/03/2023

Message Queuing technology enables apps running at different times to communicate across heterogeneous networks and systems that may be temporarily offline. Message Queuing provides guaranteed message delivery, efficient routing, security, and priority-based messaging. It can be used to implement solutions for both asynchronous and synchronous messaging scenarios. For more information about Message Queuing, see Message Queuing (MSMQ).

Syntax

```
mqsvc.exe
```

Related links

- Command-Line Syntax Key
- MSMQ Powershell Reference

mqtgsvc

Article • 02/03/2023

Monitors a queue for incoming messages and performs an action, in the form of an executable file or COM component, when the rules of a trigger are evaluated as true. For examples of how the Message Queuing Triggers service can be used, see Message Queuing Triggers.

Syntax

```
mqtgsvc.exe
```

Related links

- Command-Line Syntax Key
- MSMQ Powershell Reference

msdt

Article • 02/21/2023

Invokes a troubleshooting pack at the command line or as part of an automated script, and enables additional options without user input.

> **Note**
>
> The Microsoft Support Diagnostic Tool (MSDT) is deprecated. For more information, see **Deprecated Windows features**.

Syntax

```
msdt </id <name> | /path <name> | /cab < name>> <</parameter> [options] …
<parameter> [options]>>
```

Parameters

Parameter	Description
/id `<packagename>`	Specifies which diagnostic package to run. For a list of available packages, see Available Troubleshooting packs.
/path `<directory|.diagpkg file|.diagcfg file>`	Specifies the full path to a diagnostic package. If you specify a directory, the directory must contain a diagnostic package. You cannot use the **/path** parameter in conjunction with the** /id**, **/dci**, or **/cab** parameters.
/dci `<passkey>`	Prepopulates the passkey field. This parameter is only used when a support provider has supplied a passkey.
/dt `<directory>`	Displays the troubleshooting history in the specified directory. Diagnostic results are stored in the user's **%LOCALAPPDATA%\Diagnostics** or **%LOCALAPPDATA%\ElevatedDiagnostics** directories.
/af `<answerfile>`	Specifies an answer file in XML format that contains responses to one or more diagnostic interactions.

Parameter	Description
/modal `<ownerHWND>`	Makes the troubleshooting pack modal to a window designated by the parent Console Window Handle (HWND), in decimal. This parameter is typically used by applications that launch a troubleshooting pack. For more information about obtaining Console Window Handles, see How to Obtain a Console Window Handle (HWND).
/moreoptions `<true|false>`	Enables (true) or suppresses (false) the final troubleshooting screen that asks if the user wants to explore additional options. This parameter is typically used when the troubleshooting pack is launched by a troubleshooter that isn't part of the operating system.
/param `<parameters>`	Specifies a set of interaction responses at the command line, similar to an answer file. This parameter isn't typically used within the context of troubleshooting packs created with TSP Designer. For more information about developing custom parameters, see Windows Troubleshooting Platform.
/advanced	Expands the advanced link on the Welcome page by default when the troubleshooting pack is started.
/custom	Prompts the user to confirm each possible resolution before it's applied.

Return codes

Troubleshooting packs comprise a set of root causes, each of which describes a specific technical problem. After completing the troubleshooting pack tasks, each root cause returns a state of fixed, not fixed, detected (but not fixable), or not found. In addition to specific results reported in the troubleshooter user interface, the troubleshooting engine returns a code in the results describing, in general terms, whether or not the troubleshooter fixed the original problem. The codes are:

Code	Description
-1	**Interruption:** The troubleshooter was closed before the troubleshooting tasks were completed.
0	**Fixed:** The troubleshooter identified and fixed at least one root cause, and no root causes remain in a not fixed state.
1	**Present, but not fixed:** The troubleshooter identified one or more root causes that remain in a not fixed state. This code is returned even if another root cause was fixed.
2	**Not found:** The troubleshooter didn't identify any root causes.

Related links

- Command-Line Syntax Key
- Available troubleshooting packs
- TroubleshootingPack PowerShell reference

msg

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sends a message to a user on a Remote Desktop Session Host server.

> **Note**
>
> You must have Message special access permission to send a message.

Syntax

```
msg {<username> | <sessionname> | <sessionID>| @<filename> | *} [/server:<servername>] [/time:<seconds>] [/v] [/w] [<message>]
```

Parameters

Parameter	Description
`<username>`	Specifies the name of the user that you want to receive the message. If you don't specify a user or a session, this command displays an error message. When specifying a session, it must be an active one.
`<sessionname>`	Specifies the name of the session that you want to receive the message. If you don't specify a user or a session, this command displays an error message. When specifying a session, it must be an active one.
`<sessionID>`	Specifies the numeric ID of the session whose user you want to receive a message.
`@<filename>`	Identifies a file containing a list of user names, session names, and session IDs that you want to receive the message.
*	Sends the message to all user names on the system.
/server:`<servername>`	Specifies the Remote Desktop Session Host server whose session or user you want to receive the message. If unspecified, **/server** uses the server to which you are currently logged on.

Parameter	Description
/time:`<seconds>`	Specifies the amount of time that the message you sent is displayed on the user's screen. After the time limit is reached, the message disappears. If no time limit is set, the message defaults to **60 seconds** and disappears.
/v	Displays information about the actions being performed.
/w	Waits for an acknowledgment from the user that the message has been received. Use this parameter with `/time:<*seconds*>` to avoid a possible long delay if the user does not immediately respond. Using this parameter with **/v** is also helpful.
`<message>`	Specifies the text of the message that you want to send. If no message is specified, you will be prompted to enter a message. To send a message that is contained in a file, type the less than (<) symbol followed by the file name.
/?	Displays help at the command prompt.

Examples

To send a message entitled, *Let's meet at 1PM today* to all sessions for *User1*, type:

```
msg User1 Let's meet at 1PM today
```

To send the same message to session *modeM02*, type:

```
msg modem02 Let's meet at 1PM today
```

To send the message to all sessions contained in the file *userlist*, type:

```
msg @userlist Let's meet at 1PM today
```

To send the message to all users who are logged on, type:

```
msg * Let's meet at 1PM today
```

To send the message to all users, with an acknowledgment time-out (for example, 10 seconds), type:

```
msg * /time:10 Let's meet at 1PM today
```

Related links

- Command-Line Syntax Key

msiexec

Article • 02/03/2023

Provides the means to install, modify, and perform operations on Windows Installer from the command line.

Install options

Set the install type for launching an installation package.

Syntax

```
msiexec.exe [/i][/a][/j{u|m|/g|/t}][/x] <path_to_package>
```

Parameters

Parameter	Description
/i	Specifies normal installation.
/a	Specifies administrative installation.
/ju	Advertise the product to the current user.
/jm	Advertise the product to all users.
/j/g	Specifies the language identifier used by the advertised package.
/j/t	Applies transform to the advertised package.
/x	Uninstalls the package.
`<path_to_package>`	Specifies the location and name of the installation package file.

Examples

To install a package named *example.msi* from the C: drive, using a normal installation process, type:

```
msiexec.exe /i "C:\example.msi"
```

Display options

You can configure what a user sees during the installation process, based on your target environment. For example, if you're distributing a package to all clients for manual installation, there should be a full UI. However, if you're deploying a package using Group Policy, which requires no user interaction, there should be no UI involved.

Syntax

```
msiexec.exe /i <path_to_package> [/quiet][/passive][/q{n|b|r|f}]
```

Parameters

Parameter	Description
`<path_to_package>`	Specifies the location and name of the installation package file.
/quiet	Specifies quiet mode, which means there's no user interaction required.
/passive	Specifies unattended mode, which means the installation only shows a progress bar.
/qn	Specifies there's no UI during the installation process.
/qn+	Specifies there's no UI during the installation process, except for a final dialog box at the end.
/qb	Specifies there's a basic UI during the installation process.
/qb+	Specifies there's a basic UI during the installation process, including a final dialog box at the end.
/qr	Specifies a reduced UI experience during the installation process.
/qf	Specifies a full UI experience during the installation process.

Remarks

- The modal box isn't shown if the installation is cancelled by the user. You can use **qb+!** or **qb!+** to hide the **CANCEL** button.

Examples

To install package *C:\example.msi*, using a normal installation process and no UI, type:

```
msiexec.exe /i "C:\example.msi" /qn
```

Restart options

If your installation package overwrites files or attempts to change files that are in use, a reboot might be required before the installation completes.

Syntax

```
msiexec.exe /i <path_to_package> [/norestart][/promptrestart][/forcerestart]
```

Parameters

Parameter	Description
`<path_to_package>`	Specifies the location and name of the installation package file.
/norestart	Stops the device from restarting after the installation completes.
/promptrestart	Prompts the user if a reboot is required.
/forcerestart	Restarts the device after the installation completes.

Examples

To install package *C:\example.msi*, using a normal installation process with no reboot at the end, type:

```
msiexec.exe /i "C:\example.msi" /norestart
```

Logging options

If you need to debug your installation package, you can set the parameters to create a log file with specific information.

Syntax

```
msiexec.exe [/i][/x] <path_to_package> [/L{i|w|e|a|r|u|c|m|o|p|v|x+|!|*}]
<path_to_log>
```

Parameters

Parameter	Description
/i	Specifies normal installation.
/x	Uninstalls the package.
`<path_to_package>`	Specifies the location and name of the installation package file.
/li	Turns on logging and includes status messages in the output log file.
/lw	Turns on logging and includes non-fatal warnings in the output log file.
/le	Turns on logging and includes all error messages in the output log file.
/la	Turns on logging and includes information about when an action started in the output log file.
/lr	Turns on logging and includes action-specific records in the output log file.
/lu	Turns on logging and includes user request information in the output log file.
/lc	Turns on logging and includes the initial UI parameters in the output log file.
/lm	Turns on logging and includes out-of-memory or fatal exit information in the output log file.
/lo	Turns on logging and includes out-of-disk-space messages in the output log file.
/lp	Turns on logging and includes terminal properties in the output log file.

Parameter	Description
/lv	Turns on logging and includes verbose output in the output log file.
/lx	Turns on logging and includes extra debugging information in the output log file.
/l+	Turns on logging and appends the information to an existing log file.
/l!	Turns on logging and flushes each line to the log file.
/l*	Turns on logging and logs all information, except verbose information (**/lv**) or extra debugging information (**/lx**).
`<path_to_logfile>`	Specifies the location and name for the output log file.

Examples

To install package *C:\example.msi*, using a normal installation process with all logging information provided, including verbose output, and storing the output log file at *C:\package.log*, type:

```
msiexec.exe /i "C:\example.msi" /L*V "C:\package.log"
```

Update options

You can apply or remove updates using an installation package.

Syntax

```
msiexec.exe [/p][/update][/uninstall[/package<product_code_of_package>]]
<path_to_package>
```

Parameters

Parameter	Description

Parameter	Description
/p	Installs a patch. If you're installing silently, you must also set the REINSTALLMODE property to *ecmus* and REINSTALL to *ALL*. Otherwise, the patch only updates the MSI cached on the target device.
/update	Install patches option. If you're applying multiple updates, you must separate them using a semi-colon (;).
/package	Installs or configures a product.

Examples

```
msiexec.exe /p "C:\MyPatch.msp"
msiexec.exe /p "C:\MyPatch.msp" /qb REINSTALLMODE="ecmus" REINSTALL="ALL"
msiexec.exe /update "C:\MyPatch.msp"
```

```
msiexec.exe /uninstall {1BCBF52C-CD1B-454D-AEF7-852F73967318} /package
{AAD3D77A-7476-469F-ADF4-04424124E91D}
```

Where the first GUID is the patch GUID, and the second one is the MSI product code to which the patch was applied.

Repair options

You can use this command to repair an installed package.

Syntax

```
msiexec.exe [/f{p|o|e|d|c|a|u|m|s|v}] <product_code>
```

Parameters

Parameter	Description
/fp	Repairs the package if a file is missing.

Parameter	Description
/fo	Repairs the package if a file is missing, or if an older version is installed.
/fe	Repairs the package if file is missing, or if an equal or older version is installed.
/fd	Repairs the package if file is missing, or if a different version is installed.
/fc	Repairs the package if file is missing, or if checksum does not match the calculated value.
/fa	Forces all files to be reinstalled.
/fu	Repairs all the required user-specific registry entries.
/fm	Repairs all the required computer-specific registry entries.
/fs	Repairs all existing shortcuts.
/fv	Runs from source and re-caches the local package.

Examples

To force all files to be reinstalled based on the MSI product code to be repaired, *{AAD3D77A-7476-469F-ADF4-04424124E91D}*, type:

```
msiexec.exe /fa {AAD3D77A-7476-469F-ADF4-04424124E91D}
```

Set public properties

You can set public properties through this command. For information about the available properties and how to set them, see Public Properties.

Related links

- Command-Line Syntax Key
- Msiexec.exe Command-Line Options
- Standard Installer Command-Line Options

msinfo32

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Opens the System Information tool to display a comprehensive view of the hardware, system components, and software environment on the local computer.

Some System Information categories contain large amounts of data. You can use the **start /wait** command to optimize reporting performance for these categories. For more information, see System Information.

Syntax

```
msinfo32 [/pch] [/nfo <path>] [/report <path>] [/computer <computername>]
[/showcategories] [/category <categoryID>] [/categories {+<categoryID>(+
<categoryID>)|+all(-<categoryID>)}]
```

Parameters

Parameter	Description
`<path>`	Specifies the file to be opened in the format *C:\Folder1\File1.xxx*, where *C* is the drive letter, *Folder1* is the folder, *File1* is the file name, and *xxx* is the file name extension. This file can be an **.nfo**, **.xml**, **.txt**, or **.cab** file.
`<computername>`	Specifies the name of the target or local computer. This can be a UNC name, an IP address, or a full computer name.
`<categoryID>`	Specifies the ID of the category item. You can obtain the category ID by using **/showcategories**.
/pch	Displays the System History view in the System Information tool.
/nfo	Saves the exported file as an **.nfo** file. If the file name that is specified in *path* does not end in an **.nfo** extension, the **.nfo** extension is automatically appended to the file name.

Parameter	Description
/report	Saves the file in *path* as a text file. The file name is saved exactly as it appears in *path*. The .txt extension is not appended to the file unless it is specified in path.
/computer	Starts the System Information tool for the specified remote computer. You must have the appropriate permissions to access the remote computer.
/showcategories	Starts the System Information tool with all available category IDs displayed, rather than displaying the friendly or localized names. For example, the Software Environment category is displayed as the **SWEnv** category.
/category	Starts System Information with the specified category selected. Use **/showcategories** to display a list of available category IDs.
/categories	Starts System Information with only the specified category or categories displayed. It also limits the output to the selected category or categories. Use **/showcategories** to display a list of available category IDs.
/?	Displays help at the command prompt.

Examples

To list the available category IDs, type:

```
msinfo32 /showcategories
```

To start the System Information tool with all available information displayed, except Loaded Modules, type:

```
msinfo32 /categories +all -loadedmodules
```

To display **System Summary** information and to create an .nfo file called *syssum.nfo*, which contains information in the **System Summary** category, type:

```
msinfo32 /nfo syssum.nfo /categories +systemsummary
```

To display resource conflict information and to create an .nfo file called *conflicts.nfo*, which contains information about resource conflicts, type:

```
msinfo32 /nfo conflicts.nfo /categories
+componentsproblemdevices+resourcesconflicts+resourcesforcedhardware
```

Related links

- Command-Line Syntax Key

mstsc

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates connections to Remote Desktop Session Host servers or other remote computers and edits an existing Remote Desktop Connection (.rdp) configuration file.

Syntax

```
mstsc.exe [<connectionfile>] [/v:<server>[:<port>]] [/g:<gateway>] [/admin]
[/f <fullscreen>] [/w:<width> /h:<height>] [/public] [/multimon] [/l]
[/restrictedadmin] [/remoteguard] [/prompt] [/shadow:<sessionid>] [/control]
[/noconsentprompt]
mstsc.exe /edit <connectionfile>
```

Parameters

Parameter	Description
`<connectionfile>`	Specifies the name of an **.rdp** file for the connection.
/v:`<server>[:<port>]`	Specifies the remote computer and, optionally, the port number to which you want to connect.
/g:`<gateway>`	Specifies the RD Gateway server to use for the connection. This parameter is only read if the endpoint PC is specified with **/v**.
/admin	Connects you to a session for administering the server.
/f	Starts Remote Desktop Connection in full-screen mode.
/w:`<width>`	Specifies the width of the Remote Desktop window.
/h:`<height>`	Specifies the height of the Remote Desktop window.
/public	Runs Remote Desktop in public mode. In public mode, passwords and bitmaps aren't cached.
/multimon	Configures the Remote Desktop Services session monitor layout to be identical to the current client-side configuration.

Parameter	Description
/l	Enumerates the monitor attached to the local PC and the ID associated with each monitor. The monitor ID can be used to populate the selected monitors RDP file setting.
/edit `<connectionfile>`	Opens the specified **.rdp** file for editing.
/restrictedAdmin	This mode won't send your credentials to the remote PC, which can protect you if you connect to a compromised device. Connections made from the remote PC might not be authenticated by other PCs, which impact application functionality and compatibility. The **/admin** parameter is implied.
/remoteGuard	This mode prevents credentials from being sent to the remote PC, which can help protect your credentials if you connect to a compromised device. Unlike Restricted Administrator mode, Remote Guard also supports connections made from the remote PC by redirecting all requests back to your device.
/prompt	Prompts you for your credentials when you connect to the remote PC.
/shadow:`<sessionID>`	Specifies the ID of the session to shadow.
/control	Allows control of the session when shadowing.
/noConsentPrompt	Allows shadowing without user consent.
/?	Displays help at the command prompt.

Remarks

- Default.rdp is stored for each user as a hidden file in the user's **Documents** folder.
- User created **.rdp** files are saved by default in the user's **Documents** folder, but can be saved anywhere.
- To span across monitors, the monitors must use the same resolution and must be aligned horizontally (that is, side-by-side). There's currently no support for spanning multiple monitors vertically on the client system.

Examples

To connect to a session in full-screen mode, type:

```
```

```
mstsc /f
```

or

```
mstsc /v:computer1 /f
```

To assign width/height, type:

```
mstsc /v:computer1 /w:1920 /h:1080
```

To open a file called *filename.rdp* for editing, type:

```
mstsc /edit filename.rdp
```

Related links

- Command-Line Syntax Key

nbtstat

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. This command also allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, this command displays Help information.

This command is available only if the Internet Protocol (TCP/IP) protocol is installed as a component in the properties of a network adapter in Network Connections.

Syntax

```
nbtstat [/a <remotename>] [/A <IPaddress>] [/c] [/n] [/r] [/R] [/RR] [/s]
[/S] [<interval>]
```

Parameters

Parameter	Description
/a `<remotename>`	Displays the NetBIOS name table of a remote computer, where *remotename* is the NetBIOS computer name of the remote computer. The NetBIOS name table is the list of NetBIOS names that corresponds to NetBIOS applications running on that computer.
/A `<IPaddress>`	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer.
/c	Displays the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses.
/n	Displays the NetBIOS name table of the local computer. The status of **registered** indicates that the name is registered either by broadcast or with a WINS server.
/r	Displays NetBIOS name resolution statistics.

Parameter	Description
/R	Purges the contents of the NetBIOS name cache and then reloads the pre-tagged entries from the **Lmhosts** file.
/RR	Releases and then refreshes NetBIOS names for the local computer that is registered with WINS servers.
/s	Displays NetBIOS client and server sessions, attempting to convert the destination IP address to a name.
/S	Displays NetBIOS client and server sessions, listing the remote computers by destination IP address only.
`<interval>`	Displays selected statistics, pausing the number of seconds specified in *interval* between each display. Press CTRL+C to stop displaying statistics. If this parameter is omitted, **nbtstat** prints the current configuration information only once.
/?	Displays help at the command prompt.

Remarks

- The **nbtstat** command-line parameters are case-sensitive.
- The column headings generated by the **nbtstat** command, include:

Heading	Description
Input	The number of bytes received.
Output	The number of bytes sent.
In/Out	Whether the connection is from the computer (outbound) or from another computer to the local computer (inbound).
Life	The remaining time that a name table cache entry will live before it is purged.
Local Name	The local NetBIOS name associated with the connection.
Remote Host	The name or IP address associated with the remote computer.
`<03>`	The last byte of a NetBIOS name converted to hexadecimal. Each NetBIOS name is 16 characters long. This last byte often has special significance because the same name might be present several times on a computer, differing only in the last byte. For example, `<20>` is a space in ASCII text.
type	The type of name. A name can either be a unique name or a group name.

Heading	Description
Status	Whether the NetBIOS service on the remote computer is running (registered) or a duplicate computer name has registered the same service (Conflict).
State	The state of NetBIOS connections.

- The possible NetBIOS connection states, include:

State	Description
Connected	A session has been established.
listening	This endpoint is available for an inbound connection.
Idle	This endpoint has been opened but cannot receive connections.
Connecting	A session is in the connecting phase and the name-to-IP address mapping of the destination is being resolved.
Accepting	An inbound session is currently being accepted and will be connected shortly.
Reconnecting	A session is trying to reconnect (it failed to connect on the first attempt).
Outbound	A session is in the connecting phase and the TCP connection is currently being created.
Inbound	An inbound session is in the connecting phase.
Disconnecting	A session is in the process of disconnecting.
Disconnected	The local computer has issued a disconnect and it is waiting for confirmation from the remote system.

Examples

To display the NetBIOS name table of the remote computer with the NetBIOS computer name of *CORP07*, type:

```
nbtstat /a CORP07
```

To display the NetBIOS name table of the remote computer assigned the IP address of *10.0.0.99*, type:

```
```

```
nbtstat /A 10.0.0.99
```

To display the NetBIOS name table of the local computer, type:

```
nbtstat /n
```

To display the contents of the local computer NetBIOS name cache, type:

```
nbtstat /c
```

To purge the NetBIOS name cache and reload the pre-tagged entries in the local *Lmhosts* file, type:

```
nbtstat /R
```

To release the NetBIOS names registered with the WINS server and re-register them, type:

```
nbtstat /RR
```

To display NetBIOS session statistics by IP address every five seconds, type:

```
nbtstat /S 5
```

Related links

- Command-Line Syntax Key

netcfg

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Installs the Windows Preinstallation Environment (WinPE), a lightweight version of Windows used to deploy workstations.

Syntax

```
netcfg [/v] [/e] [/winpe] [/l ] /c /i
```

Parameters

Parameter	Description
/v	Runs in verbose (detailed) mode.
/e	Uses servicing environment variables during install and uninstall.
/winpe	Installs TCP/IP, NetBIOS, and Microsoft Client for Windows preinstallation environment (WinPE).
/l	Provides the location of the INF file.
/c	Provides the class of the component to be installed; **protocol**, **service**, or **client**.
/i `<comp-ID>`	Provides the component ID.
/s	Provides the type of components to show, including **\ta** for adapters or **n** for net components.
/b	Displays the binding paths, when followed by a string containing the name of the path.
/q `<comp-ID>`	Queries whether component ID is installed
/u `<comp-ID>`	Uninstalls the component ID.

Parameter	Description
/m	Outputs the binding map to NetworkBindingMap.txt in the current directory. Using with /v will also display the binding map to the console.
/d	Performs a cleanup on all networking devices. This will require a reboot.
/x	Performs a cleanup on networking devices, skipping those without physical object names. This will require a reboot.
/?	Displays help at the command prompt.

Examples

To install the protocol *example* using c:\oemdir\example.inf, type:

```
netcfg /l c:\oemdir\example.inf /c p /i example
```

To install the *MS_Server* service, type:

```
netcfg /c s /i MS_Server
```

To install TCP/IP, NetBIOS and Microsoft Client for Windows preinstallation environment, type:

```
netcfg /v /winpe
```

To display if component *MS_IPX* is installed, type:

```
netcfg /q MS_IPX
```

To uninstall component *MS_IPX*, type:

```
netcfg /u MS_IPX
```

To show all installed net components, type:

```
netcfg /s n
```

To display binding paths containing *MS_TCPIP*, type:

```
netcfg /b ms_tcpip
```

Related links

- Command-Line Syntax Key

net print

Article • 03/21/2024

> **Important**
>
> This command has been deprecated. However, you can perform many of the same tasks using the prnjobs command, Windows Management Instrumentation (WMI), PrintManagement in Powershell.

Displays information about a specified printer queue or a specified print job, or controls a specified print job.

Syntax

```
net print {\\<computername>\<sharename> | \\<computername> <jobnumber>
[/hold | /release | /delete]} [help]
```

Parameters

Expand table

Parameters	Description
`\\<computername>\<sharename>`	Specifies (by name) the computer and print queue about which you want to display information.
`\\<computername>`	Specifies (by name) the computer that hosts the print job you want to control. If you do not specify a computer, the local computer is assumed. Requires the `<jobnumber>` parameter.
`<jobnumber>`	Specifies the number of the print job you want to control. This number is assigned by the computer that hosts the print queue where the print job is sent. After a computer assigns a number to a print job, that number is not assigned to any other print jobs in any queue hosted by that computer. Required when using the `\\<computername>` parameter.
`[/hold | /release | /delete]`	Specifies the action to take with the print job. If you specify a job number, but don't specify any action, information about the print job is displayed. • **/hold** - Delays the job, allowing other print jobs to bypass it until it is released.

Parameters	Description
	• **/release** - Releases a print job that has been delayed. • **/delete** - Removes a print job from a print queue.
help	Displays help at the command prompt.

Remarks

- The `net print\\<computername>` command displays information about print jobs in a shared printer queue. The following is an example of a report for all print jobs in a queue for a shared printer named *LASER*:

```
printers at \\PRODUCTION
Name               Job #      Size      Status
-----------------------------
LASER Queue        3 jobs               *printer active*
USER1          84        93844      printing
USER2          85        12555      Waiting
USER3          86        10222      Waiting
```

- The following is an example of a report for a print job:

```
Job #            35
Status           Waiting
Size             3096
remark
Submitting user  USER2
Notify           USER2
Job data type
Job parameters
additional info
```

Examples

To list the contents of the *Dotmatrix* print queue on the *Production* computer, type:

```
net print \\Production\Dotmatrix
```

To display information about job number *35* on the *Production* computer, type:

```
net print \\Production 35
```

To delay job number *263* on the *Production* computer, type:

```
net print \\Production 263 /hold
```

To release job number *263* on the *Production* computer, type:

```
net print \\Production 263 /release
```

Related links

- Command-Line Syntax Key
- print command reference
- prnjobs command
- Windows Management Instrumentation (WMI)
- PrintManagement in Powershell

netsh

Article • 06/16/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016

The Network Shell command-line scripting utility that allows you to, either locally or remotely, display or modify the network configuration of a currently running computer. You can start this utility at the command prompt or in Windows PowerShell.

Syntax

```
netsh [-a <Aliasfile>][-c <Context>][-r <Remotecomputer>][-u [<domainname>\
<username>][-p <Password> | [{<NetshCommand> | -f <scriptfile>}]
```

Parameters

Parameter	Description
-a `<Aliasfile>`	Specifies that you are returned to the netsh prompt after running Aliasfile and the name of the text file that contains one or more netsh commands.
-c `<Context>`	Specifies that netsh enters the specified netsh context and the netsh context to enter.
-r `<Remotecomputer>`	Specifies the remote computer to configure. **Important:** If you use this parameter, you must make sure the Remote Registry service is running on the remote computer. If it isn't running, Windows displays a “Network Path Not Found” error message.
-u `<domainname>\<username>`	Specifies the domain and user account name to use while running the netsh command under a user account. If you omit the domain, the local domain is used by default.
-p `<Password>`	Specifies the password for the user account specified by the `-u <username>` parameter.
`<NetshCommand>`	Specifies the netsh command to run.
-f `<scriptfile>`	Exits the netsh command after running the specified script file.
/?	Displays help at the command prompt.

Remarks

- If you specify **-r** followed by another command, netsh runs the command on the remote computer and then returns to the Cmd.exe command prompt. If you specify **-r** without another command, netsh opens in remote mode. The process is similar to using **set machine** at the Netsh command prompt. When you use **-r**, you set the target computer for the current instance of netsh only. After you exit and reenter netsh, the target computer is reset as the local computer. You can run netsh commands on a remote computer by specifying a computer name stored in WINS, a UNC name, an Internet name to be resolved by the DNS server, or an IP address.

- If your string value contains spaces between characters, you must enclose the string value in quotation marks. For example, `-r "contoso remote device"`

Related links

- Command-Line Syntax Key
- Network shell (netsh)

netstat

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, this command displays active TCP connections.

> **ⓘ Important**
>
> This command is available only if the Internet Protocol (TCP/IP) protocol is installed as a component in the properties of a network adapter in Network Connections.

Syntax

```
netstat [-a] [-b] [-e] [-n] [-o] [-p <Protocol>] [-r] [-s] [<interval>]
```

Parameters

Parameter	Description
-a	Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
-b	Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
-e	Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with **-s**.
-n	Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names.

Parameter	Description
-o	Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with **-a**, **-n**, and **-p**.
-p `<Protocol>`	Shows connections for the protocol specified by *Protocol*. In this case, the *Protocol* can be tcp, udp, tcpv6, or udpv6. If this parameter is used with **-s** to display statistics by protocol, *Protocol* can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
-s	Displays statistics by protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol is installed, statistics are shown for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols.
-r	Displays the contents of the IP routing table. This is equivalent to the route print command.
`<interval>`	Redisplays the selected information every *interval* seconds. Press CTRL+C to stop the redisplay. If this parameter is omitted, this command prints the selected information only once.
/?	Displays help at the command prompt.

Remarks

- The **netstat** command provides statistics for the following:

Parameter	Description
Proto	The name of the protocol (TCP or UDP).
Local address	The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the **-n** parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
Foreign address	The IP address and port number of the remote computer to which the socket is connected. The names that corresponds to the IP address and the port are shown unless the **-n** parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).

Parameter	Description
State	Indicates the state of a TCP connection, including: ○ CLOSE_WAIT ○ CLOSED ○ ESTABLISHED ○ FIN_WAIT_1 ○ FIN_WAIT_2 ○ LAST_ACK ○ LISTEN ○ SYN_RECEIVED ○ SYN_SEND ○ TIMED_WAIT

Examples

To display both the Ethernet statistics and the statistics for all protocols, type:

```
netstat -e -s
```

To display the statistics for only the TCP and UDP protocols, type:

```
netstat -s -p tcp udp
```

To display active TCP connections and the process IDs every 5 seconds, type:

```
netstat -o 5
```

To display active TCP connections and the process IDs using numerical form, type:

```
netstat -n -o
```

Related links

- Command-Line Syntax Key

nfsadmin

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

A command-line utility that administers Server for NFS or Client for NFS on the local or remote computer running Microsoft Services for Network File System (NFS). Used without parameters, nfsadmin server displays the current Server for NFS configuration settings and nfsadmin client displays the current Client for NFS configuration settings.

Syntax

```
nfsadmin server [computername] [-u Username [-p Password]] -l
nfsadmin server [computername] [-u Username [-p Password]] -r {client | all}
nfsadmin server [computername] [-u Username [-p Password]] {start | stop}
nfsadmin server [computername] [-u Username [-p Password]] config
option[...]
nfsadmin server [computername] [-u Username [-p Password]] creategroup
<name>
nfsadmin server [computername] [-u Username [-p Password]] listgroups
nfsadmin server [computername] [-u Username [-p Password]] deletegroup
<name>
nfsadmin server [computername] [-u Username [-p Password]] renamegroup
<oldname> <newname>
nfsadmin server [computername] [-u Username [-p Password]] addmembers
<hostname>[...]
nfsadmin server [computername] [-u Username [-p Password]] listmembers
nfsadmin server [computername] [-u Username [-p Password]] deletemembers
<hostname><groupname>[...]
nfsadmin client [computername] [-u Username [-p Password]] {start | stop}
nfsadmin client [computername] [-u Username [-p Password]] config
option[...]
```

General Parameters

Parameter	Description
computername	Specifies the remote computer you want to administer. You can specify the computer using a Windows Internet Name Service (WINS) name or a Domain Name System (DNS) name, or by Internet Protocol (IP) address.

Parameter	Description
-u Username	Specifies the user name of the user whose credentials are to be used. It might be necessary to add the domain name to the user name in the form *domain\username*.
-p Password	Specifies the password of the user specified using the **-u** option. If you specify the **-u** option but omit the **-p** option, you are prompted for the user's password.

Server for NFS-related parameters

Parameter	Description
-l	Lists all locks held by clients.
-r `{client|all}`	Releases the locks held by a client or, if all is specified, by all clients.
start	Starts the Server for NFS service.
stop	Stops the Server for NFS service.
config	Specifies general settings for Server for NFS. You must supply at least one of the following options with the **config** command argument: • **mapsvr=**`<server>` - Sets server as the User Name Mapping server for Server for NFS. Although this option continues to be supported for compatibility with previous versions, you should use the sfuadmin utility instead. • **auditlocation=**`{eventlog|file|both|none}` - Specifies whether events will be audited and where the events will be recorded. One of the following arguments is required: ◦ **eventlog** - Specifies that audited events will be recorded only in the Event Viewer application log. ◦ **file** - Specifies that audited events will be recorded only in the file specified by `config fname`. ◦ **both** - Specifies that audited events will be recorded in the Event Viewer application log as well as the file specified by `config fname`. ◦ **none** - Specifies that events aren't audited. • **fname=**`<file>` - Sets the file specified by file as the audit file. The default is **%sfudir%\log\nfssvr.log**. • **fsize=**`<size>` - Sets size as the maximum size in megabytes of the audit file. The default maximum size is **7 MB**. • `audit=[+|-]mount [+|-]read [+|-]write [+|-]create [+|-]delete [+|-]locking [+|-]all` - Specifies the events to be logged. To start logging an event, type a plus sign (+) before the event name; to stop logging an event, type a minus sign (-) before the event name. If the sign is omitted, the + sign is assumed. Don't use **all** with any other event name.

Parameter	Description
	• **lockperiod=** `<seconds>` - Specifies the number of seconds that Server for NFS will wait to reclaim locks after a connection to Server for NFS has been lost and then reestablished or after the Server for NFS service has been restarted. • **portmapprotocol=** `{TCP|UDP|TCP+UDP}` - Specifies which transport protocols Portmap supports. The default setting is **TCP+UDP**. • **mountprotocol=** `{TCP|UDP|TCP+UDP}` - Specifies which transport protocols mount supports. The default setting is **TCP+UDP**. • **nfsprotocol=** `{TCP|UDP|TCP+UDP}` - Specifies which transport protocols Network File System (NFS) supports. The default setting is **TCP+UDP** • **nlmprotocol=** `{TCP|UDP|TCP+UDP}` - Specifies which transport protocols Network Lock Manager (NLM) supports. The default setting is **TCP+UDP**. • **nsmprotocol=** `{TCP|UDP|TCP+UDP}` - Specifies which transport protocols Network Status Manager (NSM) supports. The default setting is **TCP+UDP**. • **enableV3=** `{yes|no}` - Specifies whether NFS version 3 protocols will be supported. The default setting is **yes**. • **renewauth=** `{yes|no}` - Specifies whether client connections will be required to be reauthenticated after the period specified by config renewauthinterval. The default setting is **no**. • **renewauthinterval=** `<seconds>` - Specifies the number of seconds that elapse before a client is forced to be reauthenticated if `config renewauth` is set to **yes**. The default value is **600 seconds**. • **dircache=** `<size>` - Specifies the size in kilobytes of the directory cache. The number specified as size must be a multiple of 4 between 4 and 128. The default directory cache size is **128 KB**. • **translationfile=** `<file>` - Specifies a file containing mapping information for replacing characters in the names of files when moving them from Windows-based to UNIX-based file systems. If file is not specified, then file name character translation is disabled. If the value of **translationfile** is changed, you must restart the server for the change to take effect. • **dotfileshidden=** `{yes|no}` - Specifies whether files with names beginning with a period (.) are marked as hidden in the Windows file system, and consequently hidden from NFS clients. The default setting is **no**. • **casesensitivelookups=** `{yes|no}` - Specifies whether directory lookups are case sensitive (require exact matching of character case). You must also disable Windows kernel case-insensitivity to support case-sensitive file names. To support case-sensitivity, change the **DWord** value of the registry key, `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\kernel`, to **0**. • **ntfscase=** `{lower|upper|preserve}` - Specifies whether the case of characters in the names of files in the NTFS file system will be returned in lowercase, uppercase, or in the form stored in the directory. The default setting is **preserve**. This setting can't be changed if **casesensitivelookups** is set to **yes**.

Parameter	Description
creategroup `<name>`	Creates a new client group, giving it the specified name.
listgroups	Displays the names of all client groups.
deletegroup `<name>`	Removes the client group specified by name.
renamegroup `<oldname>` `<newname>`	Changes the name of the client group specified by *oldname* to *newname*.
addmembers `<hostname>` `[...]`	Adds a *host* to the client group specified by *name*.
listmembers `<name>`	Lists the host computers in the client group specified by *name*.
deletemembers `<hostname>` `<groupname>` `[...]`	Removes the client specified by *host* from the client group specified by *group*.

Client for NFS-related parameters

Parameter	Description
start	Starts the Client for NFS service.
stop	Stops the Client for NFS service.

Parameter	Description
config	Specifies general settings for Client for NFS. You must supply at least one of the following options with the **config** command argument: • **fileaccess=**`<mode>` - Specifies the default permission mode for files created on Network File System (NFS) servers. The **mode** argument consists of a three digit number, from 0 to 7 (inclusive), which represent the default permissions granted the user, group, and others. The digits translate to UNIX-style permissions as follows: *0=none*, *1=x (execute)*, *2=w (write only)*, *3=wx (write and execute)*, *4=r (read only)*, *5=rx (read and execute)*, *6=rw (read and write)*, and *7=rwx (read, write, and execute)*. For example, `fileaccess=750` gives read, write, and execute permissions to the owner, read and execute permissions to the group, and no access permission to others. • **mapsvr=**`<server>` - Sets server as the User Name Mapping server for Client for NFS. Although this option continues to be supported for compatibility with previous versions, you should use the sfuadmin utility instead. • **mtype=**`{hard|soft}` - Specifies the default mount type. For a hard mount, Client for NFS continues to retry a failed RPC until it succeeds. For a soft mount, Client for NFS returns failure to the calling application after retrying the call the number of times specified by the retry option. • **retry=**`<number>` - Specifies the number of times to try to make a connection for a soft mount. This value must be from 1 to 10, inclusive. The default is **1**. • **timeout=**`<seconds>` - Specifies the number of seconds to wait for a connection (remote procedure call). This value must be *0.8*, *0.9*, or an integer from *1 to 60*, inclusive. The default is **0.8**. • **protocol=**`{TCP|UDP|TCP+UDP}` - Specifies which transport protocols the client supports. The default setting is **TCP+UDP**. • **rsize=**`<size>` -Specifies the size, in kilobytes, of the read buffer. This value can be *0.5, 1, 2, 4, 8, 16,* or *32*. The default is **32**. • **wsize=**`<size>` - Specifies the size, in kilobytes, of the write buffer. This value can be *0.5, 1, 2, 4, 8, 16,* or *32*. The default is **32**. • **perf=default** - Restores the following performance settings to default values, *mtype*, *retry*, *timeout*, *rsize*, or *wsize*.

Examples

To stop Server for NFS or Client for NFS, type:

```
nfsadmin server stop
nfsadmin client stop
```

To start Server for NFS or Client for NFS, type:

```
nfsadmin server start
nfsadmin client start
```

To set Server for NFS to not be case-sensitive, type:

```
nfsadmin server config casesensitive=no
```

To set Client for NFS to be case-sensitive, type:

```
nfsadmin client config casesensitive=yes
```

To display all the current Server for NFS or Client for NFS options, type:

```
nfsadmin server config
nfsadmin client config
```

Related links

- Command-Line Syntax Key
- NFS cmdlets reference

nfsshare

Article • 02/03/2023

Controls Network File System (NFS) shares. Used without parameters, this command displays all Network File System (NFS) shares exported by Server for NFS.

Syntax

```
nfsshare <sharename>=<drive:path> [-o <option=value>...]
nfsshare {<sharename> | <drive>:<path> | * } /delete
```

Parameters

Parameter	Description
-o anon=`{yes|no}`	Specifies whether anonymous (unmapped) users can access the share directory.
-o rw=`[<host>[:<host>]...]`	Provides read-write access to the shared directory by the hosts or client groups specified by *host*. You must separate host and group names with a colon (:). If *host* isn't specified, all hosts and client groups (except those specified with the **ro** option) get read-write access. If neither the **ro** nor the **rw** option is set, all clients have read-write access to the shared directory.
-o ro=`[<host>[:<host>]...]`	Provides read-only access to the shared directory by the hosts or client groups specified by *host*. You must separate host and group names with a colon (:). If *host* isn't specified, all clients (except those specified with the **rw** option) get read-only access. If the **ro** option is set for one or more clients, but the **rw** option isn't set, only the clients specified with the **ro** option have access to the shared directory.

Parameter	Description
-o encoding=`{euc-jp|euc-tw|euc-kr|shift-jis|Big5|Ksc5601|Gb2312-80|Ansi)`	Specifies the language encoding to configure on an NFS share. You can use only one language on the share. This value can include any of the following values: • **euc-jp:** Japanese • **euc-tw:** Chinese • **euc-kr:** Korean • **shift-jis:** Japanese • **Big5:** Chinese • **Ksc5601:** Korean • **Gb2312-80:** Simplified Chinese • **Ansi:** ANSI-encoded
-o anongid=`<gid>`	Specifies that anonymous (unmapped) users access the share directory using *gid* as their group identifier (GID). The default is **-2**. The anonymous GID is used when reporting the owner of a file owned by an unmapped user, even if anonymous access is disabled.
-o anonuid=`<uid>`	Specifies that anonymous (unmapped) users access the share directory using *uid* as their user identifier (UID). The default is **-2**. The anonymous UID is used when reporting the owner of a file owned by an unmapped user, even if anonymous access is disabled.
-o root=`[<host>[:<host>]...]`	Provides root access to the shared directory by the hosts or client groups specified by *host*. You must separate host and group names with a colon (:). If *host* isn't specified, all clients get root access. If the **root** option isn't set, no clients have root access to the shared directory.
/delete	If *sharename* or `<drive>:<path>` is specified, this parameter deletes the specified share. If a wildcard (*) is specified, this parameter deletes all NFS shares.
/?	Displays help at the command prompt.

Remarks

- If *sharename* as the only parameter, this command lists the properties of the NFS share identified by *sharename*.
- If *sharename* and `<drive>:<path>` are used, this command exports the folder identified by `<drive>:<path>` as *sharename*. If you use the **/delete** option, the specified folder stops being available to NFS clients.

Related links

- Command-Line Syntax Key
- Services for Network File System Command Reference
- NFS cmdlets reference

nfsstat

Article • 02/03/2023

A command-line utility that displays statistical info about the Network File System (NFS) and Remote Procedure Call (RPC) calls. Used without parameters, this command displays all of the statistical data without resetting anything.

Syntax

```
nfsstat [-c][-s][-n][-r][-z][-m]
```

Parameters

Parameter	Description
-c	Displays only the client-side NFS and RPC and NFS calls sent and rejected by the client. To display NFS or RPC information only, combine this flag with the **-n** or **-r** parameter.
-s	Displays only the server-side NFS and RPC and NFS calls sent and rejected by the server. To display NFS or RPC information only, combine this flag with the **-n** or **-r** parameter.
-m	Displays information about mount flags set by mount options, mount flags internal to the system, and other mount information.
-n	Displays NFS information for both the client and server. To display only the NFS client or server information, combine this flag with the **-c** or **-s** parameter.
-r	Displays RPC information for both the client and server. To display only the RPC client or server information, combine this flag with the **-c** or **-s** parameter.
-z	Resets the call statistics. This flag is only available to the root user and can be combined with any of the other parameters to reset particular sets of statistics after displaying them.

Examples

To display information about the number of RPC and NFS calls sent and rejected by the client, type:

```
nfsstat -c
```

To display and print the client NFS call-related information, type:

```
nfsstat -cn
```

To display RPC call-related information for both the client and server, type:

```
nfsstat -r
```

To display information about the number of RPC and NFS calls received and rejected by the server, type:

```
nfsstat -s
```

To reset all call-related information to zero on the client and server, type:

```
nfsstat -z
```

Related links

- Command-Line Syntax Key
- Services for Network File System Command Reference
- NFS cmdlets reference

nlbmgr

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configure and manage your Network Load Balancing clusters and all cluster hosts from a single computer, using the Network Load Balancing Manager. You can also use this command to replicate the cluster configuration to other hosts.

You can start the Network Load Balancing Manager from the command-line using the command **nlbmgr.exe**, which is installed in the **systemroot\System32** folder.

Syntax

```
nlbmgr [/noping][/hostlist <filename>][/autorefresh <interval>][/help | /?]
```

Parameters

Parameter	Description
/noping	Prevents the Network Load Balancing Manager from pinging the hosts prior to trying to contact them through Windows Management Instrumentation (WMI). Use this option if you have disabled Internet Control Message Protocol (ICMP) on all available network adapters. If the Network Load Balancing Manager attempts to contact a host that isn't available, you'll experience a delay when using this option.
/hostlist `<filename>`	Loads the hosts specified in filename into the Network Load Balancing Manager.
/autorefresh `<interval>`	Causes the Network Load Balancing Manager to refresh its host and cluster information every `<interval>` seconds. If no interval is specified, the information is refreshed every 60 seconds.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- NetworkLoadBalancingClusters cmdlets reference

nslookup

Article • 09/12/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works. The nslookup command-line tool is available only if you have installed the TCP/IP protocol.

Syntax

```
nslookup [exit | finger | help | ls | lserver | root | server | set | view]
[options]
```

Parameters

Parameter	Description
nslookup exit	Exits the nslookup command-line tool.
nslookup finger	Connects with the finger server on the current computer.
nslookup help	Displays a short summary of subcommands.
nslookup ls	Lists information for a DNS domain.
nslookup lserver	Changes the default server to the specified DNS domain.
nslookup root	Changes the default server to the server for the root of the DNS domain name space.
nslookup server	Changes the default server to the specified DNS domain.
nslookup set	Changes configuration settings that affect how lookups function.
nslookup set all	Prints the current values of the configuration settings.

Parameter	Description
nslookup set class	Changes the query class. The class specifies the protocol group of the information.
nslookup set d2	Turns exhaustive Debugging mode on or off. All fields of every packet are printed.
nslookup set debug	Turns Debugging mode on or off.
nslookup set domain	Changes the default DNS domain name to the name specified.
nslookup set port	Changes the default TCP/UDP DNS name server port to the value specified.
nslookup set querytype	Changes the resource record type for the query.
nslookup set recurse	Tells the DNS name server to query other servers if it doesn't have the information.
nslookup set retry	Sets the number of retries.
nslookup set root	Changes the name of the root server used for queries.
nslookup set search	Appends the DNS domain names in the DNS domain search list to the request until an answer is received. This applies when the set and the lookup request contain at least one period, but do not end with a trailing period.
nslookup set srchlist	Changes the default DNS domain name and search list.
nslookup set timeout	Changes the initial number of seconds to wait for a reply to a request.
nslookup set type	Changes the resource record type for the query.
nslookup set vc	Specifies to use or not use a virtual circuit when sending requests to the server.
nslookup view	Sorts and lists the output of the previous **ls** subcommand or commands.

Remarks

- The nslookup command-line tool has two modes: interactive and noninteractive.

- If you need to look up only a single piece of data, or you're using nslookup in scripts, command lines, or PowerShell, use the noninteractive mode. In noninteractive mode, also called command mode, the first command line parameter is the name or IP address of the computer that you want to look up. The second parameter is the name or IP address of a DNS name server. If you omit the second argument, nslookup uses the default DNS name server.

- If you need to look up more than one piece of data or set several configurations, you can use interactive mode. To enter interactive mode, type a hyphen (-) instead of the first parameter in the nslookup command line. Enter the name or IP address of a DNS name server for the second parameter. If you omit the second argument, nslookup uses the default DNS name server. You can also invoke interactive mode by simply entering `nslookup` at the command prompt, and then entering names or IP addresses to search for in the interactive command line.

- Once you enter `nslookup -` or `nslookup` alone, the command prompt changes to the interactive prompt `>`. While in interactive mode, you can:
  - Enter names or IP addresses, `set` variables, and other options on separate lines.
  - Interrupt interactive commands at any time by pressing CTRL+B.
  - Exit, by entering `exit`.
  - Treat a built-in command as a computer name by preceding it with the escape character (`\`). An unrecognized command is interpreted as a computer name.

- If the computer to find is an IP address and the query is for an **A** or **PTR** resource record type, the name of the computer is returned.

- If the computer to find is a name and doesn't have a trailing period, the default DNS domain name is appended to the name. This behavior depends on the state of the following **set** subcommands: **domain**, **srchlist**, **defname**, and **search**.

- If the lookup request fails, the command-line tool provides one of the following error messages:

Error message	Description
timed out	The server didn't respond to a request after a certain amount of time and a certain number of retries. You can set the time-out period with the nslookup set timeout command. You can set the number of retries with the nslookup set retry command.
No response from server	No DNS name server is running on the server computer.

Error message	Description
No records	The DNS name server doesn't have resource records of the current query type for the computer, although the computer name is valid. The query type is specified with the nslookup set querytype command.
Nonexistent domain	The computer or DNS domain name doesn't exist.
Connection refused or Network is unreachable	The connection to the DNS name server or finger server couldn't be made. This error commonly occurs with the **ls** and **finger** requests.
Server failure	The DNS name server found an internal inconsistency in its database and couldn't return a valid answer.
Refused	The DNS name server refused to service the request.
format error	The DNS name server found that the request packet wasn't in the proper format. It may indicate an error in **nslookup**.

Examples

In nslookup noninteractive mode, you specify parameters and options in the Windows command line or script. In interactive mode, you specify arguments and options on separate lines at the interactive command prompt.

Noninteractive mode

In nslookup noninteractive mode, the first parameter is the computer to find, and the second parameter is the DNS name server to use. If you don't specify a second parameter, nslookup uses the default DNS name server. The following examples use `nslookup` in noninteractive mode.

- The following example looks up the IP addresses for the domain name `mydomain.com` on the DNS name server at `1.1.1.1`:

  Windows Command Prompt

  ```
  nslookup mydomain.com 1.1.1.1
  ```

- The following example looks up the domain name for the IP address `4.4.4.4` on the default DNS name server:

  Windows Command Prompt

```
nslookup 4.4.4.4
```

- To specify options, you can use `nslookup -<option>`. For example, the following command turns on the nslookup `debug` option to get more information about packets sent.

  Windows Command Prompt

  ```
  nslookup -debug mydomain.com
  ```

- To return certain types of records or information, use the `-type=<resourcerecordtype>` option. For example, the following command returns only IPv6 record types:

  Windows Command Prompt

  ```
  nslookup -type=AAAA mydomain.com
  ```

- You can combine options and resource record type queries in command lines. The following example enables debug output, retrieves both IPv6 and IPv4 addresses, doesn't attempt to use the search domain, uses recursive lookup, and uses the 1.1.1.1 DNS lookup server:

  Windows Command Prompt

  ```
  nslookup -debug -type=A+AAAA -nosearch -recurse mydomain.com 1.1.1.1
  ```

Interactive mode

To use interactive mode, enter `-` instead of the first parameter of a nslookup command line, or simply enter `nslookup`. The command prompt then changes to the interactive prompt `>`. The following examples show interactive mode commands.

- The following command places nslookup in interactive mode and sets `1.1.1.1` as the default DNS lookup server:

  Windows Command Prompt

  ```
  nslookup - 1.1.1.1
  ```

- The following command at the interactive prompt returns nslookup option and parameter settings for the current server:

  Windows Command Prompt

  ```
  set all
  ```

- The following command at the interactive prompt returns the IP addresses for `mydomain.com`:

  Windows Command Prompt

  ```
  mydomain.com
  ```

- The following command at the interactive prompt changes the default DNS name server to `4.4.4.4`:

  Windows Command Prompt

  ```
  server 4.4.4.4
  ```

- The following command at the interactive prompt sets the query resource record type to `HINFO`:

  Windows Command Prompt

  ```
  set type=HINFO
  ```

- The following command at the interactive prompt exits interactive mode and returns to the Windows command prompt:

  Windows Command Prompt

  ```
  exit
  ```

Related links

- Command-Line Syntax Key

nslookup /exit

Article • 02/03/2023

Exits the nslookup command-line tool.

Syntax

```
nslookup /exit
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup /finger

Article • 02/03/2023

Connects with the finger server on the current device.

Syntax

```
finger [<username>] [{[>] <filename> | [>>] <filename>}]
```

Parameters

Parameter	Description
`<username>`	Specifies the name of the user to look up.
`<filename>`	Specifies a file name in which to save the output. You can use the greater than (`>`) and double greater than (`>>`) characters to redirect the output in the usual manner.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup help

Article • 02/03/2023

Displays the subcommand help text.

Syntax

```
help
```

```
?
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup ls

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Lists DNS domain information.

Syntax

```
ls [<option>] <DNSdomain> [{[>] <filename>|[>>] <filename>}]
```

Parameters

Parameter	Description
`<option>`	The valid options include: • **-t:** Lists all records of the specified type. For more information, see nslookup set querytype. • **-a:** Lists aliases of computers in the DNS domain. This parameter is the same as **-t CNAME** • **-d:** Lists all records for the DNS domain. This parameter is the same as **-t ANY** • **-h:** Lists CPU and operating system information for the DNS domain. This parameter is the same as **-t HINFO** • **-s:** Lists well-known services of computers in the DNS domain. This parameter is the same as **-t WKS**.
`<DNSdomain>`	Specifies the DNS domain for which you want information.
`<filename>`	Specifies a file name to use for the saved output. You can use the greater than (`>`) and double greater than (`>>`) characters to redirect the output in the usual manner.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Remarks

- The default output of this command includes computer names and their associated IP addresses.
- If your output is directed to a file, hash marks are added for every 50 records received from the server.

Related links

- Command-Line Syntax Key
- nslookup set querytype

nslookup lserver

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the initial server to the specified Domain Name System (DNS) domain.

This command uses the initial server to look up the information about the specified DSN domain. If you want to lookup information using the current default server, use the nslookup server command.

Syntax

```
lserver <DNSdomain>
```

Parameters

Parameter	Description
`<DNSdomain>`	Specifies the DNS domain for the initial server.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- nslookup server

nslookup root

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the default server to the server for the root of the Domain Name System (DNS) domain name space. Currently, the ns.nic.ddn.mil name server is used. You can change the name of the root server using the nslookup set root command.

> **Note**
>
> This command is the same as `lserver ns.nic.ddn.mil`.

Syntax

```
root
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- nslookup set root

nslookup server

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the default server to the specified Domain Name System (DNS) domain.

This command uses the current default server to look up the information about the specified DNS domain. If you want to lookup information using the initial server, use the nslookup lserver command.

Syntax

```
server <DNSdomain>
```

Parameters

Parameter	Description
`<DNSdomain>`	Specifies the DNS domain for the default server.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- nslookup lserver

nslookup set

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes configuration settings that affect how lookups function.

Syntax

```
set all [class | d2 | debug | domain | port | querytype | recurse | retry |
root | search | srchlist | timeout | type | vc] [options]
```

Parameters

Parameter	Description
nslookup set all	Lists all current settings.
nslookup set class	Changes the query class, which specifies the protocol group of the information.
nslookup set d2	Turns the verbose debugging mode on or off.
nslookup set debug	Turns off debugging mode completely.
nslookup set domain	Changes the default Domain Name System (DNS) domain name to the specified name.
nslookup set port	Changes the default TCP/UDP Domain Name System (DNS) name server port to the specified value.
nslookup set querytype	Changes the resource record type for the query.
nslookup set recurse	Tells the Domain Name System (DNS) name server to query other servers if it doesn't find any information.

Parameter	Description
nslookup set retry	Sets the number of retries.
nslookup set root	Changes the name of the root server used for queries.
nslookup set search	Appends the Domain Name System (DNS) domain names in the DNS domain search list to the request until an answer is received.
nslookup set srchlist	Changes the default Domain Name System (DNS) domain name and search list.
nslookup set timeout	Changes the initial number of seconds to wait for a reply to a lookup request.
nslookup set type	Changes the resource record type for the query.
nslookup set vc	Specifies whether to use a virtual circuit when sending requests to the server.

Related links

- Command-Line Syntax Key

nslookup set all

Article • 02/03/2023

Outputs the current configuration setting values, including the default server and computer (the host).

Syntax

```
set all
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup set class

Article • 02/03/2023

Changes the query class. The class specifies the protocol group of the information.

Syntax

```
set class=<class>
```

Parameters

Parameter	Description
`<class>`	The valid values include: • **IN:** Specifies the Internet class. This is the default value. • **CHAOS:** Specifies the Chaos class. • **HESIOD:** Specifies the MIT Athena Hesiod class. • **ANY:** Specifies to use any of the previously listed values.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup set d2

Article • 02/03/2023

Turns the verbose debugging mode on or off. All fields of every packet are printed.

Syntax

```
set [no]d2
```

Parameters

Parameter	Description
nod2	Turns off the verbose debugging mode. This is the default value.
d2	Turns on the verbose debugging mode.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup set debug

Article • 02/03/2023

Turns debugging mode on or off.

Syntax

```
set [no]debug
```

Parameters

Parameter	Description
nodebug	Turns off debugging mode. This is the default value.
debug	Turns on debugging mode. By turning debugging mode on, you can view more information about the packet sent to the server and the resulting answer.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup set domain

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the default Domain Name System (DNS) domain name to the specified name.

Syntax

```
set domain=<domainname>
```

Parameters

Parameter	Description
`<domainname>`	Specifies a new name for the default DNS domain name. The default value is the name of the host.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Remarks

- The default DNS domain name is appended to a lookup request depending on the state of the **defname** and **search** options.
- The DNS domain search list contains the parents of the default DNS domain if it has at least two components in its name. For example, if the default DNS domain is mfg.widgets.com, the search list is named both mfg.widgets.com and widgets.com.
- Use the nslookup set srchlist command to specify a different list and the nslookup set all command to display the list.

Related links

- Command-Line Syntax Key

- nslookup set srchlist
- nslookup set all

nslookup set port

Article • 02/03/2023

Changes the default TCP/UDP Domain Name System (DNS) name server port to the specified value.

Syntax

```
set port=<port>
```

Parameters

Parameter	Description
`<port>`	Specifies the new value for the default TCP/UDP DNS name server port. The default port is **53**.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup set querytype

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the resource record type for the query. For information about resource record types, see Request for Comment (Rfc) 1035 .

> **Note**
>
> This command is the same as the **nslookup set type** command.

Syntax

```
set querytype=<resourcerecordtype>
```

Parameters

Parameter	Description

Parameter	Description
`<resourcerecordtype>`	Specifies a DNS resource record type. The default resource record type is **A**, but you can use any of the following values: • **A:** Specifies a computer's IP address. • **ANY:** Specifies a computer's IP address. • **CNAME:** Specifies a canonical name for an alias. • **GID** Specifies a group identifier of a group name. • **HINFO:** Specifies a computer's CPU and type of operating system. • **MB:** Specifies a mailbox domain name. • **MG:** Specifies a mail group member. • **MINFO:** Specifies mailbox or mail list information. • **MR:** Specifies the mail rename domain name. • **MX:** Specifies the mail exchanger. • **NS:** Specifies a DNS name server for the named zone. • **PTR:** Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information. • **SOA:** Specifies the start-of-authority for a DNS zone. • **TXT:** Specifies the text information. • **UID:** Specifies the user identifier. • **UINFO:** Specifies the user information. • **WKS:** Describes a well-known service.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- nslookup set type

nslookup set recurse

Article • 02/03/2023

Tells the Domain Name System (DNS) name server to query other servers if it can't find the information on the specified server.

Syntax

```
set [no]recurse
```

Parameters

Parameter	Description
norecurse	Stops the Domain Name System (DNS) name server from querying other servers if it can't find the information on the specified server.
recurse	Tells the Domain Name System (DNS) name server to query other servers if it can't find the information on the specified server. This is the default value.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup set retry

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

If a reply isn't received within a certain amount of time, the time-out period is doubled, and the request is resent. This command sets the number of times a request is resent to a server for information, before giving up.

> **Note**
>
> To change the length of time before the request times out, use the **nslookup set timeout** command.

Syntax

```
set retry=<number>
```

Parameters

Parameter	Description
`<number>`	Specifies the new value for the number of retries. The default number of retries is **4**.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- nslookup set timeout

nslookup set root

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the name of the root server used for queries.

> **Note**
>
> This command supports the **nslookup root** command.

Syntax

```
set root=<rootserver>
```

Parameters

Parameter	Description
`<rootserver>`	Specifies the new name for the root server. The default value is **ns.nic.ddn.mil**.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- nslookup root

nslookup set search

Article • 02/03/2023

Appends the Domain Name System (DNS) domain names in the DNS domain search list to the request until an answer is received. This applies when the set and the lookup request contain at least one period, but do not end with a trailing period.

Syntax

```
set [no]search
```

Parameters

Parameter	Description
nosearch	Stops appending the Domain Name System (DNS) domain names in the DNS domain search list for the request.
search	Appends the Domain Name System (DNS) domain names in the DNS domain search list for the request until an answer is received. This is the default value.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup set srchlist

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the default Domain Name System (DNS) domain name and search list. This command overrides the default DNS domain name and search list of the nslookup set domain command.

Syntax

```
set srchlist=<domainname>[/...]
```

Parameters

Parameter	Description
`<domainname>`	Specifies new names for the default DNS domain and search list. The default domain name value is based on the host name. You can specify a maximum of six names separated by slashes (/).
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Remarks

- Use the nslookup set all command to display the list.

Examples

To set the DNS domain to *mfg.widgets.com* and the search list to the three names:

```
set srchlist=mfg.widgets.com/mrp2.widgets.com/widgets.com
```

Related links

- Command-Line Syntax Key
- nslookup set domain
- nslookup set all

nslookup set timeout

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the initial number of seconds to wait for a reply to a lookup request. If a reply isn't received within the specified amount of time, the time-out period is doubled, and the request is resent. Use the nslookup set retry command to determine the number of times to try to send the request.

Syntax

```
set timeout=<number>
```

Parameters

Parameter	Description
`<number>`	Specifies the number of seconds to wait for a reply. The default number of seconds to wait is **5**.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Examples

To set the timeout for getting a response to 2 seconds:

```
set timeout=2
```

Related links

- Command-Line Syntax Key

- nslookup set retry

nslookup set type

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the resource record type for the query. For information about resource record types, see Request for Comment (Rfc) 1035 .

> **Note**
>
> This command is the same as the **nslookup set querytype** command.

Syntax

```
set type=<resourcerecordtype>
```

Parameters

Parameter	Description

Parameter	Description
`<resourcerecordtype>`	Specifies a DNS resource record type. The default resource record type is **A**, but you can use any of the following values: • **A:** Specifies a computer's IP address. • **ANY:** Specifies a computer's IP address. • **CNAME:** Specifies a canonical name for an alias. • **GID** Specifies a group identifier of a group name. • **HINFO:** Specifies a computer's CPU and type of operating system. • **MB:** Specifies a mailbox domain name. • **MG:** Specifies a mail group member. • **MINFO:** Specifies mailbox or mail list information. • **MR:** Specifies the mail rename domain name. • **MX:** Specifies the mail exchanger. • **NS:** Specifies a DNS name server for the named zone. • **PTR:** Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information. • **SOA:** Specifies the start-of-authority for a DNS zone. • **TXT:** Specifies the text information. • **UID:** Specifies the user identifier. • **UINFO:** Specifies the user information. • **WKS:** Describes a well-known service.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- nslookup set type

nslookup set vc

Article • 02/03/2023

Specifies whether to use a virtual circuit when sending requests to the server.

Syntax

```
set [no]vc
```

Parameters

Parameter	Description
novc	Specifies to never use a virtual circuit when sending requests to the server. This is the default value.
vc	Specifies to always use a virtual circuit when sending requests to the server.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

nslookup view

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sorts and lists the output of the previous **ls** commands or subcommands.

Syntax

```
view <filename>
```

Parameters

Parameter	Description
`<filename>`	Specifies the name of the file containing output from the previous **ls** commands or subcommands.
/?	Displays help at the command prompt.
/help	Displays help at the command prompt.

Related links

- Command-Line Syntax Key
- nslookup ls

ntbackup

Article • 05/03/2023

Applies to: Windows Server (All supported versions)

The `ntbackup` command backs up and restores your computer and files from a command prompt. This command is replaced with the wbadmin command.

> **ⓘ Important**
>
> The `wbadmin` command can't recover backups created by using the `ntbackup` commands. The Windows NT Backup - Restore utility is needed to recover from legacy backups.

Related links

- Command-Line Syntax Key
- wbadmin

ntcmdprompt

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Runs the command interpreter **Cmd.exe**, rather than **Command.com**, after running a Terminate and Stay Resident (TSR) or after starting the command prompt from within an MS-DOS application.

Syntax

```
ntcmdprompt
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.

Remarks

- When **Command.com** is running, some features of **Cmd.exe**, such as the **doskey** display of command history, aren't available. If you would prefer to run the **Cmd.exe** command interpreter after you've started a Terminate and Stay Resident (TSR) or started the command prompt from within an application based on MS-DOS, you can use the **ntcmdprompt** command. However, keep in mind that the TSR may not be available for use when you are running **Cmd.exe**. You can include the **ntcmdprompt** command in your **Config.nt** file or the equivalent custom startup file in an application's program information file (Pif).

Related links

- Command-Line Syntax Key

ntfrsutl

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Dumps the internal tables, thread, and memory information for the NT File Replication Service (NTFRS) from both the local and remote servers. The recovery setting for NTFRS in Service Control Manager (SCM) can be critical to locating and keeping important log events on the computer. This tool provides a convenient method of reviewing those settings.

Syntax

```
ntfrsutl[idtable|configtable|inlog|outlog][<computer>]
ntfrsutl[memory|threads|stage][<computer>]
ntfrsutl ds[<computer>]
ntfrsutl [sets][<computer>]
ntfrsutl [version][<computer>]
ntfrsutl poll[/quickly[=[<n>]]][/slowly[=[<n>]]][/now][<computer>]
```

Parameters

Parameter	Description
idtable	Specifies the ID table.
configtable	Specifies the FRS configuration table.
inlog	Specifies the inbound log.
outlog	Specifies the outbound log.
`<computer>`	Specifies the computer.
memory	Specifies the memory usage.
threads	Specifies the memory usage.
stage	Specifies the memory usage.
ds	Lists the NTFRS service's view of the DS.

Parameter	Description
sets	Specifies the active replica sets.
version	Specifies the API and NTFRS service versions.
poll	Specifies the current polling intervals. • `/quickly` - Polls quickly until it retrieves a stable configuration. • `/quickly=` - Polls quickly every default number of minutes. • `/quickly=<n>` - Polls quickly every *n* minutes. • `/slowly` - Polls slowly until it retrieves a stable configuration. • `/slowly=` - Polls slowly every default number of minutes. • `/slowly=<n>` - Polls slowly every *n* minutes. • `/now` - Polls now.
/?	Displays help at the command prompt.

Examples

To determine the polling interval for file replication, type:

```
C:\Program Files\SupportTools>ntfrsutl poll wrkstn-1
```

To determine the current NTFRS application program interface (API) version, type:

```
C:\Program Files\SupportTools>ntfrsutl version
```

Related links

- Command-Line Syntax Key

openfiles

Article • 02/03/2023

Enables an administrator to query, display, or disconnect files and directories that have been opened on a system. This command also enables or disables the system **Maintain Objects List** global flag.

openfiles /disconnect

Enables an administrator to disconnect files and folders that have been opened remotely through a shared folder.

Syntax

```
openfiles /disconnect [/s <system> [/u [<domain>\]<username> [/p
[<password>]]]] {[/id <openfileID>] | [/a <accessedby>] | [/o {read | write
| read/write}]} [/op <openfile>]
```

Parameters

Parameter	Description
/s `<system>`	Specifies the remote system to connect to (by name or IP address). Don't use backslashes. If you don't use the **/s** option, the command is run on the local computer by default. This parameter applies to all files and folders that are specified in the command.
/u `[<domain>\]` `<username>`	Runs the command using the permissions of the specified user account. If you don't use the **/u** option, system permissions are used by default.
/p `[<password>]`	Specifies the password of the user account that is specified in the **/u** option. If you don't use the **/p** option, a password prompt appears when the command is run.
/id `<openfileID>`	Disconnects open files by the specified file ID. You can use the wildcard character (*) with this parameter. Note: You can use the **openfiles /query** command to find the file ID.

Parameter	Description
/a `<accessedby>`	Disconnects all open files associated with the user name specified in the *accessedby* parameter. You can use the wildcard character (*) with this parameter.
/o `{read | write | read/write}`	Disconnects all open files with the specified open mode value. Valid values are **Read**, **Write**, or **Read/Write**. You can use the wildcard character (*) with this parameter.
/op `<openfile>`	Disconnects all open file connections that are created by a specific open file name. You can use the wildcard character (*) with this parameter.
/?	Displays help at the command prompt.

Examples

To disconnect all open files with the *file ID 26843578*, type:

```
openfiles /disconnect /id 26843578
```

To disconnect all open files and directories accessed by the user *hiropln*, type:

```
openfiles /disconnect /a hiropln
```

To disconnect all open files and directories with *read/write mode*, type:

```
openfiles /disconnect /o read/write
```

To disconnect the directory with the open file name *C:\testshare*, regardless of who is accessing it, type:

```
openfiles /disconnect /a * /op c:\testshare\
```

To disconnect all open files on the remote computer *srvmain* that are being accessed by the user *hiropln*, regardless of their ID, type:

```
```

```
openfiles /disconnect /s srvmain /u maindom\hiropln /id *
```

openfiles /query

Queries and displays all open files.

Syntax

```
openfiles /query [/s <system> [/u [<domain>\]<username> [/p [<password>]]]]
[/fo {TABLE | LIST | CSV}] [/nh] [/v]
```

Parameters

Parameter	Description
/s `<system>`	Specifies the remote system to connect to (by name or IP address). Don't use backslashes. If you don't use the **/s** option, the command is run on the local computer by default. This parameter applies to all files and folders that are specified in the command.
/u `[<domain>\]` `<username>`	Runs the command using the permissions of the specified user account. If you don't use the **/u** option, system permissions are used by default.
/p `[<password>]`	Specifies the password of the user account that is specified in the **/u** option. If you don't use the **/p** option, a password prompt appears when the command is run.
[/fo `{TABLE | LIST | CSV}`]	Displays the output in the specified format. Valid values include: • **TABLE** - Displays output in a table. • **LIST** - Displays output in a list. • **CSV** - Displays output in Comma Separated Values (CSV) format.
/nh	Suppresses column headers in the output. Valid only when the **/fo** parameter is set to **TABLE** or **CSV**.
/v	Specifies that detailed (verbose) information be displayed in the output.
/?	Displays help at the command prompt.

Examples

To query and display all open files, type:

```
openfiles /query
```

To query and display all open files in table format without headers, type:

```
openfiles /query /fo table /nh
```

To query and display all open files in list format with detailed information, type:

```
openfiles /query /fo list /v
```

To query and display all open files on the remote system *srvmain* by using the credentials for the user *hiropln* on the *maindom* domain, type:

```
openfiles /query /s srvmain /u maindom\hiropln /p p@ssW23
```

> ⓘ **Note**
>
> In this example, the password is supplied on the command line. To prevent displaying the password, leave out the **/p** option. You'll be prompted for the password, which won't be echoed to the screen.

openfiles /local

Enables or disables the system **Maintain Objects List** global flag. If used without parameters, **openfiles /local** displays the current status of the **Maintain Objects List** global flag.

> ⓘ **Note**

Changes made by using the **on** or **off** option don't take effect until you restart the system. Enabling the **Maintain Objects List** global flag might slow down your system.

Syntax

```
openfiles /local [on | off]
```

Parameters

Parameter	Description
`[on | off]`	Enables or disables the system **Maintain Objects List** global flag, which tracks local file handles.
/?	Displays help at the command prompt.

Examples

To check the current status of the **Maintain Objects List** global flag, type:

```
openfiles /local
```

By default, the **Maintain Objects List** global flag is disabled, and the following message appears, `INFO: The system global flag 'maintain objects list' is currently disabled.`

To enable the **Maintain Objects List** global flag, type:

```
openfiles /local on
```

The following message appears when the global flag is enabled, `SUCCESS: The system global flag 'maintain objects list' is enabled. This will take effect after the system is restarted.`

To disable the **Maintain Objects List** global flag, type:

```
openfiles /local off
```

Related links

- Command-Line Syntax Key

pagefileconfig

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

> **ⓘ Important**
>
> This command has been deprecated.

Enables an administrator to display and configure a system's paging file Virtual Memory settings. For descriptions and usage information, see pagefileconfig.

Related links

- Command-Line Syntax Key

path

Article • 02/03/2023

Sets the command path in the PATH environment variable, specifying the set of directories used to search for executable (.exe) files. If used without parameters, this command displays the current command path.

Syntax

```
path [[<drive>:]<path>[;...][;%PATH%]]
path ;
```

Parameters

Parameter	Description
`[<drive>:]<path>`	Specifies the drive and directory to set in the command path. The current directory is always searched before the directories specified in the command path.
;	Separates directories in the command path. If used without other parameters, **;** clears the existing command paths from the PATH environment variable and directs Cmd.exe to search only in the current directory.
`%PATH%`	Appends the command path to the existing set of directories listed in the PATH environment variable. If you include this parameter, Cmd.exe replaces it with the command path values found in the PATH environment variable, eliminating the need to manually enter these values at the command prompt.
/?	Displays help at the command prompt.

Remarks

- The Windows operating system searches using default file name extensions in the following order of precedence: .exe, .com, .bat, and .cmd. Which means if you're looking for a batch file named, acct.bat, but have an app named acct.exe in the same directory, you must include the .bat extension at the command prompt.
- If two or more files in the command path have the same file name and extension, this command first searches for the specified file name in the current directory.

Then, it searches the directories in the command path in the order that they're listed in the PATH environment variable.

- If you place the **path** command in your Autoexec.nt file, the Windows operating system automatically appends the specified MS-DOS subsystem search path every time you log on to your computer. Cmd.exe does not use the Autoexec.nt file. When started from a shortcut, Cmd.exe inherits the environment variables set in My Computer/Properties/Advanced/Environment.

Examples

To search the paths *c:\user\taxes*, *b:\user\invest*, and *b:\bin* for external commands, type:

```
path c:\user\taxes;b:\user\invest;b:\bin
```

Related links

- Command-Line Syntax Key

pathping

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Provides information about network latency and network loss at intermediate hops between a source and destination. This command sends multiple echo Request messages to each router between a source and destination, over a period of time, and then computes results based on the packets returned from each router. Because this command displays the degree of packet loss at any given router or link, you can determine which routers or subnets might be having network problems. Used without parameters, this command displays help.

> **Note**
>
> This command is available only if the Internet Protocol (TCP/IP) protocol is installed as a component in the properties of a network adapter in Network Connections.
>
> Additionally, this command identifies which routers are on the path, same as using the **tracert command**. Howevever, this command also sends pings periodically to all of the routers over a specified time period and computes statistics based on the number returned from each.

Syntax

```
pathping [/n] [/h <maximumhops>] [/g <hostlist>] [/p <Period>] [/q
<numqueries> [/w <timeout>] [/i <IPaddress>] [/4 <IPv4>] [/6 <IPv6>]
[<targetname>]
```

Parameters

Parameter	Description
/n	Prevents **pathping** from attempting to resolve the IP addresses of intermediate routers to their names. This might expedite the display of **pathping** results.

Parameter	Description
/h `<maximumhops>`	Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.
/g `<hostlist>`	Specifies that the echo Request messages use the **Loose Source Route** option in the IP header with the set of intermediate destinations specified in *hostlist*. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is **9**. The *hostlist* is a series of IP addresses (in dotted decimal notation) separated by spaces.
/p `<period>`	Specifies the number of milliseconds to wait between consecutive pings. The default is 250 milliseconds (1/4 second). This parameter sends individual pings to each intermediate hop. Because of this, the interval between two pings sent to the same hop is *period* multiplied by the number of hops.
/q `<numqueries>`	Specifies the number of echo Request messages sent to each router in the path. The default is 100 queries.
/w `<timeout>`	Specifies the number of milliseconds to wait for each reply. The default is 3000 milliseconds (3 seconds). This parameter sends multiple pings in parallel. Because of this, the amount of time specified in the *timeout* parameter isn't bounded by the amount of time specified in the *period* parameter for waiting between pings.
/i `<IPaddress>`	Specifies the source address.
/4 `<IPv4>`	Specifies that pathping uses IPv4 only.
/6 `<IPv6>`	Specifies that pathping uses IPv6 only.
`<targetname>`	Specifies the destination, which is identified either by IP address or host name.
/?	Displays help at the command prompt.

Remarks

- All parameters are case-sensitive.
- To avoid network congestion and to minimize the effects of burst losses, pings should be sent at a sufficiently slow pace.

Example of the pathping command output

```
```

```
D:\>pathping /n contoso1
Tracing route to contoso1 [10.54.1.196]
over a maximum of 30 hops:
  0  172.16.87.35
  1  172.16.87.218
  2  192.168.52.1
  3  192.168.80.1
  4  10.54.247.14
  5  10.54.1.196
computing statistics for 125 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  address
  0                                           172.16.87.35
                                 0/ 100 =  0%   |
  1   41ms     0/ 100 =  0%     0/ 100 =  0%  172.16.87.218
                                13/ 100 = 13%   |
  2   22ms    16/ 100 = 16%     3/ 100 =  3%  192.168.52.1
                                 0/ 100 =  0%   |
  3   24ms    13/ 100 = 13%     0/ 100 =  0%  192.168.80.1
                                 0/ 100 =  0%   |
  4   21ms    14/ 100 = 14%     1/ 100 =  1%  10.54.247.14
                                 0/ 100 =  0%   |
  5   24ms    13/ 100 = 13%     0/ 100 =  0%  10.54.1.196
Trace complete.
```

When **pathping** is run, the first results list the path. Next, a busy message is displayed for approximately 90 seconds (the time varies by hop count). During this time, information is gathered from all routers previously listed and from the links between them. At the end of this period, the test results are displayed.

In the above sample report, the **This Node/Link**, **Lost/Sent** = **Pct** and **address** columns show that the link between *172.16.87.218* and *192.168.52.1* is dropping 13% of the packets. The routers at hops 2 and 4 are also dropping packets addressed to them, but this loss doesn't affect their ability to forward traffic that isn't addressed to them.

The loss rates displayed for the links, identified as a vertical bar (|) in the **address** column, indicate link congestion that is causing the loss of packets that are being forwarded on the path. The loss rates displayed for routers (identified by their IP addresses) indicate that these routers might be overloaded.

Related links

- Command-Line Syntax Key
- tracert command

pause

Article • 02/03/2023

Suspends the processing of a batch program, displaying the prompt, `Press any key to continue . . .`

Syntax

```
pause
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.

Remarks

- If you press CTRL+C to stop a batch program, the following message appears, `Terminate batch job (Y/N)?`. If you press **Y** (for yes) in response to this message, the batch program ends and control returns to the operating system.
- You can insert the **pause** command before a section of the batch file that you might not want to process. When **pause** suspends processing of the batch program, you can press CTRL+C and then press **Y** to stop the batch program.

Examples

To create a batch program that prompts the user to change disks in one of the drives, type:

```
@echo off
:Begin
copy a:*.*
echo Put a new disk into Drive A
```

```
pause
goto begin
```

In this example, all the files on the disk in Drive A are copied to the current directory. After the message prompts you to put a new disk in Drive A, the **pause** command suspends processing so that you can change disks and then press any key to resume processing. This batch program runs in an endless loop—the **goto begin** command sends the command interpreter to the Begin label of the batch file.

Related links

- Command-Line Syntax Key

pbadmin

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

ⓘ Important

This command has been deprecated.

Administers phone books. Used without parameters, pbadmin starts Phone Book Administrator. For descriptions and usage information, see pbadmin.

Related links

- Command-Line Syntax Key

pentnt

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

> **Important**
>
> This command has been deprecated.

Detects floating point division error (if present) in the Pentium chip, disables floating point hardware, and turns on floating point emulation. For descriptions and usage information, see pentnt.

Related links

- Command-Line Syntax Key

perfmon

Article • 02/03/2023

Start Windows Reliability and Performance Monitor in a specific standalone mode.

Syntax

```
perfmon </res|report|rel|sys>
```

Parameters

Parameter	Description
/res	Starts the Resource View.
/report	Starts the System Diagnostics Data Collector Set and displays a report of the results.
/rel	Starts the Reliability Monitor.
/sys	Starts the Performance Monitor.

Related links

- Command-Line Syntax Key
- Windows Performance Monitor

ping

Article • 09/20/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) echo Request messages. The receipt of the corresponding echo Reply messages is displayed, along with round-trip times. ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, this command displays Help content.

You can also use this command to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name isn't, you might have a name resolution problem. In this case, make sure the computer name you're specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.

> **Note**
>
> This command is available only if the Internet Protocol (TCP/IP) is installed as a component in the properties of a network adapter in Network Connections.

Syntax

```
ping [/t] [/a] [/n <count>] [/l <size>] [/f] [/I <TTL>] [/v <TOS>] [/r
<count>] [/s <count>] [{/j <hostlist> | /k <hostlist>}] [/w <timeout>] [/R]
[/S <Srcaddr>] [/4] [/6] <targetname>
```

Parameters

Parameter	Description
/t	Specifies ping continue sending echo Request messages to the destination until interrupted. To interrupt and display statistics, press CTRL+ENTER. To interrupt and quit this command, press CTRL+C.

Parameter	Description
/a	Specifies reverse name resolution be performed on the destination IP address. If this operation is successful, ping displays the corresponding host name.
/n `<count>`	Specifies the number of echo Request messages be sent. The default is 4.
/l `<size>`	Specifies the length, in bytes, of the **Data** field in the echo Request messages. The default is 32. The maximum size is 65,500.
/f	Specifies that echo Request messages are sent with the **Do not Fragment** flag in the IP header set to 1 (available on IPv4 only). The echo Request message can't be fragmented by routers in the path to the destination. This parameter is useful for troubleshooting path Maximum Transmission Unit (PMTU) problems.
/l `<TTL>`	Specifies the value of the Time To Live (TTL) field in the IP header for echo Request messages sent. The default is the default TTL value for the host. The maximum *TTL* is 255.
/v `<TOS>`	Specifies the value of the Type Of Service (TOS) field in the IP header for echo Request messages sent (available on IPv4 only). The default is 0. *TOS* is specified as a decimal value from 0 through 255.
/r `<count>`	Specifies the **Record Route** option in the IP header is used to record the path taken by the echo Request message and corresponding echo Reply message (available on IPv4 only). Each hop in the path uses an entry in the **Record Route** option. If possible, specify a *count* equal to or greater than the number of hops between the source and destination. The *count* must be a minimum of 1 and a maximum of 9.
/s `<count>`	Specifies that the **Internet timestamp** option in the IP header is used to record the time of arrival for the echo Request message and corresponding echo Reply message for each hop. The *count* must be a minimum of 1 and a maximum of 4. This parameter is required for link-local destination addresses.
/j `<hostlist>`	Specifies the echo Request messages use the **Loose Source Route** option in the IP header with the set of intermediate destinations specified in *hostlist* (available on IPv4 only). With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the host list is 9. The host list is a series of IP addresses (in dotted decimal notation) separated by spaces.
/k `<hostlist>`	Specifies the echo Request messages use the **Strict Source Route** option in the IP header with the set of intermediate destinations specified in *hostlist* (available on IPv4 only). With strict source routing, the next intermediate destination must be directly reachable (it must be a neighbor on an interface of the router). The maximum number of addresses or names in the host list is 9. The host list is a series of IP addresses (in dotted decimal notation) separated by spaces.
/w `<timeout>`	Specifies the amount of time, in milliseconds, to wait for the echo Reply message corresponding to a given echo Request message. If the echo Reply message isn't

Parameter	Description
	received within the time-out, the "Request timed out" error message is displayed. The default time-out is 4000 (4 seconds).
/R	Specifies the round-trip path is traced (available on IPv6 only).
/S `<Srcaddr>`	Specifies the source address to use (available on IPv6 only).
/4	Specifies IPv4 used to ping. This parameter isn't required to identify the target host with an IPv4 address. It's only required to identify the target host by name.
/6	Specifies IPv6 used to ping. This parameter isn't required to identify the target host with an IPv6 address. It's only required to identify the target host by name.
`<targetname>`	Specifies the host name or IP address of the destination.
/?	Displays help at the command prompt.

Example of the ping command output

```
C:\>ping example.microsoft.com
    pinging example.microsoft.com [192.168.239.132] with 32 bytes of data:
    Reply from 192.168.239.132: bytes=32 time=101ms TTL=124
    Reply from 192.168.239.132: bytes=32 time=100ms TTL=124
    Reply from 192.168.239.132: bytes=32 time=120ms TTL=124
    Reply from 192.168.239.132: bytes=32 time=120ms TTL=124
```

Examples

To ping the destination 10.0.99.221 and resolve 10.0.99.221 to its host name, type:

```
ping /a 10.0.99.221
```

To ping the destination 10.0.99.221 with 10 echo Request messages, each of which has a Data field of 1000 bytes, type:

```
ping /n 10 /l 1000 10.0.99.221
```

To ping the destination 10.0.99.221 and record the route for 4 hops, type:

```
ping /r 4 10.0.99.221
```

To ping the destination 10.0.99.221 and specify the loose source route of 10.12.0.1-10.29.3.1-10.1.44.1, type:

```
ping /j 10.12.0.1 10.29.3.1 10.1.44.1 10.0.99.221
```

Related links

- Command-Line Syntax Key

pktmon

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Packet Monitor (Pktmon) is an in-box, cross-component network diagnostics tool for Windows. It can be used for advanced packet capture and event collection, drop detection, filtering, and counting. Pktmon is especially helpful in virtualization scenarios such as container networking and SDN, because it provides visibility within the networking stack.

Syntax

```
pktmon { filter | list | start | stop | status | unload | counters | reset |
etl2txt | etl2pcap | hex2pkt | help } [options]
```

Commands

Command	Description
pktmon filter	Manage packet filters.
pktmon list	List packet processing components.
pktmon start	Start packet capture and event collection.
pktmon stop	Stop data collection.
pktmon status	Query current status.
pktmon unload	Unload PktMon driver.
pktmon counters	Display current packet counters.
pktmon reset	Reset packet counters to zero.
pktmon etl2txt	Convert log file to text format.
pktmon etl2pcap	Convert log file to pcapng format.
pktmon hex2pkt	Decode packet in hexadecimal format.

Command	Description
pktmon help	Show help text for specific command.

Related links

- Packet Monitor overview
- Pktmon support for Microsoft Network Monitor (Netmon)

pktmon counters

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Pktmon counters allows you to query and display current packet counters from monitored components to confirm the presence of expected traffic and get a high-level view of how the traffic flowed in the machine.

Syntax

```
pktmon counters [--type { all | flow | drop }] [--include-hidden] [--zero]
[--drop-reason] [--live] [--refresh-rate <n>] [--json]
```

Parameters

Parameter	Description
-t, --type	Select which types of counters to show. Supported values are **all** counters (default), **flow** (flows only), or **drop** (drops only).
-z, --zero	Show counters that are zero in both directions.
-i, --include-hidden	Show counters from components that are hidden by default.
-r, --drop-reason	Show the most recent drop reason for each drop counter.
--live	Automatically refresh the counters. Press **Ctrl+C** to stop.
--refresh-rate <n>	Number of times to refresh the counters per second, from 1 to 30. Default is 10.
--json	Output the counters in JSON format. Implies -i and -r.

Related links

- Pktmon
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon list
- Pktmon reset
- Pktmon start
- Pktmon status
- Pktmon unload
- Packet Monitor overview

pktmon etl2pcap

Article • 09/05/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Convert pktmon log file to pcapng format. Dropped packets are not included by default. These logs can be analyzed using Wireshark (or any pcapng analyzer).

Syntax

```
pktmon etl2pcap <file> [--out <name>] [--drop-only] [--component-id <id>]
```

Where `<file>` is the ETL file to convert.

Parameters

Parameter	Description
-o, --out <name>	Name of the formatted pcapng file.
-d, --drop-only	Convert dropped packets only.
-c, --component-id <id>	Filter packets by a specific component ID.

Output filtering

All information about the packet drop reports and packet flow through the networking stack is lost in pcapng format output. Log contents should be carefully prefiltered to show the complete conversion. For example:

- Pcapng format doesn't distinguish between a flowing packet and a dropped packet. To separate all the packets in the capture from dropped packets, generate two pcapng files; one that contains all the packets (`pktmon etl2pcap log.etl --out log-capture.etl`), and another that contains only dropped packets (`pktmon etl2pcap log.etl --drop-only --out log-drop.etl`). This way you're able to analyze the dropped packets in a separate log.

- Pcapng format doesn't distinguish between different networking components where a packet was captured. For such multilayered scenarios, specify the desired component ID in the pcapng output `pktmon etl2pcap log.etl --component-id 5`. Repeat this command for each set of component IDs that you're interested in.

Related links

- Pktmon
- Pktmon counters
- Pktmon etl2txt
- Pktmon filter
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon list
- Pktmon reset
- Pktmon start
- Pktmon status
- Pktmon unload
- Packet Monitor overview

pktmon etl2txt

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Convert ETL log file to text format.

Syntax

```
pktmon etl2txt <file> [--out <name>] [--stats-only] [--timestamp-only] [--
metadata]
                      [--tmfpath <path>] [--brief] [--verbose <n>] [--hex]
                      [--no-ethernet] [--vxlan <port>]
```

Where `<file>` is the ETL file to convert.

Parameters

Parameter	Description
-o, --out <name>	Name of the formatted text file.
-s, --stats-only	Display log file statistical information.
-t, --timestamp-only	Use timestamp only prefix for events and packets.
-m, --metadata	Print event metadata, such as logging level and keywords.
-p, --tmfpath <path>	Path to TMF files for decoding WPP traces. Multiple paths should be separated by semicolons. All WPP traces are skipped when this option is not specified.

Network packet formatting options

Parameter	Description
-b, --brief	Use abbreviated packet format.
-v, --verbose <n>	Verbosity level from 1 to 3.
-x, --hex	Include hexadecimal format.
-e, --no-ethernet	Don't print ethernet header.
-l, --vxlan <port>	Custom VXLAN port.

Related links

- Pktmon
- Pktmon counters
- Pktmon etl2pcap
- Pktmon filter
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon list
- Pktmon reset
- Pktmon start
- Pktmon status
- Pktmon unload
- Packet Monitor overview

pktmon filter

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Pktmon filter allows you to list, add, or remove packet filters.

Syntax

```
pktmon filter { list | add | remove } [OPTIONS | help]
```

Parameters

Parameter	Description
pktmon filter list	Display active packet filters.
pktmon filter add	Add a filter to control which packets are reported.
pktmon filter remove	Remove all packet filters.

Related links

- Pktmon
- Pktmon counters
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon list
- Pktmon reset
- Pktmon start
- Pktmon status
- Pktmon unload
- Packet Monitor overview

pktmon filter add

Article • 02/15/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Pktmon filter add allows you to add a filter to control which packets are reported. For a packet to be reported, it must match all conditions specified in at least one filter. Up to 32 filters can be active at once.

Syntax

```
pktmon filter add <name> [-m <mac> [mac2]] [-v <vlan>] [-d { IPv4 | IPv6 | number }]
                         [-t { TCP [flags...] | UDP | ICMP | ICMPv6 | number }]
                         [-i <ip> [ip2]] [-p <port> [port2]] [-b] [-e [port]]
```

You may provide an optional name or description of the filter.

> **Note**
>
> When two MACs (-m), IPs (-i), or ports (-p) are specified, the filter matches packets that contain both. It will not distinguish between source or destination for this purpose.

Parameters

You can supply parameters for Ethernet frame, IP header, TCP/UDP header, cluster heartbeat, and encapsulation.

Parameter	Description
-m, --mac[-address]	Match source or destination MAC address. See note above.
-v, --vlan	Match by VLAN ID (VID) in the 802.1Q header.

Parameter	Description
-d, --data-link[-protocol], --ethertype	Match by data link (layer 2) protocol. Can be IPv4, IPv6, ARP, or a protocol number.
-t, --transport[-protocol], --ip-protocol	Match by transport (layer 4) protocol. Can be TCP, UDP, ICMP, ICMPv6, or a protocol number. To further filter TCP packets, an optional list of TCP flags to match can be provided. Supported flags are FIN, SYN, RST, PSH, ACK, URG, ECE, and CWR.
-i, --ip[-address]	Match source or destination IP address. See note above. To match by subnet, use CIDR notation with the prefix length.
-p, --port	Match source or destination port number. See note above.
-b, --heartbeat	Match RCP heartbeat messages over UDP port 3343.
-e, --encap	Apply above filtering parameters to both inner and outer encapsulation headers. Supported encapsulation methods are VXLAN, GRE, NVGRE, and IP-in-IP. Custom VXLAN port is optional, and defaults to 4789.

Examples

The following set of filters will capture any ICMP traffic from or to the IP address 10.0.0.10 along with any traffic on port 53.

PowerShell

```
C:\Test> pktmon filter add -i 10.0.0.10 -t icmp
C:\Test> pktmon filter add -p 53
```

The following filter will capture all the SYN packets sent or received by the IP address 10.0.0.10:

PowerShell

```
C:\Test> pktmon filter add -i 10.0.0.10 -t tcp syn
```

The following filter called **MyPing** pings 10.10.10.10 using the ICMP protocol:

PowerShell

```
C:\Test> pktmon filter add MyPing -i 10.10.10.10 -t ICMP
```

The following filter called **MySmbSyb** captures TCP synchronized SMB traffic:

PowerShell

```
C:\Test> pktmon filter add MySmbSyn -i 10.10.10.10 -t TCP SYN -p 445
```

The following filter called **MySubnet** captures traffic on the subnet mask 255.255.255.0, or /24 in CIDR notation:

PowerShell

```
C:\Test> pktmon filter add MySubnet -i 10.10.10.0/24
```

Other references

- Pktmon
- Pktmon counters
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter
- Pktmon hex2pkt
- Pktmon list
- Pktmon reset
- Pktmon start
- Pktmon status
- Pktmon unload
- Packet Monitor overview

pktmon hex2pkt

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Decode packet in hexadecimal format.

Syntax

```
pktmon hex2pkt [--type { Ethernet | IP | HTTP }]
```

Parameters

Parameter	Description
-t, --type	Packet type to decode. Options are Ethernet, IP, and HTTP. Default is Ethernet.

Related links

- Pktmon
- Pktmon counters
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter
- Pktmon filter add
- Pktmon list
- Pktmon reset
- Pktmon start
- Pktmon status
- Pktmon unload
- Packet Monitor overview

pktmon list

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Lists all active networking components that can be monitored, allowing you to examine the networking stack layout. The command shows networking components (drivers) arranged by adapters bindings.

Syntax

```
pktmon list [--all] [--include-hidden] [--json]
```

Parameters

Parameter	Description
-a, --all	Show all component types. Only network adapters are displayed by default.
-i, --include-hidden	Show components that are hidden by default.
--json	Output the list in JSON format. Implies -i and -a.

Related links

- Pktmon
- Pktmon counters
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon reset
- Pktmon start
- Pktmon status
- Pktmon unload

- Packet Monitor overview

pktmon reset

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Reset counters to zero.

Syntax

```
pktmon reset [-counters]
```

Related links

- Pktmon
- Pktmon counters
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon list
- Pktmon start
- Pktmon status
- Pktmon unload
- Packet Monitor overview

pktmon start

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Starts packet capture and event collection.

Syntax

```
pktmon start [--capture [--counters-only] [--comp <selector>] [--type
<type>] [--pkt-size <bytes>] [--flags <mask>]]
             [--trace --provider <name> [--keywords <k>] [--level <n>] ...]
             [--file-name <name>] [--file-size <size>] [--log-mode <mode>]
```

Packet capture parameters

Use **-c** or **--capture** to enable packet capture and packet counters, along with the following optional parameters.

Parameter	Description
-o, --counters-only	Collect packet counters only. No packet logging.
--comp	Select components to capture packets on. Can be all components (all), NICs only (nics), or a list of component IDs. Defaults to all.
--type	Select which packets to capture. Can be all, flow, or drop. Default is all.
--pkt-size <bytes>	Number of bytes to log from each packet. To always log the entire packet, set this to 0. Default is 128 bytes.
--flags <mask>	Hexadecimal bitmask that controls information logged during packet capture. Default is 0x012. Packet capture flags, below.

Packet capture flags

The following flags apply to the **--flags** parameter (see above).

Flag	Description
0x001	Internal Packet Monitor errors.
0x002	Information about components, counters, and filters. This information is added to the end of the log file.
0x004	Source and destination information for the first packet in NET_BUFFER_LIST group.
0x008	Select packet metadata from NDIS_NET_BUFFER_LIST_INFO enumeration.
0x010	Raw packet, truncated to the size specified in the [--pkt-size] parameter.

Event collection parameters

Use **-t** or **--trace** to enable event collection, along with the following optional parameters.

Parameter	Description
-p, --provider <name>	Event provider name or GUID. For multiple providers, use this parameter more than once.
-k, --keywords <k>	Hexadecimal bitmask that controls which events are logged for the corresponding provider. Default is 0xFFFFFFFF.
-l, --level <n>	Logging level for the corresponding provider. Default is 4 (info level).

Logging parameters

Use the following parameters for logging:

Parameter	Description
-f, --file-name <name>	Log file name. Default is PktMon.etl.
-s, --file-size <size>	Maximum log file size in megabytes. Default is 512 MB.
-m, --log-mode	Sets the logging mode (see below). Default is circular.

Logging modes

The following modes apply to the **-m** or **--log-mode** parameter (see above).

Mode	Description

Mode	Description
circular	New events overwrite the oldest ones when the log is full.
multi-file	A new log file is created each time the log is full. Log files are sequentially numbered: PktMon1.etl, PktMon2.etl, etc. No limited on the number of captured events.
real-time	Display events and packets on screen at real time. No log file is created. Press **Ctrl+C** to stop monitoring.
memory	Like circular, but the entire log is stored in memory. It is written to a file when pktmon is stopped. Memory buffer size is specified in [--file-size] parameter.

Examples

Example 1: Packet capture

PowerShell

```
C:\Test> pktmon start --capture
```

Example 2: Packet counters only

PowerShell

```
C:\Test> pktmon start --capture --counters-only
```

Example 3: Event logging

PowerShell

```
C:\Test> pktmon start --trace -p Microsoft-Windows-TCPIP -p Microsoft-
Windows-NDIS
```

Example 4: Packet capture with event logging

PowerShell

```
C:\Test> pktmon start --capture --trace -p Microsoft-Windows-TCPIP -k 0xFF -
l 4
```

Related links

- Pktmon

- Pktmon counters
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon list
- Pktmon reset
- Pktmon status
- Pktmon unload
- Packet Monitor overview

pktmon status

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Query current Packet Monitor status.

Syntax

```
pktmon status [--buffer-info]
```

Parameters

Parameter	Description
-b, --buffer-info	Display ETW buffer information.

Related links

- Pktmon
- Pktmon counters
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon list
- Pktmon reset
- Pktmon start
- Pktmon unload
- Packet Monitor overview

pktmon unload

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, Azure

Stop the PktMon driver service and unload PktMon.sys. Effectively equivalent to 'sc.exe stop PktMon'. Measurement (if active) will immediately stop, and any state will be deleted (counters, filters, etc.).

Syntax

```
pktmon unload
```

Related links

- Pktmon
- Pktmon counters
- Pktmon etl2pcap
- Pktmon etl2txt
- Pktmon filter
- Pktmon filter add
- Pktmon hex2pkt
- Pktmon list
- Pktmon reset
- Pktmon start
- Pktmon status
- Packet Monitor overview

pnpunattend

Article • 02/03/2023

Audits a computer for device drivers, and perform unattended driver installations, or search for drivers without installing and, optionally, report the results to the command line. Use this command to specify the installation of specific drivers for specific hardware devices.

Prerequisites

Preliminary preparation is required for older versions of the Windows operating system. Prior to using this command, you must complete the following tasks:

1. Create a directory for the drivers you want to install. For example, create a folder at **C:\Drivers\Video** for video adapter drivers.
2. Download and extract the driver package for your device. Copy the contents of the subfolder that contains the INF file for your version of the operating system and any subfolders to the video folder that you created. For example, copy the video driver files to **C:\Drivers\Video**.
3. Add a system environment path variable to the folder you created in step 1.For example, **C:\Drivers\Video**.
4. Create the following registry key, and then for the **DriverPaths** key you create, set the **Value Data** to **1**.
5. For Windows® 7 navigate the registry path: **HKEY_LOCAL_Machine\Software\Microsoft\Windows NT\CurrentVersion**, and then create the keys: **UnattendSettings\PnPUnattend\DriverPaths**

Syntax

```
PnPUnattend.exe auditsystem [/help] [/?] [/h] [/s] [/l]
```

Parameters

Parameter	Description

Parameter	Description
auditsystem	Specifies online driver install. Required, except when this command is run with either the **/help** or **/?** parameters.
/s	Optional. Specifies to search for drivers without installing.
/l	Optional. Specifies to display the log information for this command in the command prompt.
`/? | /help`	Optional. Displays help for this command at the command prompt.

Examples

To command shows how to use the **PNPUnattend.exe** to audit a computer for possible driver updates, and then report the findings to the command prompt, type:

```
pnpunattend auditsystem /s /l
```

Related links

- Command-Line Syntax Key

pnputil

Article • 02/03/2023

Pnputil.exe is a command line utility that you can use to manage the driver store. You can use this command to add driver packages, remove driver packages, and list driver packages that are in the store.

Syntax

```
pnputil.exe [-f | -i] [ -? | -a | -d | -e ] <INF name>
```

Parameters

Parameter	Description
-a	Specifies to add the identified INF file.
-d	Specifies to delete the identified INF file.
-e	Specifies to enumerate all third-party INF files.
-f	Specifies to force the deletion of the identified INF file. Can't be used in conjunction with the **–i** parameter.
-i	Specifies to install the identified INF file. Can't be used in conjunction with the **-f** parameter.
/?	Displays help at the command prompt.

Examples

To add an INF file, named USBCAM.INF, type:

```
pnputil.exe -a a:\usbcam\USBCAM.INF
```

To add all INF files, located in c:\drivers, type:

```
```

```
pnputil.exe -a c:\drivers\*.inf
```

To add and install the USBCAM.INF driver, type:

```
pnputil.exe -i -a a:\usbcam\USBCAM.INF
```

To enumerate all third-party drivers, type:

```
pnputil.exe –e
```

To delete the INF file and driver named oem0.inf, type:

```
pnputil.exe -d oem0.inf
```

Related links

- Command-Line Syntax Key
- popd command

popd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

The **popd** command changes the current directory to the directory that was most recently stored by the **pushd** command.

Every time you use the **pushd** command, a single directory is stored for your use. However, you can store multiple directories by using the **pushd** command multiple times. The directories are stored sequentially in a virtual stack, so if you use the **pushd** command once, the directory in which you use the command is placed at the bottom of the stack. If you use the command again, the second directory is placed on top of the first one. The process repeats every time you use the **pushd** command.

If you use the **popd** command, the directory on the top of the stack is removed and the current directory is changed to that directory. If you use the **popd** command again, the next directory on the stack is removed. If command extensions are enabled, the **popd** command removes any drive-letter assignments created by the **pushd** command.

Syntax

```
popd
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.

Examples

To change the current directory from the one in which the batch program was run, and then to change it back, type:

```
```

```
@echo off
rem This batch file deletes all .txt files in a specified directory
pushd %1
del *.txt
popd
cls
echo All text files deleted in the %1 directory
```

Related links

- Command-Line Syntax Key
- pushd

PowerShell

Article • 02/03/2023

Windows PowerShell is a task-based command-line shell and scripting language designed especially for system administration. Built on the .NET Framework, Windows PowerShell helps IT professionals and power users control and automate the administration of the Windows operating system and applications that run on Windows.

Using PowerShell.exe

The **PowerShell.exe** command-line tool starts a Windows PowerShell session in a Command Prompt window. When you use **PowerShell.exe**, you can use its optional parameters to customize the session. For example, you can start a session that uses a particular execution policy or one that excludes a Windows PowerShell profile. Otherwise, the session is the same as any session that is started in the Windows PowerShell console.

- To start a Windows PowerShell session in a Command Prompt window, type `PowerShell`. A **PS** prefix is added to the command prompt to indicate that you are in a Windows PowerShell session.

- To start a session with a particular execution policy, use the **ExecutionPolicy** parameter, and type:

  PowerShell

  ```
  PowerShell.exe -ExecutionPolicy Restricted
  ```

- To start a Windows PowerShell session without your Windows PowerShell profiles, use the **NoProfile** parameter, and type:

  PowerShell

  ```
  PowerShell.exe -NoProfile
  ```

- To start a session , use the **ExecutionPolicy** parameter, and type:

  PowerShell

  ```
  PowerShell.exe -ExecutionPolicy Restricted
  ```

- To see the PowerShell.exe help file, type:

  ```PowerShell
  PowerShell.exe -help
  PowerShell.exe -?
  PowerShell.exe /?
  ```

- To end a Windows PowerShell session in a Command Prompt window, type `exit`. The typical command prompt returns.

Remarks

- For a complete list of the **PowerShell.exe** command-line parameters, see about_PowerShell.Exe.
- For information about other ways to start Windows PowerShell, see Starting Windows PowerShell.
- Windows PowerShell runs on the Server Core installation option of Windows Server operating systems. However, features that require a graphic user interface, such as the Windows PowerShell Integrated Scripting Environment (ISE), and the Out-GridView and Show-Command cmdlets, don't run on Server Core installations.

Related links

- about_PowerShell.Exe
- about_PowerShell_Ise.exe
- Windows PowerShell

PowerShell_ise

Article • 02/03/2023

Windows PowerShell Integrated Scripting Environment (ISE) is a graphical host application that enables you to read, write, run, debug, and test scripts and modules in a graphic-assisted environment. Key features such as IntelliSense, Show-Command, snippets, tab completion, syntax-coloring, visual debugging, and context-sensitive Help provide a rich scripting experience.

Using PowerShell.exe

The **PowerShell_ISE.exe** tool starts a Windows PowerShell ISE session. When you use **PowerShell_ISE.exe**, you can use its optional parameters to open files in Windows PowerShell ISE or to start a Windows PowerShell ISE session with no profile or with a multithreaded apartment.

- To start a Windows PowerShell ISE session in a Command Prompt window, in Windows PowerShell, or at the **Start** menu, type:

  ```
  PowerShell
  ```

  ```
  PowerShell_Ise.exe
  ```

- To open a script (.ps1), script module (.psm1), module manifest (.psd1), XML file, or any other supported file in Windows PowerShell ISE, type:

  ```
  PowerShell
  ```

  ```
  PowerShell_Ise.exe <filepath>
  ```

  In Windows PowerShell 3.0, you can use the optional **File** parameter as follows:

  ```
  PowerShell
  ```

  ```
  PowerShell_Ise.exe -file <filepath>
  ```

- To start a Windows PowerShell ISE session without your Windows PowerShell profiles, use the **NoProfile** parameter. (The **NoProfile** parameter is introduced in Windows PowerShell 3.0.), type:

  ```
  PowerShell
  ```

```
PowerShell_Ise.exe -NoProfile
```

- To see the PowerShell_ISE.exe help file, type:

```PowerShell
PowerShell_Ise.exe -help
PowerShell_Ise.exe -?
PowerShell_Ise.exe /?
```

Remarks

- For a complete list of the **PowerShell_ISE.exe** command-line parameters, see about_PowerShell_Ise.Exe.
- For information about other ways to start Windows PowerShell, see Starting Windows PowerShell.
- Windows PowerShell runs on the Server Core installation option of Windows Server operating systems. However, because Windows PowerShell ISE requires a graphic user interface, it does not run on Server Core installations.

Related links

- about_PowerShell_Ise.exe

print

Article • 02/03/2023

Sends a text file to a printer. A file can print in the background if you send it to a printer connected to a serial or parallel port on the local computer.

> **Note**
>
> You can perform many configuration tasks from the command prompt by using the **Mode command**, including configuring a printer connected to a parallel or a serial port, displaying printer status, or preparing a printer for code page switching.

Syntax

```
print [/d:<printername>] [<drive>:][<path>]<filename>[ ...]
```

Parameters

Parameter	Description
/d:`<printername>`	Specifies the printer that you want to print the job. To print to a locally connected printer, specify the port on your computer where the printer is connected. Valid values for parallel ports are **LPT1**, **LPT2**, and **LPT3**. Valid values for serial ports are **COM1**, **COM2**, **COM3**, and **COM4**. You can also specify a network printer by using its queue name (`\\server_name\printer_name`). If you don't specify a printer, the print job is sent to **LPT1** by default.
`<drive>`:	Specifies the logical or physical drive where the file you want to print is located. This parameter isn't required if the file you want to print is located on the current drive.
`<path>`	Specifies the location of the file you want to print. This parameter isn't required if the file you want to print is located in the current directory.
`<filename>[ ...]`	Required. Specifies the file you want to print. You can include multiple files in one command.
/?	Displays help at the command prompt.

Examples

To send the **report.txt** file, located in the current directory, to a printer connected to **lpt2** on the local computer, type:

```
print /d:lpt2 report.txt
```

To send the **report.txt** file, located in the **c:\accounting** directory, to the **printer1** print queue on the **/d:\copyroom** server, type:

```
print /d:\\copyroom\printer1 c:\accounting\report.txt
```

Related links

- Command-Line Syntax Key
- Print Command Reference
- Mode command

prncnfg

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configures or displays configuration information about a printer. This command is a Visual Basic script located in the `%WINdir%\System32\printing_Admin_Scripts\<language>` directory. To use this command at a command prompt, type **cscript** followed by the full path to the prncnfg file, or change directories to the appropriate folder. For example: `cscript %WINdir%\System32\printing_Admin_Scripts\en-US\prncnfg`.

Syntax

```
cscript prncnfg {-g | -t | -x | -?} [-S <Servername>] [-P <Printername>] [-z
<newprintername>] [-u <Username>] [-w <password>] [-r <portname>] [-l
<location>] [-h <sharename>] [-m <comment>] [-f <separatorfilename>] [-y
<datatype>] [-st <starttime>] [-ut <untiltime>] [-i <defaultpriority>] [-o
<priority>] [<+|->shared] [<+|->direct] [<+|->hidden] [<+|->published] [<+|-
>rawonly] [<+|->queued] [<+|->enablebidi] [<+|->keepprintedjobs] [<+|-
>workoffline] [<+|->enabledevq] [<+|->docompletefirst]
```

Parameters

Parameter	Description
-g	Displays configuration information about a printer.
-t	Configures a printer.
-x	Renames a printer.
-S `<Servername>`	Specifies the name of the remote computer that hosts the printer that you want to manage. If you don't specify a computer, the local computer is used.
-P `<Printername>`	Specifies the name of the printer that you want to manage. Required.
-z `<newprintername>`	Specifies the new printer name. Requires the **-x** and **-P** parameters.

Parameter	Description
-u `<Username>` -w `<password>`	Specifies an account with permissions to connect to the computer that hosts the printer that you want to manage. All members of the target computer's local Administrators group have these permissions, but the permissions can also be granted to other users. If you don't specify an account, you must be logged on under an account with these permissions for the command to work.
-r `<portname>`	Specifies the port where the printer is connected. If this is a parallel or a serial port, then use the ID of the port (for example, LPT1 or COM1). If this is a TCP/IP port, use the port name that was specified when the port was added.
-l `<location>`	Specifies the printer location, such as **Copyroom**. If the location contains spaces, use quotation marks around the text, such as **"Copy Room"**.
-h `<sharename>`	Specifies the printer's share name.
-m `<comment>`	Specifies the printer's comment string.
-f `<separatorfilename>`	Specifies a file that contains the text that appears on the separator page.
-y `<datatype>`	Specifies the data types that the printer can accept.
-st `<starttime>`	Configures the printer for limited availability. Specifies the time of day the printer is available. If you send a document to a printer when it is unavailable, the document is held (spooled) until the printer becomes available. You must specify time as a 24-hour clock. For example, to specify 11:00 P.M., type **2300**.
-ut `<endtime>`	Configures the printer for limited availability. Specifies the time of day the printer is no longer available. If you send a document to a printer when it is unavailable, the document is held (spooled) until the printer becomes available. You must specify time as a 24-hour clock. For example, to specify 11:00 P.M., type **2300**.
-o `<priority>`	Specifies a priority that the spooler uses to route print jobs into the print queue. A print queue with a higher priority receives all its jobs before any queue with a lower priority.
-i `<defaultpriority>`	Specifies the default priority assigned to each print job.
`{+|-}`shared	Specifies whether this printer is shared on the network.
`{+|-}`direct	Specifies whether the document should be sent directly to the printer without being spooled.

Parameter	Description
{+|-}published	Specifies whether this printer should be published in active directory. If you publish the printer, other users can search for it based on its location and capabilities (such as color printing and stapling).
{+|-}hidden	Reserved function.
{+|-}rawonly	Specifies whether only raw data print jobs can be spooled in this queue.
{+|-}}queued	Specifies that the printer should not begin to print until after the last page of the document is spooled. The printing program is unavailable until the document has finished printing. However, using this parameter ensures that the whole document is available to the printer.
{+|-}keepprintedjobs	Specifies whether the spooler should retain documents after they are printed. Enabling this option allows a user to resubmit a document to the printer from the print queue instead of from the printing program.
{+|-}workoffline	Specifies whether a user is able to send print jobs to the print queue if the computer is not connected to the network.
{+|-}enabledevq	Specifies whether print jobs that don't match the printer setup (for example, PostScript files spooled to non-PostScript printers) should be held in the queue rather than being printed.
{+|-}docompletefirst	Specifies whether the spooler should send print jobs with a lower priority that have completed spooling before sending print jobs with a higher priority that have not completed spooling. If this option is enabled and no documents have completed spooling, the spooler will send larger documents before smaller ones. You should enable this option if you want to maximize printer efficiency at the cost of job priority. If this option is disabled, the spooler always sends higher priority jobs to their respective queues first.
{+|-}enablebidi	Specifies whether the printer sends status information to the spooler.
/?	Displays help at the command prompt.

Examples

To display configuration information for the printer named *colorprinter_2* with a print queue hosted by the remote computer named *HRServer*, type:

```
cscript prncnfg -g -S HRServer -P colorprinter_2
```

To configure a printer named *colorprinter_2* so that the spooler in the remote computer named *HRServer* keeps print jobs after they have been printed, type:

```
cscript prncnfg -t -S HRServer -P colorprinter_2 +keepprintedjobs
```

To change the name of a printer on the remote computer named *HRServer* from *colorprinter_2* to *colorprinter 3*, type:

```
cscript prncnfg -x -S HRServer -P colorprinter_2 -z "colorprinter 3"
```

Related links

- Command-Line Syntax Key
- Print Command Reference

prndrvr

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds, deletes, and lists printer drivers. This command is a Visual Basic script located in the `%WINdir%\System32\printing_Admin_Scripts\<language>` directory. To use this command at a command prompt, type **cscript** followed by the full path to the prndrvr file, or change directories to the appropriate folder. For example: `cscript %WINdir%\System32\printing_Admin_Scripts\en-US\prndrvr`.

Used without parameters, **prndrvr** displays command-line help.

Syntax

```
cscript prndrvr {-a | -d | -l | -x | -?} [-m <model>] [-v {0|1|2|3}] [-e
<environment>] [-s <Servername>] [-u <Username>] [-w <password>] [-h <path>]
[-i <inf file>]
```

Parameters

Parameter	Description
-a	Installs a driver.
-d	Deletes a driver.
-l	Lists all printer drivers installed on the server specified by the **-s** parameter. If you don't specify a server, Windows lists the printer drivers installed on the local computer.
-x	Deletes all printer drivers and additional printer drivers not in use by a logical printer on the server specified by the **-s** parameter. If you don't specify a server to remove from the list, Windows deletes all unused printer drivers on the local computer.
-m `<model_name>`	Specifies (by name) the driver you want to install. Drivers are often named for the model of printer they support. See the printer documentation for more information.

Parameter	Description
`-v {0|1|2|3}`	Specifies the version of the driver you want to install. See the description of the **-e**parameter for information on which versions are available for which environment. If you don't specify a version, the version of the driver appropriate for the version of Windows running on the computer where you are installing the driver is installed.
-e `<environment>`	Specifies the environment for the driver you want to install. If you don't specify an environment, the environment of the computer where you are installing the driver is used. The supported environment parameters are: **Windows NT x86**, **Windows x64** or **Windows IA64**.
-s `<Servername>`	Specifies the name of the remote computer that hosts the printer that you want to manage. If you don't specify a computer, the local computer is used.
-u `<Username>` -w `<password>`	Specifies an account with permissions to connect to the computer that hosts the printer that you want to manage. All members of the target computer's local Administrators group have these permissions, but the permissions can also be granted to other users. If you don't specify an account, you must be logged on under an account with these permissions for the command to work.
-h `<path>`	Specifies the path to the driver file. If you don't specify a path, the path to the location where Windows was installed is used.
-i `<filename.inf>`	Specifies the complete path and file name for the driver you want to install. If you don't specify a file name, the script uses one of the inbox printer .inf files in the inf subdirectory of the Windows directory. if the driver path is not specified, the script searches for driver files in the driver.cab file.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces, use quotation marks around the text (for example, "Computer Name").
- The **-x** parameter deletes all additional printer drivers (drivers installed for use on clients running alternate versions of Windows), even if the primary driver is in use. If the fax component is installed, this option also deletes fax drivers. The primary fax driver is deleted if it is not in use (that is, if there is no queue using it). If the primary fax driver is deleted, the only way to re-enable fax is to reinstall the fax component.

Examples

To list all drivers on the local \printServer1 server, type:

```
cscript prndrvr -l -s
```

To add a version 3 Windows x64 printer driver for the Laser printer model 1 model of printer using the c:\temp\Laserprinter1.inf driver information file for a driver stored in the c:\temp folder, type:

```
cscript prndrvr -a -m Laser printer model 1 -v 3 -e Windows x64 -i
c:\temp\Laserprinter1.inf -h c:\temp
```

To delete a version 3 Windows x64 printer driver for Laser printer model 1, type:

```
cscript prndrvr -a -m Laser printer model 1 -v 3 -e Windows x64
```

Related links

- Command-Line Syntax Key
- Print Command Reference

prnjobs

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Pauses, resumes, cancels, and lists print jobs. This command is a Visual Basic script located in the `%WINdir%\System32\printing_Admin_Scripts\<language>` directory. To use this command at a command prompt, type **cscript** followed by the full path to the prnjobs file, or change directories to the appropriate folder. For example: `cscript %WINdir%\System32\printing_Admin_Scripts\en-US\prnjobs.vbs`.

Syntax

```
cscript prnjobs {-z | -m | -x | -l | -?} [-s <Servername>] [-p
<Printername>] [-j <JobID>] [-u <Username>] [-w <password>]
```

Parameters

Parameter	Description
-z	Pauses the print job specified by the **-j** parameter.
-m	Resumes the print job specified by the **-j** parameter.
-x	Cancels the print job specified by the **-j** parameter.
-l	Lists all the print jobs in a print queue.
-s `<Servername>`	Specifies the name of the remote computer that hosts the printer that you want to manage. If you don't specify a computer, the local computer is used.
-p `<Printername>`	Required. Specifies the name of the printer that you want to manage.
-j `<JobID>`	Specifies (by ID number) the print job you want to cancel.

Parameter	Description
-u `<Username>` -w `<password>`	Specifies an account with permissions to connect to the computer that hosts the printer that you want to manage. All members of the target computer's local Administrators group have these permissions, but the permissions can also be granted to other users. If you don't specify an account, you must be logged on under an account with these permissions for the command to work.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces, use quotation marks around the text (for example, "Computer Name").

Examples

To pause a print job with a job ID of 27 sent to the remote computer named HRServer for printing on the printer named colorprinter, type:

```
cscript prnjobs.vbs -z -s HRServer -p colorprinter -j 27
```

To list all current print jobs in the queue for the local printer named colorprinter_2, type:

```
cscript prnjobs.vbs -l -p colorprinter_2
```

Related links

- Command-Line Syntax Key
- Print Command Reference

prnmngr

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds, deletes, and lists printers or printer connections, in addition to setting and displaying the default printer. This command is a Visual Basic script located in the `%WINdir%\System32\printing_Admin_Scripts\<language>` directory. To use this command at a command prompt, type **cscript** followed by the full path to the prnmngr file, or change directories to the appropriate folder. For example: `cscript %WINdir%\System32\printing_Admin_Scripts\en-US\prnmngr`.

Syntax

```
cscript prnmngr {-a | -d | -x | -g | -t | -l | -?}[c] [-s <Servername>] [-p
<Printername>] [-m <printermodel>] [-r <portname>] [-u <Username>]
[-w <password>]
```

Parameters

Parameter	Description
-a	Adds a local printer connection.
-d	Deletes a printer connection.
-x	Deletes all printers from the server specified by the **-s** parameter. If you don't specify a server, Windows deletes all printers on the local computer.
-g	Displays the default printer.
-t	Sets the default printer to the printer specified by the **-p** parameter.
-l	Lists all printers installed on the server specified by the **-s** parameter. If you don't specify a server, Windows lists the printers installed on the local computer.
c	Specifies that the parameter applies to printer connections. Can be used with the **-a** and **-x** parameters.

Parameter	Description
-s `<Servername>`	Specifies the name of the remote computer that hosts the printer that you want to manage. If you don't specify a computer, the local computer is used.
-p `<Printername>`	Specifies the name of the printer that you want to manage.
-m `<Modelname>`	Specifies (by name) the driver you want to install. Drivers are often named for the model of printer they support. See the printer documentation for more information.
-r `<portname>`	Specifies the port where the printer is connected. If this is a parallel or a serial port, use the ID of the port (for example, LPT1: or COM1:). If this is a TCP/IP port, use the port name that was specified when the port was added.
-u `<Username>` -w `<password>`	Specifies an account with permissions to connect to the computer that hosts the printer that you want to manage. All members of the target computer's local Administrators group have these permissions, but the permissions can also be granted to other users. If you don't specify an account, you must be logged on under an account with these permissions for the command to work.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces, use quotation marks around the text (for example, "Computer Name").

Examples

To add a printer named colorprinter_2 that is connected to LPT1 on the local computer and requires a printer driver called color printer Driver1, type:

```
cscript prnmngr -a -p colorprinter_2 -m "color printer Driver1" -r lpt1:
```

To delete the printer named colorprinter_2 from the remote computer named HRServer, type:

```
cscript prnmngr -d -s HRServer -p colorprinter_2
```

Related links

- Command-Line Syntax Key
- Print Command Reference

prnport

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates, deletes, and lists standard TCP/IP printer ports, in addition to displaying and changing port configuration. This command is a Visual Basic script located in the `%WINdir%\System32\printing_Admin_Scripts\<language>` directory. To use this command at a command prompt, type **cscript** followed by the full path to the prnport file, or change directories to the appropriate folder. For example: `cscript %WINdir%\System32\printing_Admin_Scripts\en-US\prnport`.

Syntax

```
cscript prnport {-a | -d | -l | -g | -t | -?} [-r <portname>] [-s
<Servername>] [-u <Username>] [-w <password>] [-o {raw | lpr}] [-h
<Hostaddress>] [-q <Queuename>] [-n <portnumber>] -m{e | d} [-i <SNMPindex>]
[-y <communityname>] -2{e | -d}
```

Parameters

Parameter	Description
-a	Creates a standard TCP/IP printer port.
-d	Deletes a standard TCP/IP printer port.
-l	Lists all standard TCP/IP printer ports on the computer specified by the **-s** parameter.
-g	Displays the configuration of a standard TCP/IP printer port.
-t	Configures the port settings for a standard TCP/IP printer port.
-r `<portname>`	Specifies the port to which the printer is connected.
-s `<Servername>`	Specifies the name of the remote computer that hosts the printer that you want to manage. If you don't specify a computer, the local computer is used.

Parameter	Description
-u `<Username>` -w `<password>`	Specifies an account with permissions to connect to the computer that hosts the printer that you want to manage. All members of the target computer's local Administrators group have these permissions, but the permissions can also be granted to other users. If you don't specify an account, you must be logged on under an account with these permissions for the command to work.
-o `{raw|lpr}`	Specifies which protocol the port uses: TCP raw or TCP lpr. The TCP raw protocol is a higher performance protocol on Windows than the lpr protocol. If you use TCP raw, you can optionally specify the port number by using the **-n** parameter. The default port number is 9100.
-h `<Hostaddress>`	Specifies (by IP address) the printer for which you want to configure the port.
-q `<Queuename>`	Specifies the queue name for a TCP raw port.
-n `<portnumber>`	Specifies the port number for a TCP raw port. The default port number is 9100.
-m`{e|d}`	Specifies whether SNMP is enabled. The parameter **e** enables SNMP. The parameter **d** disables SNMP.
-i `<SNMPindex`	Specifies the SNMP index, if SNMP is enabled. For more information, see **Rfc 1759** at the Rfc editor website.
-y `<communityname>`	Specifies the SNMP community name, if SNMP is enabled.
-2`{e|-d}`	Specifies whether double spools (also known as respooling) are enabled for TCP lpr ports. Double spools are necessary because TCP lpr must include an accurate byte count in the control file that is sent to the printer, but the protocol cannot get the count from the local print provider. Therefore, when a file is spooled to a TCP lpr print queue, it is also spooled as a temporary file in the system32 directory. TCP lpr determines the size of the temporary file and sends the size to the server running LPD. The parameter **e** enables double spools. The parameter **d** disables double spools.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces, use quotation marks around the text (for example, "Computer Name").

Examples

To display all standard TCP/IP printing ports on the server \Server1, type:

```
cscript prnport -l -s Server1
```

To delete the standard TCP/IP printing port on the server \Server1 that connects to a network printer at 10.2.3.4, type:

```
cscript prnport -d -s Server1 -r IP_10.2.3.4
```

To add a standard TCP/IP printing port on the server \Server1 that connects to a network printer at 10.2.3.4 and uses the TCP raw protocol on port 9100, type:

```
cscript prnport -a -s Server1 -r IP_10.2.3.4 -h 10.2.3.4 -o raw -n 9100
```

To enable SNMP, specify the "public" community name and set the SNMP index to 1 on a network printer at 10.2.3.4 shared by the server \Server1, type:

```
cscript prnport -t -s Server1 -r IP_10.2.3.4 -me -y public -i 1 -n 9100
```

To add a standard TCP/IP printing port on the local computer that connects to a network printer at 10.2.3.4 and automatically get the device settings from the printer, type:

```
cscript prnport -a -r IP_10.2.3.4 -h 10.2.3.4
```

Related links

- Command-Line Syntax Key
- Print Command Reference

prnqctl

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Prints a test page, pauses or resumes a printer, and clears a printer queue. This command is a Visual Basic script located in the `%WINdir%\System32\printing_Admin_Scripts\<language>` directory. To use this command at a command prompt, type **cscript** followed by the full path to the prnqctl file, or change directories to the appropriate folder. For example: `cscript %WINdir%\System32\printing_Admin_Scripts\en-US\prnqctl`.

Syntax

```
cscript Prnqctl {-z | -m | -e | -x | -?} [-s <Servername>] [-p
<Printername>] [-u <Username>] [-w <password>]
```

Parameters

Parameter	Description
-z	Pauses printing on the printer specified by the **-p** parameter.
-m	Resumes printing on the printer specified by the **-p** parameter.
-e	Prints a test page on the printer specified by the **-p** parameter.
-x	Cancels all print jobs on the printer specified by the **-p** parameter.
-s `<Servername>`	Specifies the name of the remote computer that hosts the printer that you want to manage. If you don't specify a computer, the local computer is used.
-p `<Printername>`	Required. Specifies the name of the printer that you want to manage.
-u `<Username>` -w `<password>`	Specifies an account with permissions to connect to the computer that hosts the printer that you want to manage. All members of the target computer's local Administrators group have these permissions, but the permissions can also be granted to other users. If you don't specify an account, you must be logged on under an account with these permissions for the command to work.

Parameter	Description
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces, use quotation marks around the text (for example, "Computer Name").

Examples

To print a test page on the Laserprinter1 printer shared by the \Server1 computer, type:

```
cscript prnqctl -e -s Server1 -p Laserprinter1
```

To pause printing on the Laserprinter1 printer on the local computer, type:

```
cscript prnqctl -z -p Laserprinter1
```

To cancel all print jobs on the Laserprinter1 printer on the local computer, type:

```
cscript prnqctl -x -p Laserprinter1
```

Related links

- Command-Line Syntax Key
- Print Command Reference

prompt

Article • 02/03/2023

Changes the Cmd.exe command prompt, including displaying any text you want, such as the name of the current directory, the time and date, or the Microsoft Windows version number. If used without parameters, this command resets the command prompt to the default setting, which is the current drive letter and directory followed by the greater than symbol (>).

Syntax

```
prompt [<text>]
```

Parameters

Parameter	Description
`<text>`	Specifies the text and information that you want to include in the command prompt.
/?	Displays help at the command prompt.

Remarks

- The character combinations you can include instead of, or in addition to, one or more character strings in the *text* parameter:

Character	Description
$q	= (Equal sign)
$$	$ (Dollar sign)
$t	Current time
$d	Current date
$p	Current drive and path
$v	Windows version number
$n	Current drive

Character	Description
$g	> (Greater than sign)
$l	< (Less than sign)
$b	| (Pipe symbol)
$_	ENTER-LINEFEED
$e	ANSI escape code (code 27)
$h	Backspace (to delete a character that has been written to the command line)
$a	& (Ampersand)
$c	((Left parenthesis)
$f	) (Right parenthesis)
$s	Space

- When command extensions are enabled the **prompt** command supports the following formatting characters:

Character	Description
$+	Zero or more plus sign (+) characters, depending on the depth of the **pushd** directory stack (one character for each level pushed).
$m	The remote name associated with the current drive letter or the empty string if current drive is not a network drive.

- If you include the **$p** character in the text parameter, your disk is read after you enter each command (to determine the current drive and path). This can take extra time, especially for floppy disk drives.

Examples

To set a two-line command prompt with the current time and date on the first line and the greater than sign on the next line, type:

```
prompt $d$s$s$t$_$g
```

The prompt is changed as follows, where the date and time are current:

```
Fri 06/01/2007  13:53:28.91
```

To set the command prompt to display as an arrow (`-->`), type:

```
prompt --$g
```

To manually change the command prompt to the default setting (the current drive and path followed by the greater than sign), type:

```
prompt $p$g
```

Related links

- Command-Line Syntax Key

pubprn

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Publishes a printer to the Active Directory Domain Services. This command is a Visual Basic script located in the `%WINdir%\System32\printing_Admin_Scripts\<language>` directory. To use this command at a command prompt, type **cscript** followed by the full path to the pubprn file, or change directories to the appropriate folder. For example: `cscript %WINdir%\System32\printing_Admin_Scripts\en-US\pubprn`.

Syntax

```
cscript pubprn {<servername> | <UNCprinterpath>} LDAP://CN=<container>,DC=
<container>
```

Parameters

Parameter	Description
`<servername>`	Specifies the name of the Windows server that hosts the printer that you want to publish. If you don't specify a computer, the local computer is used.
`<UNCprinterpath>`	The Universal Naming Convention (UNC) path to the shared printer that you want to publish.
`LDAP://CN=<Container>,DC=<Container>`	Specifies the path to the container in Active Directory Domain Services where you want to publish the printer.
/?	Displays help at the command prompt.

Remarks

- If the information that you supply contains spaces, use quotation marks around the text (for example, "Computer Name").

Examples

To publish all printers on the \Server1 computer to the MyContainer container in the MyDomain.company.com domain, type:

```
cscript pubprn Server1 LDAP://CN=MyContainer,DC=MyDomain,DC=company,DC=Com
```

To publish the Laserprinter1 printer on the \\Server1 server to the MyContainer container in the MyDomain.company.com domain, type:

```
cscript pubprn \\Server1\Laserprinter1
LDAP://CN=MyContainer,DC=MyDomain,DC=company,DC=Com
```

Related links

- Command-Line Syntax Key
- Print Command Reference

pushd

Article • 02/03/2023

Stores the current directory for use by the **popd** command, and then changes to the specified directory.

Every time you use the **pushd** command, a single directory is stored for your use. However, you can store multiple directories by using the **pushd** command multiple times. The directories are stored sequentially in a virtual stack, so if you use the **pushd** command once, the directory in which you use the command is placed at the bottom of the stack. If you use the command again, the second directory is placed on top of the first one. The process repeats every time you use the **pushd** command.

If you use the **popd** command, the directory on the top of the stack is removed and the current directory is changed to that directory. If you use the **popd** command again, the next directory on the stack is removed. If command extensions are enabled, the **popd** command removes any drive-letter assignment created by the **pushd** command.

Syntax

```
pushd [<path>]
```

Parameters

Parameter	Description
`<path>`	Specifies the directory to make the current directory. This command supports relative paths.
/?	Displays help at the command prompt.

Remarks

- If command extensions are enabled, the **pushd** command accepts either a network path or a local drive letter and path.
- If you specify a network path, the **pushd** command temporarily assigns the highest unused drive letter (starting with Z:) to the specified network resource. The

command then changes the current drive and directory to the specified directory on the newly assigned drive. If you use the **popd** command with command extensions enabled, the **popd** command removes the drive-letter assignment created by **pushd**.

Examples

To change the current directory from the one in which the batch program was run, and then to change it back:

```
@echo off
rem This batch file deletes all .txt files in a specified directory
pushd %1
del *.txt
popd
cls
echo All text files deleted in the %1 directory
```

Related links

- Command-Line Syntax Key
- popd command

pushprinterconnections

Article • 02/03/2023

Reads Deployed Printer Connection settings from Group Policy and deploys/removes printer connections as needed.

> **Important**
>
> This utility is for use in machine startup or user logon scripts, and shouldn't be run from the command line.

Syntax

```
pushprinterconnections <-log> <-?>
```

Parameters

Parameter	Description
<-log>	Writes a per user debug log file to *%temp*, or writes a per machine debug log to *%windir%\temp*.
<-?>	Displays Help at the command prompt.

Related links

- Command-Line Syntax Key
- Print Command Reference
- Deploy Printers by Using Group Policy

pwlauncher

Article • 02/03/2023

Enables or disables the Windows To Go Startup Options (pwlauncher). The **pwlauncher** command-line tool allows you to configure the computer to boot into a Windows To Go workspace automatically (assuming one is present), without requiring you to enter your firmware or change your startup options.

Windows To Go Startup Options allow a user to configure their computer to boot from USB from within Windows-without ever entering their firmware, as long as their firmware supports booting from USB. Enabling a system to always boot from USB first has implications that you should consider. For example, a USB device that includes malware could be booted inadvertently to compromise the system, or multiple USB drives could be plugged in to cause a boot conflict. For this reason, the default configuration has the Windows To Go Startup Options disabled by default. In addition, administrator privileges are required to configure Windows To Go Startup Options. If you enable the Windows To Go startup options using the pwlauncher command-line tool or the **Change Windows To Go Startup Options** app the computer will attempt to boot from any USB device that is inserted into the computer before it is started.

Syntax

```
pwlauncher {/enable | /disable}
```

Parameters

Parameter	Description
/enable	Enables Windows To Go startup options, so the computer will automatically boot from a USB device when present.
/disable	Disables Windows To Go startup options, so the computer can't be booted from a USB device unless configured manually in the firmware.
/?	Displays help at the command prompt.

Examples

To enable boot from USB:

```
pwlauncher /enable
```

Related links

- Command-Line Syntax Key

qappsrv

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays a list of all Remote Desktop Session Host servers on the network. To find out what's new in the latest version, see What's New in Remote Desktop Services in Windows Server.

> **Note**
>
> This command is the same as the **query termserver command**.

Related links

- Command-Line Syntax Key
- query termserver command
- Remote Desktop Services (Terminal Services) Command Reference

qprocess

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about processes that are running on a Remote Desktop Session Host server. To find out what's new in the latest version, see What's New in Remote Desktop Services in Windows Server.

> **Note**
>
> This command is the same as the **query process command**.

Related links

- Command-Line Syntax Key
- query process command
- Remote Desktop Services (Terminal Services) Command Reference

query commands

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about processes, sessions, and Remote Desktop Session Host servers. To find out what's new in the latest version, see What's New in Remote Desktop Services in Windows Server.

Syntax

```
query process
query session
query termserver
query user
```

Parameters

Parameter	Description
query process	Displays information about processes running on an Remote Desktop Session Host server.
query session	Displays information about sessions on a Remote Desktop Session Host server.
query termserver	Displays a list of all Remote Desktop Session Host servers on the network.
query user	Displays information about user sessions on a Remote Desktop Session Host server.

Related links

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

query process

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about processes that are running on a Remote Desktop Session Host server. You can use this command to find out which programs a specific user is running, and also which users are running a specific program. This command returns the following information:

- User who owns the process
- Session that owns the process
- ID of the session
- Name of the process
- ID of the process

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
query process [*|<processID>|<username>|<sessionname>|/id:<nn>|
<programname>] [/server:<servername>]
```

Parameters

Parameter	Description
*	Lists the processes for all sessions.
`<processID>`	Specifies the numeric ID identifying the process that you want to query.

Parameter	Description
`<username>`	Specifies the name of the user whose processes you want to list.
`<sessionname>`	Specifies the name of the active session whose processes you want to list.
/id:`<nn>`	Specifies the ID of the session whose processes you want to list.
`<programname>`	Specifies the name of the program whose processes you want to query. The .exe extension is required.
/server:`<servername>`	Specifies the Remote Desktop Session Host server whose processes you want to list. If unspecified, the server where you are currently logged on is used.
/?	Displays help at the command prompt.

Remarks

- Administrators have full access to all **query process** functions.
- If you don't specify the *<username>*, *<sessionname>*, */id:*`<nn>`, *<programname>*, or * parameters, this query displays only the processes that belong to the current user.
- When **query process** returns information, a greater than `(>)` symbol is displayed before each process that belongs to the current session.

Examples

To display information about the processes being used by all sessions, type:

```
query process *
```

To display information about the processes being used by *session ID 2*, type:

```
query process /ID:2
```

Related links

- Command-Line Syntax Key
- query command
- Remote Desktop Services (Terminal Services) Command Reference

query session

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about sessions on a Remote Desktop Session Host server. The list includes information not only about active sessions but also about other sessions that the server runs.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
query session [<sessionname> | <username> | <sessionID>] [/server:
<servername>] [/mode] [/flow] [/connect] [/counter]
```

Parameters

Parameter	Description
`<sessionname>`	Specifies the name of the session that you want to query.
`<username>`	Specifies the name of the user whose sessions you want to query.
`<sessionID>`	Specifies the ID of the session that you want to query.
/server:`<servername>`	Identifies the rd Session Host server to query. The default is the current server.
/mode	Displays current line settings.
/flow	Displays current flow-control settings.
/connect	Displays current connect settings.

Parameter	Description
/counter	Displays current counters information, including the total number of sessions created, disconnected, and reconnected.
/?	Displays help at the command prompt.

Remarks

- A user can always query the session to which the user is currently logged on. To query other sessions, the user must have special access permission.
- If you don't specify a session using the <*username*>, <*sessionname*>, or *sessionID* parameters, this query will display information about all active sessions in the system.
- When **query session** returns information, a greater than `(>)` symbol is displayed before the current session. For example:

```
C:\>query session
    SESSIONNAME     USERNAME        ID STATE    TYPE    DEVICE
    console         Administrator1  0 active    wdcon
    >rdp-tcp#1      User1           1 active    wdtshare
    rdp-tcp                         2 listen    wdtshare
                                    4 idle
                                    5 idle
```

  Where:
  - **SESSIONNAME** specifies the name assigned to the session.
  - **USERNAME** indicates the user name of the user connected to the session.
  - **STATE** provides information about the current state of the session.
  - **TYPE** indicates the session type.
  - **DEVICE**, which isn't present for the console or network-connected sessions, is the device name assigned to the session.
  - Any sessions in which the initial state is configured as DISABLED won't show up in the **query session** list until they're enabled.

Examples

To display information about all active sessions on server *Server2*, type:

```
query session /server:Server2
```

To display information about active session *modeM02*, type:

```
query session modeM02
```

Related links

- Command-Line Syntax Key
- query command
- Remote Desktop Services (Terminal Services) Command Reference

query termserver

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays a list of all Remote Desktop Session Host servers on the network. This command searches the network for all attached Remote Desktop Session Host servers and returns the following information:

- Name of the server
- Network (and node address if the /address option is used)

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
query termserver [<servername>] [/domain:<domain>] [/address] [/continue]
```

Parameters

Parameter	Description
`<servername>`	Specifies the name that identifies the Remote Desktop Session Host server.
/domain:`<domain>`	Specifies the domain to query for terminal servers. You don't need to specify a domain if you are querying the domain in which you are currently working.
/address	Displays the network and node addresses for each server.
/continue	Prevents pausing after each screen of information is displayed.
/?	Displays help at the command prompt.

Examples

To display information about all Remote Desktop Session Host servers on the network, type:

```
query termserver
```

To display information about the Remote Desktop Session Host server named *Server3*, type:

```
query termserver Server3
```

To display information about all Remote Desktop Session Host servers in domain *CONTOSO*, type:

```
query termserver /domain:CONTOSO
```

To display the network and node address for the Remote Desktop Session Host server named *Server3*, type:

```
query termserver Server3 /address
```

Related links

- Command-Line Syntax Key
- query command
- Remote Desktop Services (Terminal Services) Command Reference

query user

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about user sessions on a Remote Desktop Session Host server. You can use this command to find out if a specific user is logged on to a specific Remote Desktop Session Host server. This command returns the following information:

- Name of the user
- Name of the session on the Remote Desktop Session Host server
- Session ID
- State of the session (active or disconnected)
- Idle time (the number of minutes since the last keystroke or mouse movement at the session)
- Date and time the user logged on

> ⓘ **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
query user [<username> | <sessionname> | <sessionID>] [/server:<servername>]
```

Parameters

Parameter	Description
`<username>`	Specifies the logon name of the user that you want to query.

Parameter	Description
`<sessionname>`	Specifies the name of the session that you want to query.
`<sessionID>`	Specifies the ID of the session that you want to query.
/server:`<servername>`	Specifies the Remote Desktop Session Host server that you want to query. Otherwise, the current Remote Desktop Session Host server is used. This parameter is only required if you're using this command from a remote server.
/?	Displays help at the command prompt.

Remarks

- To use this command, you must have Full Control permission or special access permission.
- If you don't specify a user using the *<username>*, *<sessionname>*, or *sessionID* parameters, a list of all users who are logged on to the server is returned. Alternatively, you can also use the **query session** command to display a list of all sessions on a server.
- When **query user** returns information, a greater than `(>)` symbol is displayed before the current session.

Examples

To display information about all users logged on the system, type:

```
query user
```

To display information about the user *USER1* on server *Server1*, type:

```
query user USER1 /server:Server1
```

Related links

- Command-Line Syntax Key

- query command
- Remote Desktop Services (Terminal Services) Command Reference

quser

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about user sessions on a Remote Desktop Session Host server. You can use this command to find out if a specific user is logged on to a specific Remote Desktop Session Host server. This command returns the following information:

- Name of the user
- Name of the session on the Remote Desktop Session Host server
- Session ID
- State of the session (active or disconnected)
- Idle time (the number of minutes since the last keystroke or mouse movement at the session)
- Date and time the user logged on

> **Note**
>
> This command is the same as the **query user command**. To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
quser [<username> | <sessionname> | <sessionID>] [/server:<servername>]
```

Parameters

Parameter	Description
`<username>`	Specifies the logon name of the user that you want to query.

Parameter	Description
`<sessionname>`	Specifies the name of the session that you want to query.
`<sessionID>`	Specifies the ID of the session that you want to query.
/server:`<servername>`	Specifies the Remote Desktop Session Host server that you want to query. Otherwise, the current Remote Desktop Session Host server is used. This parameter is only required if you're using this command from a remote server.
/?	Displays help at the command prompt.

Remarks

- To use this command, you must have Full Control permission or special access permission.
- If you don't specify a user using the *<username>*, *<sessionname>*, or *sessionID* parameters, a list of all users who are logged on to the server is returned. Alternatively, you can also use the **query session** command to display a list of all sessions on a server.
- When **quser** returns information, a greater than `(>)` symbol is displayed before the current session.

Examples

To display information about all users logged on the system, type:

```
quser
```

To display information about the user *USER1* on server *Server1*, type:

```
quser USER1 /server:Server1
```

Related links

- Command-Line Syntax Key

- query user command
- Remote Desktop Services (Terminal Services) Command Reference

qwinsta

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about sessions on a Remote Desktop Session Host server. The list includes information not only about active sessions but also about other sessions that the server runs.

> **Note**
>
> This command is the same as the **query session command**. To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
qwinsta [<sessionname> | <username> | <sessionID>] [/server:<servername>]
[/mode] [/flow] [/connect] [/counter]
```

Parameters

Parameter	Description
`<sessionname>`	Specifies the name of the session that you want to query.
`<username>`	Specifies the name of the user whose sessions you want to query.
`<sessionID>`	Specifies the ID of the session that you want to query.
/server:`<servername>`	Identifies the rd Session Host server to query. The default is the current server.
/mode	Displays current line settings.
/flow	Displays current flow-control settings.
/connect	Displays current connect settings.

Parameter	Description
/counter	Displays current counters information, including the total number of sessions created, disconnected, and reconnected.
/?	Displays help at the command prompt.

Remarks

- A user can always query the session to which the user is currently logged on. To query other sessions, the user must have special access permission.
- If you don't specify a session using the *<username>*, *<sessionname>*, or *sessionID* parameters, this query will display information about all active sessions in the system.
- When **qwinsta** returns information, a greater than `(>)` symbol is displayed before the current session. For example:

```
C:\>qwinsta
    SESSIONNAME     USERNAME        ID STATE    TYPE    DEVICE
    console         Administrator1  0 active    wdcon
    >rdp-tcp#1      User1           1 active    wdtshare
    rdp-tcp                         2 listen    wdtshare
                                    4 idle
                                    5 idle
```

  Where:
  - **SESSIONNAME** specifies the name assigned to the session.
  - **USERNAME** indicates the user name of the user connected to the session.
  - **STATE** provides information about the current state of the session.
  - **TYPE** indicates the session type.
  - **DEVICE**, which isn't present for the console or network-connected sessions, is the device name assigned to the session.
  - Any sessions in which the initial state is configured as DISABLED won't show up in the **qwinsta** list until they're enabled.

Examples

To display information about all active sessions on server *Server2*, type:

```
qwinsta /server:Server2
```

To display information about active session *modeM02*, type:

```
qwinsta modeM02
```

Related links

- Command-Line Syntax Key
- query session command
- Remote Desktop Services (Terminal Services) Command Reference

rd

Article • 02/03/2023

Deletes a directory.

The **rd** command can also run from the Windows Recovery Console, using different parameters. For more information, see Windows Recovery Environment (WinRE).

> **Note**
>
> This command is the same as the **rmdir command**.

Syntax

```
rd [<drive>:]<path> [/s [/q]]
```

Parameters

Parameter	Description
`[<drive>:]<path>`	Specifies the location and the name of the directory that you want to delete. *Path* is required. If you include a backslash () at the beginning of the specified *path*, then the *path* starts at the root directory (regardless of the current directory).
/s	Deletes a directory tree (the specified directory and all its subdirectories, including all files).
/q	Specifies quiet mode. Does not prompt for confirmation when deleting a directory tree. The **/q** parameter works only if **/s** is also specified. **CAUTION:** When you run in quiet mode, the entire directory tree is deleted without confirmation. Make sure that important files are moved or backed up before using the **/q** command-line option.
/?	Displays help at the command prompt.

Remarks

- You can't delete a directory that contains files, including hidden or system files. If you attempt to do so, the following message appears:

`The directory is not empty`

Use the **dir /a** command to list all files (including hidden and system files). Then use the **attrib** command with **-h** to remove hidden file attributes, **-s** to remove system file attributes, or **-h -s** to remove both hidden and system file attributes. After the hidden and file attributes have been removed, you can delete the files.

- You can't use the **rd** command to delete the current directory. If you attempt to delete the current directory, the following error message appears:

  `The process can't access the file because it is being used by another process.`

  If you receive this error message, you must change to a different directory (not a subdirectory of the current directory), and then try again.

Examples

To change to the parent directory so you can safely remove the desired directory, type:

```
cd ..
```

To remove a directory named *test* (and all its subdirectories and files) from the current directory, type:

```
rd /s test
```

To run the previous example in quiet mode, type:

```
rd /s /q test
```

Related links

- Command-Line Syntax Key

rdpsign

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables you to digitally sign a Remote Desktop Protocol (.rdp) file.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
rdpsign /sha1 <hash> [/q | /v |] [/l] <file_name.rdp>
```

Parameters

Parameter	Description
/sha1 `<hash>`	Specifies the thumbprint, which is the Secure Hash Algorithm 1 (SHA1) hash of the signing certificate that is included in the certificate store. Used in Windows Server 2012 R2 and older.
/sha256 `<hash>`	Specifies the thumbprint, which is the Secure Hash Algorithm 256 (SHA256) hash of the signing certificate that is included in the certificate store. Replaces /sha1 in Windows Server 2016 and newer.
/q	Quiet mode. No output when the command succeeds and minimal output if the command fails.
/v	verbose mode. Displays all warnings, messages, and status.
/l	Tests the signing and output results without actually replacing any of the input files.
`<file_name.rdp>`	The name of the .rdp file. You must specify the .rdp file (or files) to sign by using the full file name. Wildcard characters are not accepted.

Parameter	Description
/?	Displays help at the command prompt.

Remarks

- The SHA1 or SHA256 certificate thumbprint should represent a trusted .rdp file publisher. To obtain the certificate thumbprint, open the **Certificates** snap-in, double-click the certificate that you want to use (either in the local computer's certificates store or in your personal certificates store), click the **details** tab, and then in the **Field** list, click **Thumbprint**.

  > **Note**
  >
  > When you copy the thumbprint for use with the rdpsign.exe tool, you must remove any spaces.

- The signed output files overwrite the input files.
- If multiple files are specified, and if any of the .rdp files can't be read or written to, the tool continues to the next file.

Examples

To sign an .rdp file named *file1.rdp*, navigate to the folder where you saved the .rdp file, and then type:

```
rdpsign /sha1 hash file1.rdp
```

> **Note**
>
> The *hash* value represents the SHA1 certificate thumbprint, without any spaces.

To test whether digital signing will succeed for an .rdp file without actually signing the file, type:

```
rdpsign /sha1 hash /l file1.rdp
```

To sign multiple .rdp files that are named, *file1.rdp*, *file2.rdp*, and *file3.rdp*, type (including the spaces between file names):

```
rdpsign /sha1 hash file1.rdp file2.rdp file3.rdp
```

See Also

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

recover (DiskPart)

Article • 02/03/2023

Refreshes the state of all disks in a disk group, attempt to recover disks in an invalid disk group, and resynchronizes mirrored volumes and RAID-5 volumes that have stale data. This command operates on disks that are failed or failing. It also operates on volumes that are failed, failing, or in failed redundancy state.

This command operates on groups of dynamic disks. If this command is used on a group with a basic disk, it won't return an error, but no action will be taken.

> **Note**
>
> A disk that is part of a disk group must be selected for this operation to succeed. Use the **select disk command** to select a disk and shift the focus to it.

Syntax

```
recover [noerr]
```

Parameters

Parameter	Description
noerr	For scripting only. When an error is encountered, DiskPart continues to process commands as if the error did not occur. Without this parameter, an error causes DiskPart to exit with an error code.

Examples

To recover the disk group that contains the disk with focus, type:

```
recover
```

Related links

- Command-Line Syntax Key

ReFSUtil

Article • 02/14/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10

ReFSUtil is a tool included in Windows and Windows Server that attempts to diagnose heavily damaged ReFS volumes, identify remaining files, and copy those files to another volume. This tool comes in the `%SystemRoot%\Windows\System32` folder.

ReFS salvage is the primary function of ReFSUtil, and is useful for recovering data from volumes that show as RAW in Disk Management. ReFS Salvage has two phases: Scan Phase and a Copy Phase. In automatic mode, the Scan Phase and Copy Phase will run sequentially. In manual mode, each phase can be run separately. Progress and logs are saved in a working directory to allow phases to be run separately as well as Scan Phase to be paused and resumed. You shouldn't need to use the ReFSutil tool unless the volume is RAW. If read-only, then data is still accessible.

Parameters

Parameter	Description
`<source volume>`	Specifies the ReFS volume to process. The drive letter must be formatted as "L:", or you must provide a path to the volume mount point.
`<working directory>`	Specifies the location to store temporary information and logs. It must **not** be located on the `<source volume>`.
`<target directory>`	Specifies the location where identified files are copied to. It must **not** be located on the `<source volume>`.
-m	Recovers all possible files including deleted ones. **WARNING:** Not only does this parameter cause the process to take longer to run, but it can also lead to unexpected results.
-v	Specifies to use verbose mode.
-x	Forces the volume to dismount first, if necessary. All opened handles to the volume are then invalid. For example, `refsutil salvage -QA R: N:\WORKING N:\DATA -x`.

Usage and available options

Quick automatic mode

Performs a Quick Scan Phase followed by a Copy Phase. This mode runs quicker as it assumes some critical structures of the volume aren't corrupted and so there's no need to scan the entire volume to locate them. This also reduces the recovery of stale files/directories/volumes.

```
refsutil salvage -QA <source volume> <working directory> <target directory>
<options>
```

Full automatic mode

Performs a Full Scan Phase followed by a Copy Phase. This mode may take a long time as it will scan the entire volume for any recoverable files/directories/volumes.

```
refsutil salvage -FA <source volume> <working directory> <target directory>
<options>
```

Diagnose phase (manual mode)

First, try to determine if the `<source volume>` is an ReFS volume and determine if the volume is mountable. If a volume isn't mountable, the reason(s) will be provided. This is a standalone phase.

```
refsutil salvage -D <source volume> <working directory> <options>
```

Quick Scan phase

Performs a Quick Scan of the `<source volume>` for any recoverable files. This mode runs quicker as it assumes some critical structures of the volume aren't corrupted and so there's no need to scan the entire volume to locate them. This also reduces the recovery of stale files/directories/volumes. Discovered files are logged to the `foundfiles.<volume signature>.txt` file, located in your `<working directory>`. If the Scan Phase was previously stopped, running with the **-QS** flag again resumes the scan from where it left off.

```
refsutil salvage -QS <source volume> <working directory> <options>
```

Full Scan phase

Scans the entire `<source volume>` for any recoverable files. This mode may take a long time as it will scan the entire volume for any recoverable files. Discovered files will be logged to the `foundfiles.<volume signature>.txt` file, located in your `<working directory>`. If the Scan Phase was previously stopped, running with the **-FS** flag again resumes the scan from where it left off.

```
refsutil salvage -FS <source volume> <working directory> <options>
```

Copy phase

Copies all files described in the `foundfiles.<volume signature>.txt` file to your `<target directory>`. If you stop the Scan Phase too early, it's possible that the `foundfiles.<volume signature>.txt` file might not yet exist, so no file is copied to the `<target directory>`.

```
refsutil salvage -C <source volume> <working directory> <target directory>
<options>
```

Copy phase with list

Copies all the files in the `<file list>` from the `<source volume>` to your `<target directory>`. The files in the `<file list>` must have first been identified by the Scan Phase, though the scan need not have been run to completion. The `<file list>` can be generated by copying `foundfiles.<volume signature>.txt` to a new file, removing lines referencing files that shouldn't be restored, and preserving files that should be restored. The PowerShell cmdlet **Select-String** may be helpful in filtering `foundfiles.<volume signature>.txt` to only include desired paths, extensions, or file names.

```
```

```
refsutil salvage -SL <source volume> <working directory> <target directory>
<file list> <options>
```

Copy phase with interactive console

Advanced users can salvage files using an interactive console. This mode also requires files generated from either of the Scan Phases.

```
refsutil salvage -IC <source volume> <working directory> <options>
```

Related links

- Command-Line Syntax Key

reg commands

Article • 02/03/2023

Performs operations on registry subkey information and values in registry entries.

Some operations enable you to view or configure registry entries on local or remote computers, while others allow you to configure only local computers. Using **reg** to configure the registry of remote computers limits the parameters that you can use in some operations. Check the syntax and parameters for each operation to verify that they can be used on remote computers.

> **⊗ Caution**
>
> Don't edit the registry directly unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can degrade performance, damage your system, or even require you to reinstall Windows. You can safely alter most registry settings by using the programs in Control Panel or Microsoft Management Console (MMC). If you must edit the registry directly, back it up first.

Syntax

```
reg add
reg compare
reg copy
reg delete
reg export
reg import
reg load
reg query
reg restore
reg save
reg unload
```

Parameters

Parameter	Description
reg add	Adds a new subkey or entry to the registry.

Parameter	Description
reg compare	Compares specified registry subkeys or entries.
reg copy	Copies a registry entry to a specified location on the local or remote computer.
reg delete	Deletes a subkey or entries from the registry.
reg export	Copies the specified subkeys, entries, and values of the local computer into a file for transfer to other servers.
reg import	Copies the contents of a file that contains exported registry subkeys, entries, and values into the registry of the local computer.
reg load	Writes saved subkeys and entries into a different subkey in the registry.
reg query	Returns a list of the next tier of subkeys and entries that are located under a specified subkey in the registry.
reg restore	Writes saved subkeys and entries back to the registry.
reg save	Saves a copy of specified subkeys, entries, and values of the registry in a specified file.
reg unload	Removes a section of the registry that was loaded using the **reg load** operation.

Related links

- Command-Line Syntax Key

reg add

Article • 01/03/2024

Adds a new subkey or entry to the registry.

Syntax

```
reg add <keyname> [/v valuename | /ve] [/t datatype] [/s separator] [/d
data] [/f] [/reg:32 | /reg:64]
```

Parameters

Expand table

Parameter	Description
`<keyname>`	Specifies the full path of the subkey or entry to be added. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: • **HKCR** (HKEY_CLASSES_ROOT) • **HKCU** (HKEY_CURRENT_USER) • **HKLM** (HKEY_LOCAL_MACHINE) • **HKU** (HKEY_USERS) • **HKCC** (HKEY_CURRENT_CONFIG) If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
/v `<Valuename>`	Specifies the name of the add registry entry.
/ve	Specifies that the added registry entry has a null value.
/t `<Type>`	Specifies the type for the registry entry. *Type* must be one of the following: • REG_SZ • REG_MULTI_SZ • REG_DWORD_BIG_ENDIAN • REG_DWORD

Parameter	Description
	• REG_BINARY • REG_DWORD_LITTLE_ENDIAN • REG_LINK • REG_FULL_RESOURCE_DESCRIPTOR • REG_EXPAND_SZ
/s `<Separator>`	Specifies the character to be used to separate multiple instances of data when the **REG_MULTI_SZ** data type is specified and more than one entry is listed. If not specified, the default separator is **\0**.
/d `<Data>`	Specifies the data for the new registry entry.
/f	Adds the registry entry without prompting for confirmation.
/reg:32	Specifies the key should be accessed using the 32-bit registry view.
/reg:64	Specifies the key should be accessed using the 64-bit registry view.
/?	Displays help at the command prompt.

Remarks

- Subtrees can't be added with this operation. This version of **reg** doesn't ask for confirmation when adding a subkey.
- The return values for the **reg add** operation are:

Expand table

Value	Description
0	Success
1	Failure

- For the **REG_EXPAND_SZ** key type, use the caret symbol (^) with % inside the /d parameter.

Examples

To add the key *HKLM\Software\MyCo* on remote computer *ABC*, type:

```
reg add \\ABC\HKLM\Software\MyCo
```

To add a registry entry to *HKLM\Software\MyCo* with a value named *Data*, the type *REG_BINARY*, and data of *fe340ead*, type:

```
reg add HKLM\Software\MyCo /v Data /t REG_BINARY /d fe340ead
```

To add a multi-valued registry entry to *HKLM\Software\MyCo* with a value named *MRU*, the type *REG_MULTI_SZ*, and data of *fax\0mail\0*, type:

```
reg add HKLM\Software\MyCo /v MRU /t REG_MULTI_SZ /d fax\0mail\0
```

To add an expanded registry entry to *HKLM\Software\MyCo* with a value named *Path*, the type *REG_EXPAND_SZ*, and data of *%systemroot%*, type:

```
reg add HKLM\Software\MyCo /v Path /t REG_EXPAND_SZ /d ^%systemroot^%
```

Related links

- Command-Line Syntax Key

reg compare

Article • 02/03/2023

Compares specified registry subkeys or entries.

Syntax

```
reg compare <keyname1> <keyname2> [{/v Valuename | /ve}] [{/oa | /od | /os | on}] [/s]
```

Parameters

Parameter	Description
`<keyname1>`	Specifies the full path of the subkey or entry to be added. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
`<keyname2>`	Specifies the full path of the second subkey to be compared. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. Specifying only the computer name in *keyname2* causes the operation to use the path to the subkey specified in *keyname1*. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
/v `<Valuename>`	Specifies the value name to compare under the subkey.
/ve	Specifies that only entries that have a value name of null should be compared.
/oa	Specifies that all differences and matches are displayed. By default, only the differences are listed.
/od	Specifies that only differences are displayed. This is the default behavior.

Parameter	Description
/os	Specifies that only matches are displayed. By default, only the differences are listed.
/on	Specifies that nothing is displayed. By default, only the differences are listed.
/s	Compares all subkeys and entries recursively.
/?	Displays help at the command prompt.

Remarks

- The return values for the **reg compare** operation are:

Value	Description
0	The comparison is successful and the result is identical.
1	The comparison failed.
2	The comparison was successful and differences were found.

- The symbols displayed in the results, include:

Symbol	Description
=	*KeyName1* data is equal to *KeyName2* data.
<	*KeyName1* data is less than *KeyName2* data.
>	*KeyName1* data is greater than *KeyName2* data.

Examples

To compare all values under the key **MyApp** with all values under the key **SaveMyApp**, type:

```
reg compare HKLM\Software\MyCo\MyApp HKLM\Software\MyCo\SaveMyApp
```

To compare the value for the Version under the key **MyCo** and the value for the Version under the key **MyCo1**, type:

```
```

```
reg compare HKLM\Software\MyCo HKLM\Software\MyCo1 /v Version
```

To compare all subkeys and values under HKLM\Software\MyCo on the computer named ZODIAC, with all subkeys and values under HKLM\Software\MyCo on the local computer, type:

```
reg compare \\ZODIAC\HKLM\Software\MyCo \\. /s
```

Related links

- Command-Line Syntax Key

reg copy

Article • 02/03/2023

Copies a registry entry to a specified location on the local or remote computer.

Syntax

```
reg copy <keyname1> <keyname2> [/s] [/f]
```

Parameters

Parameter	Description
`<keyname1>`	Specifies the full path of the subkey or entry to be added. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
`<keyname2>`	Specifies the full path of the second subkey to be compared. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
/s	Copies all subkeys and entries under the specified subkey.
/f	Copies the subkey without prompting for confirmation.
/?	Displays help at the command prompt.

Remarks

- This command doesn't ask for confirmation when copying a subkey.
- The return values for the **reg compare** operation are:

Value	Description
0	Success
1	Failure

Examples

To copy all subkeys and values under the key MyApp to the key SaveMyApp, type:

```
reg copy HKLM\Software\MyCo\MyApp HKLM\Software\MyCo\SaveMyApp /s
```

To copy all values under the key MyCo on the computer named ZODIAC to the key MyCo1 on the current computer, type:

```
reg copy \\ZODIAC\HKLM\Software\MyCo HKLM\Software\MyCo1
```

Related links

- Command-Line Syntax Key

reg delete

Article • 02/03/2023

Deletes a subkey or entries from the registry.

Syntax

```
reg delete <keyname> [{/v valuename | /ve | /va}] [/f]
```

Parameters

Parameter	Description
`<keyname1>`	Specifies the full path of the subkey or entry to be deleted. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
/v `<valuename>`	Deletes a specific entry under the subkey. If no entry is specified, then all entries and subkeys under the subkey will be deleted.
/ve	Specifies that only entries that have no value will be deleted.
/va	Deletes all entries within the specified key. Subkey entries that reside within the specified key are not deleted.
/f	Deletes the existing registry subkey or entry without asking for confirmation.
/?	Displays help at the command prompt.

Remarks

- The return values for the **reg delete** operation are:

Value	Description
0	Success

Value	Description
1	Failure

Examples

To delete the registry key Timeout and its all subkeys and values, type:

```
reg delete HKLM\Software\MyCo\MyApp\Timeout
```

To delete the registry value MTU under HKLM\Software\MyCo on the computer named ZODIAC, type:

```
reg delete \\ZODIAC\HKLM\Software\MyCo /v MTU
```

Related links

- Command-Line Syntax Key

reg export

Article • 02/03/2023

Copies the specified subkeys, entries, and values of the local computer into a file for transfer to other servers.

Syntax

```
reg export <keyname> <filename> [/y]
```

Parameters

Parameter	Description
`<keyname>`	Specifies the full path of the subkey. The export operation only works with the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If the registry key name contains a space, enclose the key name in quotes.
`<filename>`	Specifies the name and path of the file to be created during the operation. The file must have a .reg extension.
/y	Overwrites any existing file with the name *filename* without prompting for confirmation.
/?	Displays help at the command prompt.

Remarks

- The return values for the **reg export** operation are:

Value	Description
0	Success
1	Failure

Examples

To export the contents of all subkeys and values of the key MyApp to the file AppBkUp.reg, type:

```
reg export HKLM\Software\MyCo\MyApp AppBkUp.reg
```

Related links

- Command-Line Syntax Key

reg import

Article • 02/03/2023

Copies the contents of a file that contains exported registry subkeys, entries, and values into the registry of the local computer.

Syntax

```
reg import <filename>
```

Parameters

Parameter	Description
`<filename>`	Specifies the name and path of the file that has content to be copied into the registry of the local computer. This file must be created in advance by using **reg export**.
`/reg:32`	Specifies the key should be accessed using the 32-bit registry view.
`/reg:64`	Specifies the key should be accessed using the 64-bit registry view.
/?	Displays help at the command prompt.

Remarks

- The return values for the **reg import** operation are:

Value	Description
0	Success
1	Failure

Examples

To import registry entries from the file named AppBkUp.reg, type:

```
reg import AppBkUp.reg
```

Related links

- Command-Line Syntax Key
- reg export command

reg load

Article • 02/03/2023

Writes saved subkeys and entries into a different subkey in the registry. This command is intended for use with temporary files that are used for troubleshooting or editing registry entries.

Syntax

```
reg load <keyname> <filename>
```

Parameters

Parameter	Description
`<keyname>`	Specifies the full path of the subkey to be loaded. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
`<filename>`	Specifies the name and path of the file to be loaded. This file must be created in advance by using the **reg save** command, and must have a .hiv extension.
/?	Displays help at the command prompt.

Remarks

- The return values for the **reg load** operation are:

Value	Description
0	Success
1	Failure

Examples

To load the file named TempHive.hiv to the key HKLM\TempHive, type:

```
reg load HKLM\TempHive TempHive.hiv
```

Related links

- Command-Line Syntax Key
- reg save command

reg query

Article • 02/03/2023

Returns a list of the next tier of subkeys and entries that are located under a specified subkey in the registry.

Syntax

```
reg query <keyname> [{/v <valuename> | /ve}] [/s] [/se <separator>] [/f
<data>] [{/k | /d}] [/c] [/e] [/t <Type>] [/z] [/reg:32] [/reg:64]
```

Parameters

Parameter	Description
`<keyname>`	Specifies the full path of the subkey. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
/v `<valuename>`	Specifies the registry value name that is to be queried. If omitted, all value names for *keyname* are returned. *Valuename* for this parameter is optional if the **/f** option is also used.
/ve	Runs a query for value names that are empty.
/s	Specifies to query all subkeys and value names recursively.
/se `<separator>`	Specifies the single value separator to search for in the value name type **REG_MULTI_SZ**. If *separator* isn't specified, **\0** is used.
/f `<data>`	Specifies the data or pattern to search for. Use double quotes if a string contains spaces. If not specified, a wildcard (*) is used as the search pattern.
/k	Specifies to search in key names only. Must be used with /f.
/d	Specifies to search in data only.
/c	Specifies that the query is case sensitive. By default, queries are not case sensitive.

Parameter	Description
/e	Specifies to return only exact matches. By default, all the matches are returned.
/t `<Type>`	Specifies registry types to search. Valid types are: **REG_SZ**, **REG_MULTI_SZ**, **REG_EXPAND_SZ**, **REG_DWORD**, **REG_BINARY**, **REG_NONE**. If not specified, all types are searched.
/z	Specifies to include the numeric equivalent for the registry type in search results.
/reg:32	Specifies the key should be accessed using the 32-bit registry view.
/reg:64	Specifies the key should be accessed using the 64-bit registry view.
/?	Displays help at the command prompt.

Remarks

- The return values for the **reg query** operation are:

Value	Description
0	Success
1	Failure

Examples

To display the value of the name value Version in the HKLM\Software\Microsoft\ResKit key, type:

```
reg query HKLM\Software\Microsoft\ResKit /v Version
```

To display all subkeys and values under the key HKLM\Software\Microsoft\ResKit\Nt\Setup on a remote computer named ABC, type:

```
reg query \\ABC\HKLM\Software\Microsoft\ResKit\Nt\Setup /s
```

To display all the subkeys and values of the type REG_MULTI_SZ using # as the separator, type:

```
reg query HKLM\Software\Microsoft\ResKit\Nt\Setup /se #
```

To display the key, value, and data for exact and case sensitive matches of SYSTEM under the HKLM root of data type REG_SZ, type:

```
reg query HKLM /f SYSTEM /t REG_SZ /c /e
```

To display the key, value, and data that match **0F** in the data under the HKCU root key of data type REG_BINARY, type:

```
reg query HKCU /f 0F /d /t REG_BINARY
```

To display the keys, values, and data that match **asp.net** under the key HKLM\SOFTWARE\Microsoft and all subkeys, type:

```
reg query HKLM\SOFTWARE\Microsoft /s /f asp.net
```

To display only the keys that match **asp.net** under the key HKLM\SOFTWARE\Microsoft and all subkeys, type:

```
reg query HKLM\SOFTWARE\Microsoft /s /f asp.net /k
```

To display the value and data for value names of null (default) under HKLM\SOFTWARE, type:

```
reg query HKLM\SOFTWARE /ve
```

Related links

- Command-Line Syntax Key

reg restore

Article • 02/03/2023

Writes saved subkeys and entries back to the registry.

Syntax

```
reg restore <keyname> <filename>
```

Parameters

Parameter	Description
`<keyname>`	Specifies the full path of the subkey to be restored. The restore operation only works with the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If the registry key name contains a space, enclose the key name in quotes.
`<filename>`	Specifies the name and path of the file with content to be written into the registry. This file must be created in advance by using the **reg save** command, and must have a .hiv extension.
/?	Displays help at the command prompt.

Remarks

- Before editing any registry entries, you must save the parent subkey using the **reg save** command. If the edit fails, you can then restore the original subkey using the **reg restore** operation.
- The return values for the **reg restore** operation are:

Value	Description
0	Success
1	Failure

Examples

To restore the file named NTRKBkUp.hiv into the key HKLM\Software\Microsoft\ResKit, and overwrite the existing contents of the key, type:

```
reg restore HKLM\Software\Microsoft\ResKit NTRKBkUp.hiv
```

Related links

- Command-Line Syntax Key
- reg save command

reg save

Article • 02/03/2023

Saves a copy of specified subkeys, entries, and values of the registry in a specified file.

Syntax

```
reg save <keyname> <filename> [/y]
```

Parameters

Parameter	Description
`<keyname>`	Specifies the full path of the subkey. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
`<filename>`	Specifies the name and path of the created file. If no path is specified, the current path is used.
/y	Overwrites an existing file with the name *filename* without prompting for confirmation.
/?	Displays help at the command prompt.

Remarks

- Before editing any registry entries, you must save the parent subkey using the **reg save** command. If the edit fails, you can then restore the original subkey using the **reg restore** operation.
- The return values for the **reg save** operation are:

Value	Description
0	Success

Value	Description
1	Failure

Examples

To save the hive MyApp into the current folder as a file named AppBkUp.hiv, type:

```
reg save HKLM\Software\MyCo\MyApp AppBkUp.hiv
```

Related links

- Command-Line Syntax Key
- reg restore command

reg unload

Article • 02/03/2023

Removes a section of the registry that was loaded using the **reg load** operation.

Syntax

```
reg unload <keyname>
```

Parameters

Parameter	Description
`<keyname>`	Specifies the full path of the subkey. To specify a remote computer, include the computer name (in the format `\\<computername>\`) as part of the *keyname*. Omitting `\\<computername>\` causes the operation to default to the local computer. The *keyname* must include a valid root key. Valid root keys for the local computer are: **HKLM**, **HKCU**, **HKCR**, **HKU**, and **HKCC**. If a remote computer is specified, valid root keys are: **HKLM** and **HKU**. If the registry key name contains a space, enclose the key name in quotes.
/?	Displays help at the command prompt.

Remarks

- The return values for the **reg unload** operation are:

Value	Description
0	Success
1	Failure

Examples

To unload the hive TempHive in the file HKLM, type:

```
```

```
reg unload HKLM\TempHive
```

> **⊗ Caution**
>
> Don't edit the registry directly unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can degrade performance, damage your system, or even require you to reinstall Windows. You can safely alter most registry settings by using the programs in Control Panel or Microsoft Management Console (MMC). If you must edit the registry directly, back it up first.

Related links

- Command-Line Syntax Key
- reg load command

regini

Article • 02/03/2023

Modifies the registry from the command line or a script, and applies changes that were preset in one or more text files. You can create, modify, or delete registry keys, in addition to modifying the permissions on the registry keys.

For details on the format and content of the text script file that regini.exe uses to make changes to the registry, see How to change registry values or permissions from a command line or a script.

Syntax

```
regini [-m \\machinename | -h hivefile hiveroot][-i n] [-o outputwidth][-b]
textfiles...
```

Parameters

Parameter	Description
-m `<\\computername>`	Specifies the remote computer name with a registry that is to be modified. Use the format **\ComputerName**.
-h `<hivefile hiveroot>`	Specifies the local registry hive to modify. You must specify the name of the hive file and the root of the hive in the format **hivefile hiveroot**.
-i `<n>`	Specifies the level of indentation to use to indicate the tree structure of registry keys in the command output. The **regdmp.exe** tool (which gets a registry key's current permissions in binary format) uses indentation in multiples of four, so the default value is **4**.
-o `<outputwidth>`	Specifies the width of the command output, in characters. If the output will appear in the command window, the default value is the width of the window. If the output is directed to a file, the default value is **240** characters.
-b	Specifies that **regini.exe** output is backward compatible with previous versions of **regini.exe**.
textfiles	Specifies the name of one or more text files that contain registry data. Any number of ANSI or Unicode text files can be listed.

Remarks

The following guidelines apply primarily to the content of the text files that contain registry data that you apply by using **regini.exe**.

- Use the semicolon as an end-of-line comment character. It must be the first non-blank character in a line.
- Use the backslash to indicate continuation of a line. The command will ignore all characters from the backslash up to (but not including) the first non-blank character of the next line. If you include more than one space before the backslash, it is replaced by a single space.
- Use hard-tab characters to control indentation. This indentation indicates the tree structure of the registry keys; however, these characters are converted to a single space regardless of their position.

Related links

- Command-Line Syntax Key

regsvr32

Article • 02/03/2023

Registers .dll files as command components in the registry.

Syntax

```
regsvr32 [/u] [/s] [/n] [/i[:cmdline]] <Dllname>
```

Parameters

Parameter	Description
/u	Unregisters server.
/s	Prevents displaying messages.
/n	Prevents calling **DllRegisterServer**. This parameter requires you to also use the **/i** parameter.
/i:`<cmdline>`	Passes an optional command-line string (*cmdline*) to **DllInstall**. If you use this parameter with the **/u** parameter, it calls **DllUninstall**.
`<Dllname>`	The name of the .dll file that will be registered.
/?	Displays help at the command prompt.

Examples

To register the .dll for the Active Directory Schema, type:

```
regsvr32 schmmgmt.dll
```

Related links

- Command-Line Syntax Key

relog

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Extracts performance counters from performance counter logs into other formats, such as text-TSV (for tab-delimited text), text-CSV (for comma-delimited text), binary-BIN, or SQL.

> **Note**
>
> For more information about incorporating **relog** into your Windows Management Instrumentation (WMI) scripts, see the **Scripting blog**.

Syntax

```
relog [<filename> [<filename> ...]] [/a] [/c <path> [<path> ...]] [/cf
<filename>] [/f  {bin|csv|tsv|SQL}] [/t <value>] [/o
{outputfile|DSN!CounterLog}] [/b <M/D/YYYY> [[<HH>:] <MM>:] <SS>] [/e
<M/D/YYYY> [[<HH>:] <MM>:] <SS>] [/config {<filename>|i}] [/q]
```

Parameters

Parameter	Description
`filename [filename ...]`	Specifies the pathname of an existing performance counter log. You can specify multiple input files.
-a	Appends output file instead of overwriting. This option does not apply to SQL format where the default is always to append.
-c `path [path ...]`	Specifies the performance counter path to log. To specify multiple counter paths, separate them with a space and enclose the counter paths in quotation marks (for example, `"path1 path2"`).

Parameter	Description
-cf filename	Specifies the pathname of the text file that lists the performance counters to be included in a relog file. Use this option to list counter paths in an input file, one per line. Default setting is all counters in the original log file are relogged.
-f `{bin | csv | tsv | SQL}`	Specifies the pathname of the output file format. The default format is **bin**. For a SQL database, the output file specifies the `DSN!CounterLog`. You can specify the database location by using the ODBC manager to configure the DSN (Database System Name).
-t value	Specifies sample intervals in *n* records. Includes every nth data point in the relog file. Default is every data point.
-o `{Outputfile | SQL:DSN!Counter_Log}`	Specifies the pathname of the output file or SQL database where the counters will be written. **Note:** For the 64-bit and 32-bit versions of relog.exe, you must define a DSN in the ODBC Data Source (64-bit and 32-bit respectively) on the system. Use the "SQL Server" ODBC driver to define a DSN.
-b `<M/D/YYYY> [[<HH>:]<MM>:]<SS>]`	Specifies the beginning time to copy the first record from the input file. Date and time must be in this exact format M/D/YYYYHH:MM:SS.
-e `<M/D/YYYY> [[<HH>:]<MM>:]<SS>]`	Specifies the end time to copy the last record from the input file. Date and time must be in this exact format M/D/YYYYHH:MM:SS.
-config `{filename | i}`	Specifies the pathname of the settings file that contains command-line parameters. If you're using a configuration file, you can use **-i** as a placeholder for a list of input files that can be placed on the command line. If you're using the command line, don't use **-i**. You can also use wildcards, such as `*.blg` to specify several input file names at once.
-q	Displays the performance counters and time ranges of log files specified in the input file.
-y	Bypasses prompting by answering "yes" to all questions.
/?	Displays help at the command prompt.

Remarks

- The general format for counter paths is as follows: `[\<computer>] \<object> [<parent>\<instance#index>] \<counter>]` where the parent, instance, index, and counter components of the format may contain either a valid name or a wildcard character. The computer, parent, instance, and index components aren't necessary for all counters.

- You determine the counter paths to use based on the counter itself. For example, the **LogicalDisk** object has an instance `<index>`, so you must provide the `<#index>` or a wildcard. Therefore, you could use the following format: `\LogicalDisk(*/*#*)\\*`.
- In comparison, the **Process** object doesn't require an instance `<index>`. Therefore, you can use the following format: `\Process(*)\ID Process`.
- If a wildcard character is specified in the **Parent** name, all instances of the specified object that match the specified instance and counter fields will be returned.
- If a wildcard character is specified in the **Instance** name, all instances of the specified object and parent object will be returned if all instance names corresponding to the specified index match the wildcard character.
- If a wildcard character is specified in the **Counter** name, all counters of the specified object are returned.
- Partial counter path string matches (for example, pro*) aren't supported.
- Counter files are text files that list one or more of the performance counters in the existing log. Copy the full counter name from the log or the **/q** output in `<computer>\<object>\<instance>\<counter>` format. List one counter path on each line.
- When run, the **relog** command copies specified counters from every record in the input file, converting the format if necessary. Wildcard paths are allowed in the counter file.
- Use the **/t** parameter to specify that input files are inserted into output files at intervals of every `nth` record. By default, data is relogged from every record.
- You can specify that your output logs include records from before the beginning time (that is, **/b**) to provide data for counters that require computation values of the formatted value. The output file will have the last records from input files with timestamps less than the **/e** (that is, end time) parameter.
- The contents of the setting file used with the **/config** option should have the following format: `<commandoption>\<value>`, where `<commandoption>` is a command line option and `<value>` specifies its value.

##Q# Examples

To resample existing trace logs at fixed intervals of 30, list counter paths, output files, and formats, type:

```
relog c:\perflogs\daily_trace_log.blg /cf counter_file.txt /o
c:\perflogs\reduced_log.csv /t 30 /f csv
```

To resample existing trace logs at fixed intervals of 30, list counter paths, and output file, type:

```
relog c:\perflogs\daily_trace_log.blg /cf counter_file.txt /o
c:\perflogs\reduced_log.blg /t 30
```

To resample existing trace logs into a database, type:

```
relog "c:\perflogs\daily_trace_log.blg" -f sql -o
"SQL:sql2016x64odbc!counter_log"
```

Related links

- Command-Line Syntax Key

ren

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Renames files or directories.

> **Note**
>
> This command is the same as the **rename command**.

Syntax

```
ren [<drive>:][<path>]<filename1> <filename2>
```

Parameters

Parameter	Description
`[<drive>:][<path>]<filename1>`	Specifies the location and name of the file or set of files you want to rename. *Filename1* can include wildcard characters (* and ?).
`<filename2>`	Specifies the new name for the file. You can use wildcard characters to specify new names for multiple files.
/?	Displays help at the command prompt.

Remarks

- You can't specify a new drive or path when renaming files. You also can't use this command to rename files across drives or to move files to a different directory.
- Characters represented by wildcard characters in *filename2* will be identical to the corresponding characters in *filename1*.

- *Filename2* must be a unique file name. If *filename2* matches an existing file name, the following message appears: `Duplicate file name or file not found`.

Examples

To change all the .txt file name extensions in the current directory to .doc extensions, type:

```
ren *.txt *.doc
```

To change the name of a directory from *Chap10* to *Part10*, type:

```
ren chap10 part10
```

Related links

- Command-Line Syntax Key
- rename command

rename

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Renames files or directories.

> **Note**
>
> This command is the same as the **ren command**.

Syntax

```
rename [<drive>:][<path>]<filename1> <filename2>
```

Parameters

Parameter	Description
`[<drive>:][<path>]<filename1>`	Specifies the location and name of the file or set of files you want to rename. *Filename1* can include wildcard characters (* and ?).
`<filename2>`	Specifies the new name for the file. You can use wildcard characters to specify new names for multiple files.
/?	Displays help at the command prompt.

Remarks

- You can't specify a new drive or path when renaming files. You also can't use this command to rename files across drives or to move files to a different directory.
- Characters represented by wildcard characters in *filename2* will be identical to the corresponding characters in *filename1*.

- *Filename2* must be a unique file name. If *filename2* matches an existing file name, the following message appears: `Duplicate file name or file not found`.

Examples

To change all the .txt file name extensions in the current directory to .doc extensions, type:

```
rename *.txt *.doc
```

To change the name of a directory from *Chap10* to *Part10*, type:

```
rename chap10 part10
```

Related links

- Command-Line Syntax Key
- ren command

repair-bde

Article • 02/03/2023

Attempts to reconstruct critical parts of a severely damaged drive and salvage recoverable data if the drive was encrypted by using BitLocker and if it has a valid recovery password or recovery key for decryption.

> **ⓘ Important**
>
> If the BitLocker metadata data on the drive is corrupt, you must be able to supply a backup key package in addition to the recovery password or recovery key. If you used the default key back up setting for Active Directory Domain Services, your key package is backed up there. You can use the **BitLocker: Use BitLocker Recovery Password Viewer** to obtain the key package from AD DS.
>
> Using the key package and either the recovery password or recovery key, you can decrypt portions of a BitLocker-protected drive, even if the disk is corrupted. Each key package works only for a drive with the corresponding drive identifier.

Syntax

```
repair-bde <inputvolume> <outputvolumeorimage> [-rk] [-rp] [-pw] [-kp] [-lf]
[-f] [{-?|/?}]
```

> **⚠ Warning**
>
> The contents of the output volume will be **completely deleted and overwritten** by the decrypted contents from the damaged BitLocker drive. If you want to save any existing data on the selected target drive, move the existing data to other reliable backup media first, before running the `repair-bde` command.

Parameters

Parameter	Description

Parameter	Description
`<inputvolume>`	Identifies the drive letter of the BitLocker-encrypted drive that you want to repair. The drive letter must include a colon; for example: **C:**. If the path to a key package isn't specified, this command searches the drive for a key package. In the event that the hard drive is damaged, this command might not be able to find the package and will prompt you to provide the path.
`<outputvolumeorimage>`	Identifies the drive on which to store the content of the repaired drive. All information on the output drive will be overwritten.
-rk	Identifies the location of the recovery key that should be used to unlock the volume. This command can also be specified as **-recoverykey**.
-rp	Identifies the numerical recovery password that should be used to unlock the volume. This command can also be specified as **-recoverypassword**.
-pw	Identifies the password that should be used to unlock the volume. This command can also be specified as **-password**
-kp	Identifies the recovery key package that can be used to unlock the volume. This command can also be specified as **-keypackage**.
-lf	Specifies the path to the file that will store Repair-bde error, warning, and information messages. This command may also be specified as **-logfile**.
-f	Forces a volume to be dismounted even if it cannot be locked. This command can also be specified as **-force**.
-? or /?	Displays Help at the command prompt.

Limitations

The following limitations exist for the this command:

- This command can't repair a drive that failed during the encryption or decryption process.
- This command assumes that if the drive has any encryption, then the drive has been fully encrypted.

Examples

To attempt to repair drive C:, to write the content from drive C: to drive D: using the recovery key file (RecoveryKey.bek) stored on drive F:, and to write the results of this attempt to the log file (log.txt) on drive Z:, type:

```
repair-bde C: D: -rk F:\RecoveryKey.bek –lf Z:\log.txt
```

To attempt to repair drive C: and to write the content from drive C: to drive D: using the 48-digit recovery password specified, type:

```
repair-bde C: D: -rp 111111-222222-333333-444444-555555-666666-777777-888888
```

> **Note**
>
> The recovery password should be typed in eight blocks of six digits with a hyphen separating each block.

To force drive C: to dismount, attempt to repair drive C:, and then to write the content from drive C: to drive D: using the recovery key package and recovery key file (RecoveryKey.bek) stored on drive F:, type:

```
repair-bde C: D: -kp F:\RecoveryKeyPackage -rk F:\RecoveryKey.bek -f
```

To attempt to repair drive C: and to write the content from drive C: to drive D:, where you must type a password to unlock drive C: (when prompted), type:

```
repair-bde C: D: -pw
```

Related links

- Command-Line Syntax Key

replace

Article • 02/03/2023

Replace existing files in a directory. If used with the **/a** option, this command adds new files to a directory instead of replacing existing files.

Syntax

```
replace [<drive1>:][<path1>]<filename> [<drive2>:][<path2>] [/a] [/p] [/r]
[/w]
replace [<drive1>:][<path1>]<filename> [<drive2>:][<path2>] [/p] [/r] [/s]
[/w] [/u]
```

Parameters

Parameter	Description
`[<drive1>:][<path1>]<filename>`	Specifies the location and name of the source file or set of files. The *filename* option is required, and can include wildcard characters (* and **?**).
`[<drive2>:][<path2>]`	Specifies the location of the destination file. You can't specify a file name for files you replace. If you don't specify a drive or path, this command uses the current drive and directory as the destination.
/a	Adds new files to the destination directory instead of replacing existing files. You can't use this command-line option with the **/s** or **/u** command-line option.
/p	Prompts you for confirmation before replacing a destination file or adding a source file.
/r	Replaces Read-only and unprotected files. If you attempt to replace a Read-only file, but you don't specify **/r**, an error results and stops the replacement operation.
/w	Waits for you to insert a disk before the search for source files begins. If you don't specify **/w**, this command begins replacing or adding files immediately after you press ENTER.
/s	Searches all subdirectories in the destination directory and replaces matching files. You can't use **/s** with the **/a** command-line option. The command doesn't search subdirectories that are specified in *Path1*.

Parameter	Description
/u	Replaces only those files on the destination directory that are older than those in the source directory. You can't use **/u** with the **/a** command-line option.
/?	Displays help at the command prompt.

Remarks

- As this command adds or replaces files, the file names appear on the screen. After this command is done, a summary line is displayed in one of the following formats:

```
nnn files added
nnn files replaced
no file added
no file replaced
```

- If you're using floppy disks and you need to switch disks while running this command, you can specify the **/w** command-line option so that this command waits for you to switch the disks.
- You can't use this command to update hidden files or system files.
- The following table shows each exit code and a brief description of its meaning:

Exit code	Description
0	This command successfully replaced or added the files.
1	This command encountered an incorrect version of MS-DOS.
2	This command couldn't find the source files.
3	This command couldn't find the source or destination path.
5	The user doesn't have access to the files that you want to replace.
8	There is insufficient system memory to carry out the command.
11	The user used the wrong syntax on the command line.

> **Note**
>
> You can use the ERRORLEVEL parameter on the **if** command line in a batch program to process exit codes that are returned by this command.

Examples

To update all the versions of a file named *Phones.cli* (which appear in multiple directories on drive C:), with the latest version of the *Phones.cli* file from a floppy disk in drive A:, type:

```
replace a:\phones.cli c:\ /s
```

Related links

- Command-Line Syntax Key

rexec

Article • 03/03/2021

Runs a specified command on a remote host. The remote host must be running a rexecd service (or daemon) for rexec to connect to.

> **Important**
>
> The **rexec** command has been deprecated, and isn't guaranteed to be supported in Windows.

risetup

Article • 03/03/2021

Creates an operating system image by pulling the files from the original Windows Server 2003 CD or from a customized distribution folder containing these files.

> **Important**
>
> The **rexec** command has been deprecated, and isn't guaranteed to be supported in Windows.

rmdir

Article • 02/03/2023

Deletes a directory.

The **rmdir** command can also run from the Windows Recovery Console, using different parameters. For more information, see Windows Recovery Environment (WinRE).

> **Note**
>
> This command is the same as the **rd command**.

Syntax

```
rmdir [<drive>:]<path> [/s [/q]]
```

Parameters

Parameter	Description
`[<drive>:]<path>`	Specifies the location and the name of the directory that you want to delete. *Path* is required. If you include a backslash () at the beginning of the specified *path*, then the *path* starts at the root directory (regardless of the current directory).
/s	Deletes a directory tree (the specified directory and all its subdirectories, including all files).
/q	Specifies quiet mode. Does not prompt for confirmation when deleting a directory tree. The **/q** parameter works only if **/s** is also specified. **CAUTION:** When you run in quiet mode, the entire directory tree is deleted without confirmation. Make sure that important files are moved or backed up before using the **/q** command-line option.
/?	Displays help at the command prompt.

Remarks

- You can't delete a directory that contains files, including hidden or system files. If you attempt to do so, the following message appears:

`The directory is not empty`

Use the **dir /a** command to list all files (including hidden and system files). Then use the **attrib** command with **-h** to remove hidden file attributes, **-s** to remove system file attributes, or **-h -s** to remove both hidden and system file attributes. After the hidden and file attributes have been removed, you can delete the files.

- You can't use the **rmdir** command to delete the current directory. If you attempt to delete the current directory, the following error message appears:

  `The process can't access the file because it is being used by another process.`

  If you receive this error message, you must change to a different directory (not a subdirectory of the current directory), and then try again.

Examples

To change to the parent directory so you can safely remove the desired directory, type:

```
cd ..
```

To remove a directory named *test* (and all its subdirectories and files) from the current directory, type:

```
rmdir /s test
```

To run the previous example in quiet mode, type:

```
rmdir /s /q test
```

Related links

- Command-Line Syntax Key

robocopy

Article • 05/28/2024

Copies file data from one location to another.

Syntax

Windows Command Prompt

```
robocopy <source> <destination> [<file>[ ...]] [<options>]
```

For example, to copy a file named *yearly-report.mov* from *c:\reports* to a file share *\\marketing\videos* while enabling multi-threading for higher performance (with the **/mt** parameter) and the ability to restart the transfer in case it's interrupted (with the **/z** parameter), type:

Windows Command Prompt

```
robocopy c:\reports "\\marketing\videos" yearly-report.mov /mt /z
```

> **Important**
>
> If any data is copied from the *root* of a device, the destination directory will adopt the "hidden" attribute during the copy process.

Parameters

Expand table

Parameter	Description
`<source>`	Specifies the path to the source directory.
`<destination>`	Specifies the path to the destination directory.
`<file>`	Specifies the file or files to be copied. Wildcard characters (* or ?) are supported. If you don't specify this parameter, `*.*` is used as the default value.
`<options>`	Specifies the options to use with the **robocopy** command, including **copy**, **file**, **retry**, **logging**, and **job** options.

Copy options

Expand table

Option	Description
/s	Copies subdirectories. This option automatically excludes empty directories.
/e	Copies subdirectories. This option automatically includes empty directories.
/lev:`<n>`	Copies only the top *n* levels of the source directory tree.
/z	Copies files in restartable mode. In restartable mode, should a file copy be interrupted, robocopy can pick up where it left off rather than recopying the entire file.
/b	Copies files in backup mode. In backup mode, robocopy overrides file and folder permission settings (ACLs), which might otherwise block access.
/zb	Copies files in restartable mode. If file access is denied, switches to backup mode.
/j	Copies using unbuffered I/O (recommended for large files).
/efsraw	Copies all encrypted files in EFS RAW mode.
/copy:`<copyflags>`	Specifies which file properties to copy. The valid values for this option are: • **D** - Data • **A** - Attributes • **T** - Time stamps • **X** - Skip alt data streams • **S** - NTFS access control list (ACL) • **O** - Owner information • **U** - Auditing information The default value for the **/COPY** option is **DAT** (data, attributes, and time stamps). The **X** flag is ignored if either **/B** or **/ZB** is used.
/dcopy:`<copyflags>`	Specifies what to copy in directories. The valid values for this option are: • **D** - Data • **A** - Attributes • **T** - Time stamps • **E** - Extended attribute • **X** - Skip alt data streams The default value for this option is **DA** (data and attributes).
/sec	Copies files with security (equivalent to **/copy:DATS**).
/copyall	Copies all file information (equivalent to **/copy:DATSOU**).

Option	Description
/nocopy	Copies no file information (useful with **/purge**).
/secfix	Fixes file security on all files, even skipped ones.
/timfix	Fixes file times on all files, even skipped ones.
/purge	Deletes destination files and directories that no longer exist in the source. Using this option with the **/e** option and a destination directory, allows the destination directory security settings to not be overwritten.
/mir	Mirrors a directory tree (equivalent to **/e** plus **/purge**). Using this option with the **/e** option and a destination directory, overwrites the destination directory security settings.
/mov	Moves files, and deletes them from the source after they're copied.
/move	Moves files and directories, and deletes them from the source after they're copied.
/a+: [RASHCNET]	Adds the specified attributes to copied files. The valid values for this option are: • **R** - Read only • **A** - Archive • **S** - System • **H** - Hidden • **C** - Compressed • **N** - Not content indexed • **E** - Encrypted • **T** - Temporary
/a-: [RASHCNETO]	Removes the specified attributes from copied files. The valid values for this option are: • **R** - Read only • **A** - Archive • **S** - System • **H** - Hidden • **C** - Compressed • **N** - Not content indexed • **E** - Encrypted • **T** - Temporary • **O** - Offline
/create	Creates a directory tree and zero-length files only.
/fat	Creates destination files by using 8.3 character-length FAT file names only.
/256	Turns off support for paths longer than 256 characters.
/mon:`<n>`	Monitors the source and runs again when more than *n* changes are detected.

Option	Description
/mot:`<m>`	Monitors the source and runs again in *m* minutes if changes are detected.
/rh:hhmm-hhmm	Specifies run times when new copies can be started.
/pf	Checks run times on a per file (not per-pass) basis.
/ipg:`<n>`	Specifies the inter-packet gap to free bandwidth on slow lines.
/sj	Copies junctions (soft-links) to the destination path instead of link targets.
/sl	Don't follow symbolic links and instead create a copy of the link.
/mt:`<n>`	Creates multi-threaded copies with *n* threads. *n* must be an integer between 1 and 128. The default value for *n* is 8. For better performance, redirect your output using **/log** option. The **/mt** parameter can't be used with the **/ipg** and **/efsraw** parameters.
/nodcopy	Copies no directory info (the default **/dcopy:DA** is done).
/nooffload	Copies files without using the Windows Copy Offload mechanism.
/compress	Requests network compression during file transfer, if applicable.
/sparse:`<y|n>`	Enables or disables retaining the sparse state of files during copy process. If no option is selected, it defaults to **yes** (enabled).
/noclone	Doesn't attempt block cloning as an optimization.

ⓘ Important

When using the **/secfix** copy option, specify the type of security information you want to copy, using one of these additional copy options:

- **/copyall**
- **/copy:o**
- **/copy:s**
- **/copy:u**
- **/sec**

ⓘ Note

The **/mt** parameter was introduced in Windows Server 2008 R2 and its functionality applies to current versions of Windows Server.

Copy file throttling options

Expand table

Option	Description
/iomaxsize:`<n>` [kmg]	The requested max i/o size per read/write cycle in *n* **k**ilobytes, **m**egabytes, or **g**igabytes.
/iorate:`<n>`[kmg]	The requested i/o rate in *n* **k**ilobytes **m**egabytes, or **g**igabytes per second.
/threshold:`<n>` [kmg]	The file size threshold for throttling in *n* **k**ilobytes, **m**egabytes, or **g**igabytes (see Remarks).

These throttling options are used to specify the maximum I/O bandwidth that Robocopy allows to be used in bytes per second. If not specifying in bytes per second, whole numbers can be used if **k**, **m**, or **g** are specified. The minimum I/O bandwidth that is throttled is **524288** bytes even if a lesser value is specified.

File selection options

Expand table

Option	Description
/a	Copies only files for which the **Archive** attribute is set.
/m	Copies only files for which the **Archive** attribute is set, and resets the **Archive** attribute.
/ia:`[RASHCNETO]`	Includes only files for which any of the specified attributes are set. The valid values for this option are: • **R** - Read only • **A** - Archive • **S** - System • **H** - Hidden • **C** - Compressed • **N** - Not content indexed • **E** - Encrypted • **T** - Temporary • **O** - Offline

Option	Description
/xa:`[RASHCNETO]`	Excludes files for which any of the specified attributes are set. The valid values for this option are: • **R** - Read only • **A** - Archive • **S** - System • **H** - Hidden • **C** - Compressed • **N** - Not content indexed • **E** - Encrypted • **T** - Temporary • **O** - Offline
/xf `<filename>[ ...]`	Excludes files that match the specified names or paths. Wildcard characters (***** and **?**) are supported.
/xd `<directory>[ ...]`	Excludes directories that match the specified names and paths.
/xc	Excludes existing files with the same timestamp, but different file sizes.
/xn	Source directory files newer than the destination are excluded from the copy.
/xo	Source directory files older than the destination are excluded from the copy.
/xx	Excludes extra files and directories present in the destination but not the source. Excluding extra files won't delete files from the destination.
/xl	Excludes "lonely" files and directories present in the source but not the destination. Excluding lonely files prevents any new files from being added to the destination.
/im	Include modified files (differing change times).
/is	Includes the same files. Same files are identical in name, size, times, and all attributes.
/it	Includes "tweaked" files. Tweaked files have the same name, size, and times, but different attributes.
/max:`<n>`	Specifies the maximum file size (to exclude files bigger than *n* bytes).
/min:`<n>`	Specifies the minimum file size (to exclude files smaller than *n* bytes).
/maxage:`<n>`	Specifies the maximum file age (to exclude files older than *n* days or date).
/minage:`<n>`	Specifies the minimum file age (exclude files newer than *n* days or date).
/maxlad:`<n>`	Specifies the maximum last access date (excludes files unused since *n*).

Option	Description
/minlad:<n>	Specifies the minimum last access date (excludes files used since *n*) If *n* is less than 1900, *n* specifies the number of days. Otherwise, *n* specifies a date in the format YYYYMMDD.
/xj	Excludes junction points, which are normally included by default.
/fft	Assumes FAT file times (two-second precision).
/dst	Compensates for one-hour DST time differences.
/xjd	Excludes junction points for directories.
/xjf	Excludes junction points for files.

Retry options

Expand table

Option	Description
/r:<n>	Specifies the number of retries on failed copies. The default value of *n* is 1,000,000 (one million retries).
/w:<n>	Specifies the wait time between retries, in seconds. The default value of *n* is 30 (wait time 30 seconds).
/reg	Saves the values specified in the **/r** and **/w** options as default settings in the registry.
/tbd	Specifies that the system waits for share names to be defined (retry error 67).
/lfsm	Operate in low free space mode that enables copy, pause, and resume (see Remarks).
/lfsm:<n> [kmg]	Specifies the floor size in *n* **k**ilobytes, **m**egabytes, or **g**igabytes.

Logging options

Expand table

Option	Description
/l	Specifies that files are to be listed only (and not copied, deleted, or time stamped).

Option	Description
/x	Reports all extra files, not just the ones that are selected.
/v	Produces verbose output, and shows all skipped files.
/ts	Includes source file time stamps in the output.
/fp	Includes the full path names of the files in the output.
/bytes	Prints sizes as bytes.
/ns	Specifies that file sizes aren't to be logged.
/nc	Specifies that file classes aren't to be logged.
/nfl	Specifies that file names aren't to be logged.
/ndl	Specifies that directory names aren't to be logged.
/np	Specifies that the progress of the copying operation (the number of files or directories copied so far) won't be displayed.
/eta	Shows the estimated time of arrival (ETA) of the copied files.
/log:`<logfile>`	Writes the status output to the log file (overwrites the existing log file).
/log+: `<logfile>`	Writes the status output to the log file (appends the output to the existing log file).
/unilog: `<logfile>`	Writes the status output to the log file as unicode text (overwrites the existing log file).
/unilog+: `<logfile>`	Writes the status output to the log file as Unicode text (appends the output to the existing log file).
/tee	Writes the status output to the console window, and to the log file.
/njh	Specifies that there's no job header.
/njs	Specifies that there's no job summary.
/unicode	Displays the status output as unicode text.

Job options

Expand table

Option	Description
/job: `<jobname>`	Specifies that parameters are to be derived from the named job file. To run `/job:jobname`, you must first run the `/save:jobname` parameter to create the job file.
/save: `<jobname>`	Specifies that parameters are to be saved to the named job file. This must be ran before running `/job:jobname`. All copy, retry, and logging options must be specified before this parameter.
/quit	Quits after processing command line (to view parameters).
/nosd	Indicates that no source directory is specified.
/nodd	Indicates that no destination directory is specified.
/if	Includes the specified files.

Remarks

- Using **/PURGE** or **/MIR** on the root directory of the volume formerly caused robocopy to apply the requested operation on files inside the System Volume Information directory as well. This is no longer the case as if either is specified, robocopy will skip any files or directories with that name in the top-level source and destination directories of the copy session.
- Modified files classification applies only when both source and destination filesystems support change timestamps, such as NTFS, and the source and destination files have different change times but are otherwise the same. These files aren't copied by default. Specify **/IM** to include them.
- The **/DCOPY:E** flag requests that extended attribute copying should be attempted for directories. Robocopy will continue if a directory's EAs couldn't be copied. This flag isn't included in **/COPYALL**.
- If either **/IoMaxSize** or **/IoRate** are specified, robocopy will enable copy file throttling to reduce system load. Both can be adjusted to optimal values and copy parameters, but the system and robocopy are allowed to adjust them to allowed values as necessary.
- If **/Threshold** is used, it specifies a minimum file size for engaging throttling. Files below that size won't be throttled. Values for all three parameters can be followed by an optional suffix character such as [KMG] (kilobytes, megabytes, gigabytes).
- Using **/LFSM** requests robocopy to operate in 'low free space mode'. In this mode, robocopy will pause whenever a file copy would cause the destination volume's

free space to go below a 'floor' value. This value can be explicitly specified using **/LFSM:*n***[KMG] flag.

- If **/LFSM** is specified with no explicit floor value, the floor is set to 10% of the destination volume's size. Low free space mode is incompatible with **/MT** and **/EFSRAW**.

Exit (return) codes

Expand table

Value	Description
0	No files were copied. No failure was encountered. No files were mismatched. The files already exist in the destination directory; therefore, the copy operation was skipped.
1	All files were copied successfully.
2	There are some additional files in the destination directory that aren't present in the source directory. No files were copied.
3	Some files were copied. Additional files were present. No failure was encountered.
5	Some files were copied. Some files were mismatched. No failure was encountered.
6	Additional files and mismatched files exist. No files were copied and no failures were encountered meaning that the files already exist in the destination directory.
7	Files were copied, a file mismatch was present, and additional files were present.
8	Several files didn't copy.

> **Note**
>
> Any value equal to or greater than **8** indicates that there was at least one failure during the copy operation.

Examples

It's highly recommended when running the `robocopy` command to create a log file that can be viewed once the process completes verifying its integrity. In the following examples, each one uses the `/LOG:` parameter. To append any log information to the same log file, use the `/LOG+:` parameter instead.

To copy all files and subdirectories, including empty directories, from the "Records" folder to the "Backup" folder on drive "D", type the following:

Windows Command Prompt

```
robocopy C:\Users\Admin\Records D:\Backup /E /ZB /LOG:C:\Logs\Backup.log
```

To mirror the contents of the "Records" folder to the "Backup" folder on drive "D", delete any files in the destination that don't exist in the source with 2 retries and waiting 5 seconds between each retry, type the following:

Windows Command Prompt

```
robocopy C:\Users\Admin\Records D:\Backup /MIR /R:2 /W:5
/LOG:C:\Logs\Backup.log
```

To copy all files and subdirectories that aren't empty from the "Records" folder to the "Backup" folder on drive "D", retaining the file data, attributes, and timestamps with 16 multi-threaded copy operation, type the following:

Windows Command Prompt

```
robocopy C:\Users\Admin\Records D:\Backup /S /E /COPY:DAT /MT:16
/LOG:C:\Logs\Backup.log
```

To move files and subdirectories, excluding empty directories, from the "Records" folder to the "Backup" folder on drive "D", and exclude files older than 7 days, type the following:

Windows Command Prompt

```
robocopy C:\Users\Admin\Records D:\Backup /S /MAXAGE:7 /MOV
/LOG:C:\Logs\Backup.log
```

To copy all files and subdirectories, including empty directories, from the "Records" folder to the "Backup" folder on drive "D" showing the estimated time for each file and delete any files and directories in the destination that don't exist from the source, type the following:

Windows Command Prompt

```
robocopy C:\Users\Admin\Records D:\Backup /ETA /PURGE
/LOG:C:\Logs\Backup.log
```

To copy all files and subdirectories from the folder named "Records" on the "C" drive to a folder named "Backup" on the "D" drive while limiting the I/O rate to 1 megabyte per second during the copy operation, type the following:

Windows Command Prompt

```
robocopy C:\Records D:\Backup /iorate:1m
```

Related links

- Command-Line Syntax Key

route

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays and modifies the entries in the local IP routing table. If used without parameters, **route** displays help at the command prompt.

> **Important**
>
> This command is available only if the Internet Protocol (TCP/IP) protocol is installed as a component in the properties of a network adapter in Network Connections.

Syntax

Windows Command Prompt

```
route [/f] [/p] [<command> [<destination>] [mask <netmask>] [<gateway>] [metric
<metric>]] [if <interface>]]
```

Parameters

Parameter	Description
/f	Clears the routing table of all entries that are not host routes (routes with a netmask of 255.255.255.255), the loopback network route (routes with a destination of 127.0.0.0 and a netmask of 255.0.0.0), or a multicast route (routes with a destination of 224.0.0.0 and a netmask of 240.0.0.0). If this is used in conjunction with one of the commands (such as add, change, or delete), the table is cleared prior to running the command.
/p	When used with the add command, the specified route is added to the registry and is used to initialize the IP routing table whenever the TCP/IP protocol is started. By default, added routes are not preserved when the TCP/IP protocol is started. When used with the print command, the list of persistent routes is displayed. This parameter is ignored for all other commands. Persistent routes are stored in the registry location **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes**.
`<command>`	Specifies the command you want to run. The valid commands include: • **add** - Adds a route. • **change** - Modifies an existing route. • **delete:** - Deletes a route or routes. • **print** - Prints a route or routes.

Parameter	Description
`<destination>`	Specifies the network destination of the route. The destination can be an IP network address (where the host bits of the network address are set to 0), an IP address for a host route, or 0.0.0.0 for the default route.
`<mask>`	Specifies the next parameter for the 'netmask' value.
`<netmask>`	Specifies the network destination subnet mask. Defaults to 255.255.255.255 if not specified.
`<gateway>`	Specifies the forwarding or next hop IP address over which the set of addresses defined by the network destination and subnet mask are reachable. For locally attached subnet routes, the gateway address is the IP address assigned to the interface that is attached to the subnet. For remote routes, available across one or more routers, the gateway address is a directly reachable IP address that is assigned to a neighboring router.
metric `<metric>`	Specifies an integer cost metric (ranging from 1 to 9999) for the route, which is used when choosing among multiple routes in the routing table that most closely match the destination address of a packet being forwarded. The route with the lowest metric is chosen. The metric can reflect the number of hops, the speed of the path, path reliability, path throughput, or administrative properties.
if `<interface>`	Specifies the interface index for the interface over which the destination is reachable. For a list of interfaces and their corresponding interface indexes, use the display of the route print command. You can use either decimal or hexadecimal values for the interface index. For hexadecimal values, precede the hexadecimal number with 0x. When the if parameter is omitted, the interface is determined from the gateway address.
/?	Displays help at the command prompt.

Remarks

- Large values in the **metric** column of the routing table are the result of allowing TCP/IP to automatically determine the metric for routes in the routing table based on the configuration of IP address, subnet mask, and default gateway for each LAN interface. Automatic determination of the interface metric, enabled by default, determines the speed of each interface and adjusts the metrics of routes for each interface so that the fastest interface creates the routes with the lowest metric. To remove the large metrics, disable the automatic determination of the interface metric from the advanced properties of the TCP/IP protocol for each LAN connection.

- Names can be used for *destination* if an appropriate entry exists in the local *Networks* file stored in the `systemroot\System32\Drivers\\` folder. Names can be used for the *gateway* as long as they can be resolved to an IP address through standard host name resolution techniques such as Domain Name System (DNS) queries, use of the local Hosts file stored in the `systemroot\system32\drivers\\` folder, and NetBIOS name resolution.

- if the command is **print** or **delete**, the *gateway* parameter can be omitted and wildcards can be used for the destination and gateway. The *destination* value can be a wildcard value specified by an asterisk `(*)`. If the destination specified contains an asterisk `(*)` or a

question mark (?), it's treated as a wildcard, and only matching destination routes are printed or deleted. The asterisk matches any string, and the question mark matches any single character. For example, `10.\*.1, 192.168.\*`, `127.\*`, and `\*224\*` are all valid uses of the asterisk wildcard.

- Using an unsupported combination of a destination and subnet mask (netmask) value displays a "Route: bad gateway address netmask" error message. This error message appears when the destination contains one or more bits set to 1 in bit locations where the corresponding subnet mask bit is set to 0. To test this condition, express the destination and subnet mask using binary notation. The subnet mask in binary notation consists of a series of 1 bits, representing the network address portion of the destination, and a series of 0 bits, representing the host address portion of the destination. Check to determine whether there are bits in the destination that are set to 1 for the portion of the destination that is the host address (as defined by the subnet mask).

Examples

To display the entire contents of the IP routing table, type:

Windows Command Prompt

```
route print
```

To display the routes in the IP routing table that begin with 10, type:

Windows Command Prompt

```
route print 10.*
```

To add a default route with the default gateway address of 192.168.12.1, type:

Windows Command Prompt

```
route add 0.0.0.0 mask 0.0.0.0 192.168.12.1
```

To add a route to the destination 10.41.0.0 with the subnet mask of 255.255.0.0 and the next hop address of 10.27.0.1, type:

Windows Command Prompt

```
route add 10.41.0.0 mask 255.255.0.0 10.27.0.1
```

To add a persistent route to the destination 10.41.0.0 with the subnet mask of 255.255.0.0 and the next hop address of 10.27.0.1, type:

Windows Command Prompt

```
route /p add 10.41.0.0 mask 255.255.0.0 10.27.0.1
```

To add a route to the destination 10.41.0.0 with the subnet mask of 255.255.0.0, the next hop address of 10.27.0.1, and the cost metric of 7, type:

Windows Command Prompt

```
route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 metric 7
```

To add a route to the destination 10.41.0.0 with the subnet mask of 255.255.0.0, the next hop address of 10.27.0.1, and using the interface index 0x3, type:

Windows Command Prompt

```
route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 if 0x3
```

To delete the route to the destination 10.41.0.0 with the subnet mask of 255.255.0.0, type:

Windows Command Prompt

```
route delete 10.41.0.0 mask 255.255.0.0
```

To delete all routes in the IP routing table that begin with 10, type:

Windows Command Prompt

```
route delete 10.*
```

To change the next hop address of the route with the destination of 10.41.0.0 and the subnet mask of 255.255.0.0 from 10.27.0.1 to 10.27.0.25, type:

Windows Command Prompt

```
route change 10.41.0.0 mask 255.255.0.0 10.27.0.25
```

Related links

- Command-Line Syntax Key

rpcinfo

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Lists programs on remote computers. The **rpcinfo** command-line utility makes a remote procedure call (RPC) to an RPC server and reports what it finds.

Syntax

```
rpcinfo [/p [<node>]] [/b <program version>] [/t <node program> [<version>]]
[/u <node program> [<version>]]
```

Parameters

Parameter	Description
/p `[<node>]`	lists all programs registered with the port mapper on the specified host. If you do not specify a node (computer) name, the program queries the port mapper on the local host.
/b `<program version>`	Requests a response from all network nodes that have the specified program and version registered with the port mapper. You must specify both a program name or number and a version number.
/t `<node program> [\ <version>]`	Uses the TCP transport protocol to call the specified program. You must specify both a node (computer) name and a program name. If you do not specify a version, the program calls all versions.
/u `<node program> [\ <version>]`	Uses the UDP transport protocol to call the specified program. You must specify both a node (computer) name and a program name. If you do not specify a version, the program calls all versions.
/?	Displays help at the command prompt.

Examples

To list all programs registered with the port mapper, type:

```
rpcinfo /p [<node>]
```

To request a response from network nodes that have a specified program, type:

```
rpcinfo /b <program version>
```

To use Transmission Control Protocol (TCP) to call a program, type:

```
rpcinfo /t <node program> [<version>]
```

Use User Datagram Protocol (UDP) to call a program:

```
rpcinfo /u <node program> [<version>]
```

Related links

- Command-Line Syntax Key

rpcping

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Confirms the RPC connectivity between the computer running Microsoft Exchange Server and any of the supported Microsoft Exchange Client workstations on the network. This utility can be used to check if the Microsoft Exchange Server services are responding to RPC requests from the client workstations via the network.

Syntax

```
rpcping [/t <protseq>] [/s <server_addr>] [/e <endpoint>
        |/f <interface UUID>[,majorver]] [/O <interface object UUID]
        [/i <#_iterations>] [/u <security_package_id>] [/a <authn_level>]
        [/N <server_princ_name>] [/I <auth_identity>] [/C <capabilities>]
        [/T <identity_tracking>] [/M <impersonation_type>]
        [/S <server_sid>] [/P <proxy_auth_identity>] [/F <RPCHTTP_flags>]
        [/H <RPC/HTTP_authn_schemes>] [/o <binding_options>]
        [/B <server_certificate_subject>] [/b] [/E] [/q] [/c]
        [/A <http_proxy_auth_identity>] [/U <HTTP_proxy_authn_schemes>]
        [/r <report_results_interval>] [/v <verbose_level>] [/d]
```

Parameters

Parameter	Description
/t `<protseq>`	Specifies the protocol sequence to use. Can be one of the standard RPC protocol sequences: ncacn_ip_tcp, ncacn_np, or ncacn_http. If not specified, default is ncacn_ip_tcp.
/s `<server_addr>`	Specifies the server address. If not specified, the local machine will be pinged.
/e `<endpoint>`	Specifies the endpoint to ping. If none is specified, the endpoint mapper on the target machine will be pinged. This option is mutually exclusive with the interface (**/f**) option.
/o `<binding_options>`	Specifies the binding options for the RPC ping.

Parameter	Description
/f `<interface UUID> [,Majorver]`	Specifies the interface to ping. This option is mutually exclusive with the endpoint option. The interface is specified as a UUID. if the *majorver* is not specified, version 1 of the interface will be sought. When interface is specified, **rpcping** will query the endpoint mapper on the target machine to retrieve the endpoint for the specified interface. The endpoint mapper will be queried using the options specified in the command line.
/O `<object UUID>`	Specifies the object UUID if the interface registered one.
/i `<#_iterations>`	Specifies the number of calls to make. The default is 1. This option is useful for measuring connection latency if multiple iterations are specified.
/u `<security_package_id>`	Specifies the security package (security provider) RPC will use to make the call. The security package is identified as a number or a name. If a number is used it is the same number as in the RpcBindingSetAuthInfoEx API. If you specify this option, you must specify an authentication level other than *none*. There's no default for this option. If it isn't specified, RPC won't use security for the ping. The list below shows the names and numbers. Names are not case sensitive: • Negotiate / 9 or one of nego, snego or negotiate • NTLM / 10 or NTLM • SChannel / 14 or SChannel • Kerberos / 16 or Kerberos • Kernel / 20 or Kernel
/a `<authn_level>`	Specifies the authentication level to use. If this option is specified, the security package ID (**/u**) must also be specified. If this option isn't specified, RPC won't use security for the ping. There's no default for this option. Possible values are: • connect • call • pkt • integrity • privacy
/N `<server_princ_name>`	Specifies a server principal name. This field can be used only when authentication level and security package are selected.

Parameter	Description
/l `<auth_identity>`	Allows you to specify alternative identity to connect to the server. The identity is in the form user,domain,password. If the user name, domain, or password have special characters that can be interpreted by the shell, enclose the identity in double quotes. You can specify `\*` instead of the password and RPC will prompt you to enter the password without echoing it on the screen. If this field is not specified, the identity of the logged on user will be used. This field can be used only when authentication level and security package are selected.
/C `<capabilities>`	Specifies a hexadecimal bitmask of flags. This field can be used only when authentication level and security package are selected.
/T `<identity_tracking>`	Specifies static or dynamic. If not specified, dynamic is the default. This field can be used only when authentication level and security package are selected.
/M `<impersonation_type>`	Specifies anonymous, identify, impersonate or delegate. Default is impersonate. This field can be used only when authentication level and security package are selected.
/S `<server_sid>`	Specifies the expected SID of the server. This field can be used only when authentication level and security package are selected.
/P `<proxy_auth_identity>`	Specifies the identity to authenticate with to the RPC/HTTP proxy. Has the same format as for the **/l** option. You must specify security package (**/u**), authentication level (**/a**), and authentication schemes (**/H**) in order to use this option.
/F `<RPCHTTP_flags>`	Specifies the flags to pass for RPC/HTTP front end authentication. The flags may be specified as numbers or names The currently recognized flags are: • Use SSL / 1 or ssl or use_ssl • Use first auth scheme / 2 or first or use_first You must specify security package (**/u**) and authentication level (**/a**) to use this option.

Parameter	Description
/H `<RPC/HTTP_authn_schemes>`	Specifies the authentication schemes to use for RPC/HTTP front end authentication. This option is a list of numerical values or names separated by comma. Example: Basic,NTLM. Recognized values are (names are not case sensitive): • Basic / 1 or Basic • NTLM / 2 or NTLM • Certificate / 65536 or Cert You must specify security package (**/u**) and authentication level (**/a**) in order to use this option.
/B `<server_certificate_subject>`	Specifies the server certificate subject. You must use SSL for this option to work. You must specify security package (**/u**) and authentication level (**/a**) in order to use this option.
/b	Retrieves the server certificate subject from the certificate sent by the server and prints it to a screen or a log file. Valid only when the Proxy echo only option (/E) and the use SSL options are specified. You must specify security package (**/u**) and authentication level (**/a**) in order to use this option.
/R	Specifies the HTTP proxy. If *none*, the RPC proxy is used. The value *default* means to use the IE settings in your client machine. Any other value will be treated as the explicit HTTP proxy. If you do not specify this flag, the default value is assumed, that is, the IE settings are checked. This flag is valid only when the **/E** (echo Only) flag is enabled.
/E	Restricts the ping to the RPC/HTTP proxy only. The ping does not reach the server. Useful when trying to establish whether the RPC/HTTP proxy is reachable. To specify an HTTP proxy, use the /R flag. If an HTTP proxy is specified in the /o flag, this option will be ignored. You must specify security package (**/u**) and authentication level (**/a**) in order to use this option.
/q	Specifies quiet mode. Does not issue any prompts except for passwords. Assumes *Y* response to all queries. Use this option with care.
/c	Use smart card certificate. rpcping will prompt user to choose smart card.

Parameter	Description
/A	Specifies the identity with which to authenticate to the HTTP proxy. Has the same format as for the /I option. You must specify authentication schemes (/U), security package (**/u**) and authentication level (**/a**) in order to use this option.
/U	Specifies the authentication schemes to use for HTTP proxy authentication. This option is a list of numerical values or names separated by comma. Example: Basic,NTLM. Recognized values are (names are not case sensitive): • Basic / 1 or Basic • NTLM / 2 or NTLM You must specify security package (**/u**) and authentication level (**/a**) in order to use this option.
/r	If multiple iterations are specified, this option will make **rpcping** display current execution statistics periodically instead after the last call. The report interval is given in seconds. Default is 15.
/v	Tells **rpcping** how verbose to make the output. Default value is 1. 2 and 3 provide more output from **rpcping**.
/d	Launches RPC network diagnostic UI.
/p	Specifies to prompt for credentials if authentication fails.
/?	Displays help at the command prompt.

Examples

To find out if the Exchange server you connect through RPC/HTTP is accessible, type:

```
rpcping /t ncacn_http /s exchange_server /o RpcProxy=front_end_proxy /P
username,domain,* /H Basic /u NTLM /a connect /F 3
```

Related links

- Command-Line Syntax Key

rsh

Article • 03/03/2021

Runs commands on remote computers running the RSH service or daemon.

> **Important**
>
> The **rexec** command has been deprecated, and isn't guaranteed to be supported in Windows.

After installing the subsystem for UNIX-based Applications, you can then open a C Shell or Korn Shell command window and run **rsh**. For more information, type **man rsh** at the C Shell or Korn Shell prompt.

rundll32

Article • 02/03/2023

Loads and runs 32-bit dynamic-link libraries (DLLs). There are no configurable settings for Rundll32. Help information is provided for a specific DLL you run with the **rundll32** command.

You must run the **rundll32** command from an elevated command prompt. To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.

Syntax

```
rundll32 <DLLname>
```

Parameters

Parameter	Description
Rundll32 printui.dll,PrintUIEntry	Displays the printer user interface.

Remarks

Rundll32 can only call functions from a DLL explicitly written to be called by Rundll32.

Related links

- Command-Line Syntax Key

rundll32 printui.dll,PrintUIEntry

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Automates many printer configuration tasks. printui.dll is the executable file that contains the functions used by the printer configuration dialog boxes. These functions can also be called from within a script or a command-line batch file, or they can be run interactively from the command prompt.

Syntax

```
rundll32 printui.dll PrintUIEntry [baseparameter] [modificationparameter1]
[modificationparameter2] [modificationparameterN]
```

You can also use the following alternate syntaxes, although the examples in this topic use the previous syntax:

```
rundll32 printui.dll,PrintUIEntry [baseparameter] [modificationparameter1]
[modificationparameter2] [ModificationParameterN]
```

```
rundll32 printui PrintUIEntry [baseparameter] [modificationparameter1]
[modificationparameter2] [modificationparameterN]
```

```
rundll32 printui,PrintUIEntry [baseparameter] [modificationparameter1]
[modificationparameter2] [modificationparameterN]
```

Parameters

There are two types of parameters: base parameters and modification parameters. Base parameters specify the function that the command is to perform. Only one of these

parameters can appear in a given command line. Then, you can modify the base parameter by using one or more of the modification parameters if they are applicable to the base parameter (not all modification parameters are supported by all base parameters).

Base Parameters	Description
/dl	Deletes the local printer.
/dn	Deletes a network printer connection.
/dd	Deletes a printer driver.
/e	Displays the printing preferences for a given printer.
/ga	adds a per computer printer connection (the connection is available to any user on that computer when they log on).
/ge	Displays per computer printer connections on a computer.
/gd	Deletes a per computer printer connection (the connection is deleted the next time a user logs on).
/ia	Installs a printer driver by using an .inf file.
/id	Installs a printer driver by using the add printer Driver Wizard.
/if	Installs a printer by using an .inf file.
/ii	Installs a printer by using the add printer wizard with an .inf file.
/il	Installs a printer by using the add printer wizard.
/in	Connects to a remote network printer.
/ip	Installs a printer by using the Network printer Installation Wizard (available from the user interface from print Management).
/k	prints a test page on a printer.
/o	Displays the queue for a printer.
/p	Displays the properties of a printer. When you use this parameter, you must also specify a value for the modification parameter **/n[name]**.
/s	Displays the properties of a print server. If you want to view the local print server, you do not need to use a modification parameter. However, if you want to view a remote print server, you must specify the **/c[name]** modification parameter.

Base Parameters	Description
/Ss	Specifies what type of information for a printer will be stored. If none of the values for **/Ss** are specified, the default behavior is as if all of them were specified. Use this base parameter with the following values placed at the end of the command line: • **2**: Stores the information contained in the printer s printER_INFO_2 structure. This structure contains the basic information about the printer such as its name, server name, port name, and share name. • **7**: Used to store the directory service information contained in the printER_INFO_7 structure. • **c**: Stores the color profile information for a printer. • **d**: Stores printer specific data such as the printer s hardware ID. • **s**: Stores the printer s security descriptor. • **g**: Stores the information in the printer s global DEVmode structure. • **m**: Stores the minimal settings for the printer. This is equivalent to specifying **2 d**, and **g**. • **u**: Stores the information in the printer s per user DEVmode structure.

Base Parameters	Description
/Sr	Specifies what information about a printer is restored and how conflicts in settings are handled. Use with the following values placed at the end of the command line: • **2**: Restores the information contained in the printer s printER_INFO_2 structure. This structure contains the basic information about the printer such as its name, server name, port name, and share name. • **7**: Restores the directory service information contained in the printER_INFO_7 structure. • **c**: Restores the color profile information for a printer. • **d**: Restores printer specific data, such as the printer s hardware ID. • **s**: Restores the printer s security descriptor. • **g**: Restores the information in the printer s global DEVmode structure. • **m**: Restores the minimal settings for the printer. This is equivalent to specifying **2**, **d**, and **g**. • **u** Restores the information in the printe s per user DEVmode structure. • **r**: If the printer name stored in the file is different from the name of the printer being restored to, then use the current printer name. This cannot be specified with **f**. If neither **r** nor **f** is specified and the names do not match, restoration of the settings fails. • **f**: If the printer name stored in the file is different from the name of the printer being restored to, then use the printer name in the file. This cannot be specified with **r**. If neither **f** nor **r** is specified and the names do not match, restoration of the settings fails. • **p**: If the port name in the file being restored from does not match the current port name of the printer being restored to, the printer s current port name is used. • **h**: If the printer being restored to could not be shared using the resource share name in the saved settings file, then attempt to share the printer with either the current share name or a new generated share name if neither **H** nor **h** is specified and the printer being restored to cannot be shared with the saved share name, then restoration fails. • **h**: If the printer being restored to cannot be shared with the saved share name, then do not share the printer. If neither **H** nor **h** is specified and the printer being restored to cannot be shared with the saved share name, then restoration fails. • **i**: If the driver in the saved settings file does not match the driver for the printer being restored to, then the restoration fails.
/Xg	Retrieves the settings for a printer.
/Xs	Sets the settings for a printer.
/y	Sets the printer being installed as the default printer.
/?	Displays the in-product help for the command and its associated parameters.

Base Parameters	Description
@[file]	Specifies a command-line argument file and directly inserts the text in that file into the command line.

Modification Parameters	Description
/a[file]	Specifies the binary file name.
/b[name]	Specifies the base printer name.
/c[name]	Specifies the computer name if the action to be performed is on a remote computer.
/f[file]	Species the Universal Naming Convention (UNC) path and name of the .inf file name or the output file name, depending on the task that you are performing. Use **/F[file]** to specify a dependent .inf file.
/F[file]	Specifies the UNC path and name of a .inf file that the .inf file specified with **/f[file]** depends on.
/h[architecture]	Specifies the driver architecture. Use one of the following: **x86**, **x64**, or **Itanium**.
/j[provider]	Specifies the print provider name.
/l[path]	Specifies the UNC path where the printer driver files that you are using are located.
/m[model]	Specifies the driver model name. (This value can be specified in the .inf file.)
/n[name]	Specifies the printer name.
/q	Runs the command with no notifications to the user.
/r[port]	Specifies the port name.
/u	Specifies to use the existing printer driver if it is already installed.
/t[#]	Specifies the zero-based index page to start on.
/v[version]	Specifies the driver version. If you do not also specify a value for **/K**, you must specify one of the following values: **type 2 - Kernel mode** or **type 3 - User mode**.
/w	prompts the user for a driver if the driver is not found in the .inf file that is specified by **/f**.
/Y	Specifies that printer names should not be automatically generated.
/z	Specifies to not automatically share the printer being installed.

Modification Parameters	Description
/K	changes the meaning of the parameter **/h[architecture]** to accept **2** in place of **x86**, **3** in place of **x64**, or **4** in place of **Itanium**. It also changes the value of the parameter **/v[version]** to accept **2** in the place of **type 2 - Kernel mode** and **3** in place of **type 3 - User mode**.
/Z	Shares the printer that is being installed. Only use with the **/if** parameter.
/Mw[message]	Displays a warning message to the user before committing the changes specified in the command line.
/Mq[message]	Displays a confirmation message to the user before committing the changes specified in the command line.
/W[flags]	Specifies any parameters or options for the add printer wizard, the add printer Driver Wizard, and the Network printer Installation Wizard. **r**: Enables the wizards to be restarted from the last page.
/G[flags]	Specifies global parameters and options that you want to use. **w**: Suppresses setup driver warnings to the user.

Remarks

- The **PrintUIEntry** keyword is case sensitive, and you must enter the syntax for this command with the exact capitalization shown in the examples in this topic.
- For more examples, at a command prompt type: **rundll32 printui.dll,PrintUIEntry /?**

Examples

To add a new remote printer, printer1, for a computer, Client1, which is visible for the user account where this command is run, type:

```
rundll32 printui.dll PrintUIEntry /in /n\\client1\printer1
```

To add a printer using the add printer wizard and using an .inf file, InfFile.inf, located on drive c: at Infpath, type:

```
rundll32 printui.dll PrintUIEntry /ii /f c:\Infpath\InfFile.inf
```

To delete an existing printer, printer1, on a computer, Client1, type:

```
rundll32 printui.dll PrintUIEntry /dn /n\\client1\printer1
```

To add a per computer printer connection, printer2, for all users of a computer, Client2, type (the connection will be applied when a user logs on):

```
rundll32 printui.dll PrintUIEntry /ga /n\\client2\printer2
```

To delete a per computer printer connection, printer2, for all users of a computer, Client2, type (the connection will be deleted when a user logs on):

```
rundll32 printui.dll PrintUIEntry /gd /n\\client2\printer2
```

To view the properties of the print server, printServer1, type:

```
rundll32 printui.dll PrintUIEntry /s /t1 /c\\printserver1
```

To view the properties of a printer, printer3, type:

```
rundll32 printui.dll PrintUIEntry /p /n\\printer3
```

Related links

- rundll32
- print Command Reference

rwinsta

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Resets (deletes) a session on a Remote Desktop Session Host server.

> **Note**
>
> This command is the same as the **reset session command**.

> **Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Related links

- reset session
- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

sc.exe config

Article • 02/03/2023

Modifies the value of a service's entries in the registry and in the Service Control Manager database.

Syntax

```
sc.exe [<servername>] config [<servicename>] [type= {own | share | kernel | filesys | rec | adapt | interact type= {own | share}}] [start= {boot | system | auto | demand | disabled | delayed-auto}] [error= {normal | severe | critical | ignore}] [binpath= <binarypathname>] [group= <loadordergroup>] [tag= {yes | no}] [depend= <dependencies>] [obj= {<accountname> | <objectname>}] [displayname= <displayname>] [password= <password>]
```

Parameters

Parameter	Description
`<servername>`	Specifies the name of the remote server on which the service is located. The name must use the Universal Naming Convention (UNC) format (for example, \myserver). To run SC.exe locally, don't use this parameter.
`<servicename>`	Specifies the service name returned by the **getkeyname** operation.
`type= {own | share | kernel | filesys | rec | adapt | interact type= {own | share}}`	Specifies the service type. The options include: • **own** - Specifies a service that runs in its own process. It doesn't share an executable file with other services. This is the default value. • **share** - Specifies a service that runs as a shared process. It shares an executable file with other services. • **kernel** - Specifies a driver. • **filesys** - Specifies a file system driver. • **rec** - Specifies a file system-recognized driver that identifies file systems used on the computer. • **adapt** - Specifies an adapter driver that identifies hardware devices such as keyboards, mice, and disk drives. • **interact** - Specifies a service that can interact with the desktop, receiving input from users. Interactive services must be run under the LocalSystem account. This type must be used in conjunction with **type= own** or **type= shared** (for example, **type= interact type= own**). Using **type= interact** by itself will generate an error.

Parameter	Description
`start= {boot | system | auto | demand | disabled | delayed-auto}`	Specifies the start type for the service. The options include: • **boot** - Specifies a device driver that is loaded by the boot loader. • **system** - Specifies a device driver that is started during kernel initialization. • **auto** - Specifies a service that automatically starts each time the computer is restarted and runs even if no one logs on to the computer. • **demand** - Specifies a service that must be started manually. This is the default value if **start=** is not specified. • **disabled** - Specifies a service that cannot be started. To start a disabled service, change the start type to some other value. • **delayed-auto** - Specifies a service that starts automatically a short time after other auto services are started.
`error= {normal | severe | critical | ignore}`	Specifies the severity of the error if the service fails to start when the computer is started. The options include: • **normal** - Specifies that the error is logged and a message box is displayed, informing the user that a service has failed to start. Startup will continue. This is the default setting. • **severe** - Specifies that the error is logged (if possible). The computer attempts to restart with the last-known good configuration. This could result in the computer being able to restart, but the service may still be unable to run. • **critical** - Specifies that the error is logged (if possible). The computer attempts to restart with the last-known good configuration. If the last-known good configuration fails, startup also fails, and the boot process halts with a Stop error. • **ignore** - Specifies that the error is logged and startup continues. No notification is given to the user beyond recording the error in the Event Log.
`binpath= <binarypathname>`	Specifies a path to the service binary file. There is no default for **binpath=**, and this string must be supplied. Additionally, **ntsd -d** can be specified in front of the string for debugging. For more information, see Debugging using CDB and NTSD.
`group= <loadordergroup>`	Specifies the name of the group of which this service is a member. The list of groups is stored in the registry, in the **HKLM\System\CurrentControlSet\Control\ServiceGroupOrder** subkey. The default value is null.
`tag= {yes | no}`	Specifies whether or not to obtain a TagID from the CreateService call. Tags are used only for boot-start and system-start drivers.

Parameter	Description
`depend= <dependencies>`	Specifies the names of services or groups that must start before this service. The names are separated by forward slashes (/).
`obj= {<accountname> | <objectname>}`	Specifies a name of an account in which a service will run, or specifies a name of the Windows driver object in which the driver will run. The default setting is **LocalSystem**.
`displayname= <displayname>`	Specifies a descriptive name for identifying the service in user interface programs. For example, the subkey name of one particular service is **wuauserv**, which has a more friendly display name of Automatic Updates.
`password= <password>`	Specifies a password. This is required if an account other than the LocalSystem account is used.
/?	Displays help at the command prompt.

Remarks

- Each command-line option (parameter) must include the equal sign as part of the option name.
- A space is required between an option and its value (for example, **type= own**. If the space is omitted, the operation fails.

Examples

To specify a binary path for the *NewService* service, type:

```
sc.exe config NewService binpath= c:\windows\system32\NewServ.exe
```

Related links

- Command-Line Syntax Key

sc.exe create

Article • 09/29/2023

Creates a subkey and entries for a service in the registry and in the Service Control Manager database.

Syntax

```
sc.exe [<servername>] create [<servicename>] [type= {own | share | kernel | filesys | rec | interact type= {own | share}}] [start= {boot | system | auto | demand | disabled | delayed-auto}] [error= {normal | severe | critical | ignore}] [binpath= <binarypathname>] [group= <loadordergroup>] [tag= {yes | no}] [depend= <dependencies>] [obj= {<accountname> | <objectname>}] [displayname= <displayname>] [password= <password>]
```

Parameters

Parameter	Description
`<servername>`	Specifies the name of the remote server on which the service is located. The name must use the Universal Naming Convention (UNC) format (for example, \myserver). To run SC.exe locally, don't use this parameter.
`<servicename>`	Specifies the service name returned by the **getkeyname** operation.
`type= {own | share | kernel | filesys | rec | interact type= {own | share}}`	Specifies the service type. The options include: • **own** - Specifies a service that runs in its own process. It doesn't share an executable file with other services. This is the default value. • **share** - Specifies a service that runs as a shared process. It shares an executable file with other services. • **kernel** - Specifies a driver. • **filesys** - Specifies a file system driver. • **rec** - Specifies a file system-recognized driver that identifies file systems used on the computer. • **interact** - Specifies a service that can interact with the desktop, receiving input from users. Interactive services must be run under the LocalSystem account. This type must be used in conjunction with **type= own** or **type= share** (for example, **type= interact type= own**). Using **type= interact** by itself will generate an error.
`start= {boot | system | auto |`	Specifies the start type for the service. The options include: • **boot** - Specifies a device driver that is loaded by the boot loader.

Parameter	Description
`demand | disabled | delayed-auto}`	• **system** - Specifies a device driver that is started during kernel initialization. • **auto** - Specifies a service that automatically starts each time the computer is restarted and runs even if no one logs on to the computer. • **demand** - Specifies a service that must be started manually. This is the default value if **start=** is not specified. • **disabled** - Specifies a service that cannot be started. To start a disabled service, change the start type to some other value. • **delayed-auto** - Specifies a service that starts automatically a short time after other auto services are started.
`error= {normal | severe | critical | ignore}`	Specifies the severity of the error if the service fails to start when the computer is started. The options include: • **normal** - Specifies that the error is logged and a message box is displayed, informing the user that a service has failed to start. Startup will continue. This is the default setting. • **severe** - Specifies that the error is logged (if possible). The computer attempts to restart with the last-known good configuration. This could result in the computer being able to restart, but the service may still be unable to run. • **critical** - Specifies that the error is logged (if possible). The computer attempts to restart with the last-known good configuration. If the last-known good configuration fails, startup also fails, and the boot process halts with a Stop error. • **ignore** - Specifies that the error is logged and startup continues. No notification is given to the user beyond recording the error in the Event Log.
`binpath= <binarypathname>`	Specifies a path to the service binary file. There is no default for **binpath=**, and this string must be supplied.
`group= <loadordergroup>`	Specifies the name of the group of which this service is a member. The list of groups is stored in the registry, in the **HKLM\System\CurrentControlSet\Control\ServiceGroupOrder** subkey. The default value is null.
`tag= {yes | no}`	Specifies whether or not to obtain a TagID from the CreateService call. Tags are used only for boot-start and system-start drivers.
`depend= <dependencies>`	Specifies the names of services or groups that must start before this service. The names are separated by forward slashes (/).
`obj= {<accountname> | <objectname>}`	Specifies a name of an account in which a service will run, or specifies a name of the Windows driver object in which the driver will run. The default setting is **LocalSystem**.

Parameter	Description
`displayname= <displayname>`	Specifies a friendly name for identifying the service in user interface programs. For example, the subkey name of one particular service is **wuauserv**, which has a more friendly display name of Automatic Updates.
`password= <password>`	Specifies a password. This is required if an account other than the LocalSystem account is used.
/?	Displays help at the command prompt.

Remarks

- Each command-line option (parameter) must include the equal sign as part of the option name.
- A space is required between an option and its value (for example, **type= own**. If the space is omitted, the operation fails.

Examples

To create and register a new binary path for the *NewService* service, type:

```
sc.exe \\myserver create NewService binpath= c:\windows\system32\NewServ.exe
```

```
sc.exe create NewService binpath= c:\windows\system32\NewServ.exe type=
share start= auto depend= +TDI NetBIOS
```

To learn more about the `sc.exe` command, see SC commands.

Related links

- Command-Line Syntax Key

sc.exe delete

Article • 02/03/2023

Deletes a service subkey from the registry. If the service is running or if another process has an open handle to the service, the service is marked for deletion.

> **Note**
>
> We don't recommend you to use this command to delete built-in operating system services such as DHCP, DNS, or Internet Information Services. To install, remove, or reconfigure operating system roles, services and components, see **Install or Uninstall Roles, Role Services, or Features**

Syntax

```
sc.exe [<servername>] delete [<servicename>]
```

Parameters

Parameter	Description
`<servername>`	Specifies the name of the remote server on which the service is located. The name must use the Universal Naming Convention (UNC) format (for example, \myserver). To run SC.exe locally, don't use this parameter.
`<servicename>`	Specifies the service name returned by the **getkeyname** operation.
/?	Displays help at the command prompt.

Examples

To delete the service subkey **NewServ** from the registry on the local computer, type:

```
sc.exe delete NewServ
```

Related links

- Command-Line Syntax Key

Sc.exe query

Article • 02/03/2023

Obtains and displays information about the specified service, driver, type of service, or type of driver.

Syntax

```
sc.exe [<servername>] query [<servicename>] [type= {driver | service | all}]
[type= {own | share | interact | kernel | filesys | rec | adapt}] [state=
{active | inactive | all}] [bufsize= <Buffersize>] [ri= <Resumeindex>]
[group= <groupname>]
```

Parameters

Parameter	Description
`<servername>`	Specifies the name of the remote server on which the service is located. The name must use the Universal Naming Convention (UNC) format (for example, \myserver). To run SC.exe locally, don't use this parameter.
`<servicename>`	Specifies the service name returned by the **getkeyname** operation. This **query** parameter isn't used in conjunction with other **query** parameters (other than *servername*).
`type= {driver | service | all}`	Specifies what to enumerate. The options include: • **driver** - Specifies that only drivers are enumerated. • **service** - Specifies only services are enumerated. This is the default value. • **all** - Specifies that both drivers and services are enumerated.

Parameter	Description
`type= {own | share | interact | kernel | filesys | rec | adapt}`	Specifies the type of services or type of drivers to be enumerated. The options include: • **own** - Specifies a service that runs in its own process. It doesn't share an executable file with other services. This is the default value. • **share** - Specifies a service that runs as a shared process. It shares an executable file with other services. • **kernel** - Specifies a driver. • **filesys** - Specifies a file system driver. • **rec** - Specifies a file system-recognized driver that identifies file systems used on the computer. • **interact** - Specifies a service that can interact with the desktop, receiving input from users. Interactive services must be run under the LocalSystem account. This type must be used in conjunction with **type= own** or **type= shared** (for example, **type= interact type= own**). Using **type= interact** by itself will generate an error.
`state= {active | inactive | all}`	Specifies the started state of the service to be enumerated. The options include: • **active** - Specifies all active services. This is the default value. • **inactive** - Specifies all paused or stopped services. • **all** - Specifies all services.
`bufsize= <Buffersize>`	Specifies the size (in bytes) of the enumeration buffer. The default buffer size is 1,024 bytes. You should increase the size of the buffer when the display resulting from a query goes over 1,024 bytes.
`ri= <Resumeindex>`	Specifies the index number at which enumeration is to begin or resume. The default value is 0 (zero). If more information is returned than what the default buffer can display, use this parameter with the `bufsize=` parameter.
`group= <Groupname>`	Specifies the service group to be enumerated. By default, all groups are enumerated. By default, all groups are enumerated (**group= **).
/?	Displays help at the command prompt.

Remarks

- Each command-line option (parameter) must include the equal sign as part of the option name.
- A space is required between an option and its value (for example, **type= own**. If the space is omitted, the operation fails.
- The **query** operation displays the following information about a service: SERVICE_NAME (service's registry subkey name), TYPE, STATE (as well as states

which are not available), WIN32_EXIT_B, SERVICE_EXIT_B, CHECKPOINT, and WAIT_HINT.

- The **type=** parameter can be used twice in some cases. The first appearance of the **type=** parameter specifies whether to query services, drivers, or both (**all**). The second appearance of the **type=** parameter specifies a type from the **create** operation to further narrow a query's scope.

- When the display results from a **query** command exceed the size of the enumeration buffer, a message similar to the following is displayed:

```
Enum: more data, need 1822 bytes start resume at index 79

To display the remaining **query** information, rerun **query**,
setting **bufsize=** to be the number of bytes and setting **ri=** to
the specified index. For example, the remaining output would be
displayed by typing the following at the command prompt:

sc.exe query bufsize= 1822 ri= 79
```

Examples

To display information for active services only, type either of the following commands:

```
sc.exe query
sc.exe query type= service
```

To display information for active services, and to specify a buffer size of 2,000 bytes, type:

```
sc.exe query type= all bufsize= 2000
```

To display information for the *wuauserv* service, type:

```
sc.exe query wuauserv
```

To display information for all services (active and inactive), type:

```
sc.exe query state= all
```

To display information for all services (active and inactive), beginning at line 56, type:

```
sc.exe query state= all ri= 56
```

To display information for interactive services, type:

```
sc.exe query type= service type= interact
```

To display information for drivers only, type:

```
sc.exe query type= driver
```

To display information for drivers in the *Network Driver Interface Specification (NDIS) group*, type:

```
sc.exe query type= driver group= NDIS
```

Related links

- Command-Line Syntax Key

schtasks commands

Article • 02/03/2023

Schedules commands and programs to run periodically or at a specific time, adds and removes tasks from the schedule, starts and stops tasks on demand, and displays and changes scheduled tasks.

> **Note**
>
> The **schtasks.exe** tool performs the same operations as **Scheduled Tasks** in **Control Panel**. You can use these tools together and interchangeably.

Required permissions

- To schedule, view, and change all tasks on the local computer, you must be a member of the Administrators group.
- To schedule, view, and change all tasks on the remote computer, you must be a member of the Administrators group on the remote computer, or you must use the **/u** parameter to provide the credentials of an Administrator of the remote computer.
- You can use the **/u** parameter in a **/create** or **/change** operation if the local and remote computers are in the same domain, or if the local computer is in a domain that the remote computer domain trusts. Otherwise, the remote computer can't authenticate the user account specified, and it can't verify that the account is a member of the Administrators group.
- The task you plan to run must have the appropriate permission; these permissions vary by task. By default, tasks run with the permissions of the current user of the local computer, or with the permissions of the user specified by the **/u** parameter, if one is included. To run a task with permissions of a different user account or with system permissions, use the **/ru** parameter.

Syntax

```
schtasks /change
schtasks /create
```

```
schtasks /delete
schtasks /end
schtasks /query
schtasks /run
```

Parameters

Parameter	Description
schtasks change	Changes one or more of the following properties of a task: • The program that the task runs (/tr) • The user account under which the task runs (/ru) • The password for the user account (/rp) • Adds the interactive-only property to the task (/it)
schtasks create	Schedules a new task.
schtasks delete	Deletes a scheduled task.
schtasks end	Stops a program started by a task.
schtasks query	Displays tasks scheduled to run on the computer.
schtasks run	Starts a scheduled task immediately. The **run** operation ignores the schedule, but uses the program file location, user account, and password saved in the task to run the task immediately.

Related links

- Command-Line Syntax Key

schtasks change

Article • 02/03/2023

Changes one or more of the following properties of a task:

- The program that the task runs (**/tr**)
- The user account under which the task runs (**/ru**)
- The password for the user account (**/rp**)
- Adds the interactive-only property to the task (**/it**)

Required permissions

- To schedule, view, and change all tasks on the local computer, you must be a member of the Administrators group.
- To schedule, view, and change all tasks on the remote computer, you must be a member of the Administrators group on the remote computer, or you must use the **/u** parameter to provide the credentials of an Administrator of the remote computer.
- You can use the **/u** parameter in a **/create** or **/change** operation if the local and remote computers are in the same domain, or if the local computer is in a domain that the remote computer domain trusts. Otherwise, the remote computer can't authenticate the user account specified, and it can't verify that the account is a member of the Administrators group.
- The task you plan to run must have the appropriate permission; these permissions vary by task. By default, tasks run with the permissions of the current user of the local computer, or with the permissions of the user specified by the **/u** parameter, if one is included. To run a task with permissions of a different user account or with system permissions, use the **/ru** parameter.

Syntax

```
schtasks /change /tn <Taskname> [/s <computer> [/u [<domain>\]<user> [/p
<password>]]] [/ru <username>] [/rp <password>] [/tr <Taskrun>] [/st
<Starttime>] [/ri <interval>] [/rl <level>] [{/et <Endtime> | /du
```

```
<duration>} [/k]] [/sd <Startdate>] [/ed <Enddate>] [/{ENABLE | DISABLE}]
[/it] [/z]
```

Parameters

Parameter	Description
/tn `<Taskname>`	Identifies the task to be changed. Enter the task name (**Note**: Task names that have a space in its name are required to be wrapped in double quotes).
/s `<computer>`	Specifies the name or IP address of a remote computer (with or without backslashes). The default is the local computer.
/u `[<domain>]`	Runs this command with the permissions of the specified user account. By default, the command runs with the permissions of the current user of the local computer. The specified user account must be a member of the Administrators group on the remote computer. The **/u** and **/p** parameters are valid only when you use **/s**.
/p `<password>`	Specifies the password of the user account specified in the **/u** parameter. If you use the **/u** parameter without the **/p** parameter or the password argument, schtasks will prompt you for a password. The **/u** and **/p** parameters are valid only when you use **/s**.
/ru `<username>`	Changes the user name under which the scheduled task has to run. For the system account, valid values are "", "*NT AUTHORITY\SYSTEM*", or "*SYSTEM*".
/rp `<password>`	Specifies a new password for the existing user account, or the user account specified by the **/ru** parameter. This parameter is ignored with used with the local System account.
/tr `<Taskrun>`	Changes the program that the task runs. Enter the fully qualified path and file name of an executable file, script file, or batch file. If you don't add the path, **schtasks** assumes that the file is in the `<systemroot>\System32` directory. The specified program replaces the original program run by the task.
/st `<Starttime>`	Specifies the start time for the task, using the 24-hour time format, HH:mm. For example, a value of 14:30 is equivalent to the 12-hour time of 2:30 PM.
/ri `<interval>`	Specifies the repetition interval for the scheduled task, in minutes. Valid range is 1 - 599940 (599940 minutes = 9999 hours). If either the **/et** or **/du** parameters are specified, the default is **10 minutes**.
/rl `<level>`	Specifies the Run Level for the job. Acceptable values are LIMITED (scheduled tasks will be ran with the least level of privileges, such as Standard User accounts) and HIGHEST (scheduled tasks will be ran with the highest level of privileges, such as Superuser accounts). (**Note**: LIMITED is the default value).
/et `<Endtime>`	Specifies the end time for the task, using the 24-hour time format, HH:mm. For example, a value of 14:30 is equivalent to the 12-hour time of 2:30 PM.

Parameter	Description
/du `<duration>`	A value that specifies the duration to run the task. The time format is HH:mm (24-hour time). For example, a value of 14:30 is equivalent to the 12-hour time of 2:30 PM.
/k	Stops the program that the task runs at the time specified by **/et** or **/du**. Without **/k**, schtasks doesn't start the program again after it reaches the time specified by **/et** or **/du** nor does it stop the program if it's still running. This parameter is optional and valid only with a MINUTE or HOURLY schedule.
/sd `<Startdate>`	Specifies the first date on which the task should be run. The date format is MM/DD/YYYY.
/ed `<Enddate>`	Specifies the last date on which the task should be run. The format is MM/DD/YYYY.
/ENABLE	Specifies to enable the scheduled task.
/DISABLE	Specifies to disable the scheduled task.
/it	Specifies to run the scheduled task only when the run as user (the user account under which the task runs) is logged on to the computer. This parameter has no effect on tasks that run with system permissions or tasks that already have the interactive-only property set. You can't use a change command to remove the interactive-only property from a task. By default, run as user is the current user of the local computer when the task is scheduled or the account specified by the **/u** parameter, if one is used. However, if the command includes the **/ru** parameter, then the run as user is the account specified by the **/ru** parameter.
/z	Specifies to delete the task upon the completion of its schedule.
/?	Displays help at the command prompt.

Remarks

- The **/tn** and **/s** parameters identify the task. The **/tr**, **/ru**, and **/rp** parameters specify properties of the task that you can change.
- The **/ru** and **/rp** parameters specify the permissions under which the task runs. The **/u** and **/p** parameters specify the permissions used to change the task.
- To change tasks on a remote computer, the user must be logged on to the local computer with an account that is a member of the Administrators group on the remote computer.
- To run a **/change** command with the permissions of a different user (**/u**, **/p**), the local computer must be in the same domain as the remote computer or must be in

a domain that the remote computer domain trusts.

- The System account doesn't have interactive logon rights. Users don't see, and can't interact with, programs run with system permissions. To identify tasks with the **/it** property, use a verbose query (**/query /v**). In a verbose query display of a task with **/it**, the Logon Mode field has a value of Interactive only.

Examples

To change the program that the Virus Check task runs from *VirusCheck.exe* to *VirusCheck2.exe*, type:

```
schtasks /change /tn Virus Check /tr C:\VirusCheck2.exe
```

This command uses the **/tn** parameter to identify the task and the **/tr** parameter to specify the new program for the task. (You can't change the task name.)

To change the password of the user account for the *RemindMe* task on the remote computer, *Svr01*, type:

```
schtasks /change /tn RemindMe /s Svr01 /rp p@ssWord3
```

This procedure is required whenever the password for a user account expires or changes. If the password saved in a task is no longer valid, then the task doesn't run. The command uses the **/tn** parameter to identify the task and the **/s** parameter to specify the remote computer. It uses the **/rp** parameter to specify the new password, *p@ssWord3*.

To change the ChkNews task, which starts Notepad.exe every morning at 9:00 A.M., to start Internet Explorer instead, type:

```
schtasks /change /tn ChkNews /tr c:\program files\Internet
Explorer\iexplore.exe /ru DomainX\Admin01
```

The command uses the **/tn** parameter to identify the task. It uses the **/tr** parameter to change the program that the task runs and the /ru parameter to change the user account under which the task runs. The **/ru** and **/rp** parameters, which provide the

password for the user account, is not used. You must provide a password for the account, but you can use the **/ru** and **/rp** parameter and type the password in clear text, or wait for SchTasks.exe to prompt you for a password, and then enter the password in obscured text.

To change the SecurityScript task so that it runs with permissions of the System account, type:

```
schtasks /change /tn SecurityScript /ru
```

The command uses the **/ru** parameter to indicate the System account. Because tasks run with System account permissions do not require a password, SchTasks.exe does not prompt for one.

To add the interactive-only property to MyApp, an existing task, type:

```
schtasks /change /tn MyApp /it
```

This property assures that the task runs only when the run as user, that is, the user account under which the task runs, is logged on to the computer. The command uses the **/tn** parameter to identify the task and the **/it** parameter to add the interactive-only property to the task. Because the task already runs with the permissions of my user account, you don't need to change the **/ru** parameter for the task.

Related links

- Command-Line Syntax Key
- schtasks create command
- schtasks delete command
- schtasks end command
- schtasks query command
- schtasks run command

schtasks create

Article • 10/10/2023

Schedules a task.

Syntax

```
schtasks /create /sc <scheduletype> /tn <taskname> /tr <taskrun> [/s
<computer> [/u [<domain>\]<user> [/p <password>]]] [/ru {[<domain>\]<user> |
system}] [/rp <password>] [/mo <modifier>] [/d <day>[,<day>...] | *] [/m
<month>[,<month>...]] [/i <idletime>] [/st <starttime>] [/ri <interval>]
[{/et <endtime> | /du <duration>} [/k]] [/sd <startdate>] [/ed <enddate>]
[/it] [/np] [/z] [/xml <xmlfile>] [/v1] [/f] [/rl <level>] [/delay
<delaytime>] [/hresult]
```

Parameters

Parameter	Description
/sc `<scheduletype>`	Specifies the schedule type. The valid values include: • **MINUTE** - Specifies the number of minutes before the task should run. • **HOURLY** - Specifies the number of hours before the task should run. • **DAILY** - Specifies the number of days before the task should run. • **WEEKLY** Specifies the number of weeks before the task should run. • **MONTHLY** - Specifies the number of months before the task should run. • **ONCE** - Specifies that that task runs once at a specified date and time. • **ONSTART** - Specifies that the task runs every time the system starts. You can specify a start date, or run the task the next time the system starts. • **ONLOGON** - Specifies that the task runs whenever a user (any user) logs on. You can specify a date, or run the task the next time the user logs on. • **ONIDLE** - Specifies that the task runs whenever the system is idle for a specified period of time. You can specify a date, or run the task the next time the system is idle. • **ONEVENT** - Specifies that the task runs based on an event that matches information from the system event log including the EventID.

Parameter	Description
/tn `<taskname>`	Specifies a name for the task. Each task on the system must have a unique name and must conform to the rules for file names, not exceeding 238 characters. Use quotation marks to enclose names that include spaces. To store your scheduled task in a different folder, run **/tn** `<folder name\task name>`.
/tr `<Taskrun>`	Specifies the program or command that the task runs. Type the fully qualified path and file name of an executable file, script file, or batch file. The path name must not exceed 262 characters. If you don't add the path, **schtasks** assumes that the file is in the `<systemroot>\System32` directory.
/s `<computer>`	Specifies the name or IP address of a remote computer (with or without backslashes). The default is the local computer.
/u `[<domain>]`	Runs this command with the permissions of the specified user account. The default is the permissions of the current user of the local computer. The **/u** and **/p** parameters are valid only when you use **/s**. The permissions of the specified account are used to schedule the task and to run the task. To run the task with the permissions of a different user, use the **/ru** parameter. The user account must be a member of the Administrators group on the remote computer. Also, the local computer must be in the same domain as the remote computer, or must be in a domain that is trusted by the remote computer domain.
/p `<password>`	Specifies the password of the user account specified in the **/u** parameter. If you use the **/u** parameter without the **/p** parameter or the password argument, schtasks will prompt you for a password. The **/u** and **/p** parameters are valid only when you use **/s**.
/ru {[`<domain>`] `<user>` | `system`}	Runs the task with permissions of the specified user account. By default, the task runs with the permissions of the current user of the local computer, or with the permission of the user specified by the **/u** parameter, if one is included. The **/ru** parameter is valid when scheduling tasks on local or remote computers. The valid options include: • **Domain** - Specifies an alternate user account. • **System** - Specifies the local System account, a highly privileged account used by the operating system and system services.
/rp `<password>`	Specifies the password for the existing user account, or the user account specified by the **/ru** parameter. If you don't use this parameter when specifying a user account, SchTasks.exe will prompt you for the password next time you sign in. Don't use the **/rp** parameter for tasks that run with System account credentials (**/ru System**). The System account doesn't have a password and SchTasks.exe doesn't prompt for one.
/mo `<modifiers>`	Specifies how often the task runs within its schedule type. The valid options include:

Parameter	Description
	• **MINUTE** - Specifies that the task runs every <n> minutes. You can use any value between 1 - 1439 minutes. By default, this is 1 minute. • **HOURLY** - Specifies that the task runs every <n> hours. You can use any value between 1 - 23 hours. By default, this is 1 hour. • **DAILY** - Specifies that the task runs every <n> days. You can use any value between 1 - 365 days. By default, this is 1 day. • **WEEKLY** - Specifies that the task runs every <n> weeks. You can use any value between 1 - 52 weeks. By default, this is 1 week. • **MONTHLY** - Specifies that the task runs every <n> months. You can use any of the following values: ◦ A number between 1 - 12 months ◦ **LASTDAY** - To run the task on the last day of the month ◦ **FIRST, SECOND, THIRD, or FOURTH along with the `/d <day>` parameter** - Specifies the particular week and day to run the task. For example, on the third Wednesday of the month. • **ONCE** - Specifies that the task runs once. • **ONSTART** - Specifies that the task runs at startup. • **ONLOGON** - Specifies that the task runs when the user specified by the **/ru** parameter logs on. • **ONIDLE** - Specifies that the task runs after the system is idle for the number of minutes specified by the **/i** parameter
/d DAY[,DAY...]	Specifies how often the task runs within its schedule type. The valid options include: • **WEEKLY** - Specifies that the task runs weekly by providing a value between 1-52 weeks. Optionally, you can also add a specific day of the week by adding a value of MON - SUN or a range of [MON - SUN...]). • **MONTHLY** - Specifies that the task runs weekly each month by providing a value of FIRST, SECOND, THIRD, FOURTH, LAST. Optionally, you can also add a specific day of the week by adding a value of MON - SUN or by providing a number between 1 - 12 months. If you use this option, you can also add a specific day of the month, by providing a number between 1-31. **NOTE:** The date value of 1 - 31 is valid only without the **/mo** parameter, or if the **/mo** parameter is monthly (1 - 12). The default is day 1 (the first day of the month).
/m MONTH[,MONTH...]	Specifies a month or months of the year during which the scheduled task should run. The valid options include JAN - DEC and `*` (every month). The **/m** parameter is valid only with a MONTHLY schedule. It's required when the LASTDAY modifier is used. Otherwise, it's optional and the default value is `*` (every month).
/i `<Idletime>`	Specifies how many minutes the computer is idle before the task starts. A valid value is a whole number from 1 to 999. This parameter is valid only

Parameter	Description
	with an ONIDLE schedule, and then it's required.
/st `<Starttime>`	Specifies the start time for the task, using the 24-hour time format, HH:mm. The default value is the current time on the local computer. The **/st** parameter is valid with MINUTE, HOURLY, DAILY, WEEKLY, MONTHLY, and ONCE schedules. It's required for a ONCE schedule.
/ri `<interval>`	Specifies the repetition interval for the scheduled task, in minutes. This isn't applicable for schedule types: MINUTE, HOURLY, ONSTART, ONLOGON,ONIDLE, and ONEVENT. Valid range is 1 - 599940 (599940 minutes = 9999 hours). If either the **/et** or **/du** parameters are specified, the default is **10 minutes**.
/et `<endtime>`	Specifies the time of day that a minute or hourly task schedule ends in <HH:MM> 24-hour format. After the specified end time, schtasks does not start the task again until the start time recurs. By default, task schedules have no end time. This parameter is optional and valid only with a MINUTE or HOURLY schedule.
/du `<duration>`	Specifies a maximum length of time for a minute or hourly schedule in <HHHH:MM> 24-hour format. After the specified time elapses, schtasks does not start the task again until the start time recurs. By default, task schedules have no maximum duration. This parameter is optional and valid only with a MINUTE or HOURLY schedule.
/k	Stops the program that the task runs at the time specified by **/et** or **/du**. Without **/k**, schtasks doesn't start the program again after it reaches the time specified by **/et** or **/du** nor does it stop the program if it's still running. This parameter is optional and valid only with a MINUTE or HOURLY schedule.
/sd `<Startdate>`	Specifies the date on which the task schedule starts. The default value is the current date on the local computer. The format for **Startdate** varies with the locale selected for the local computer in **Regional and Language Options**. Only one format is valid for each locale. The valid date formats include (be sure to choose the format most similar to the format selected for **Short date** in **Regional and Language Options** on the local computer): • `<MM>//` - Specifies to use month-first formats, such as English (United States) and Spanish (Panama). • `<DD>//` - Specifies to use day-first formats, such as Bulgarian and Dutch (Netherlands). • `<YYYY>//` - Specifies to use for year-first formats, such as Swedish and French (Canada).
/ed `<Enddate>`	Specifies the date on which the schedule ends. This parameter is optional. It isn't valid in a ONCE, ONSTART, ONLOGON, ONIDLE, or ONEVENT schedule. By default, schedules have no ending date. The default value is

Parameter	Description
	the current date on the local computer. The format for **Enddate** varies with the locale selected for the local computer in **Regional and Language Options**. Only one format is valid for each locale. The valid date formats include (be sure to choose the format most similar to the format selected for **Short date** in **Regional and Language Options** on the local computer): • `<MM>//` - Specifies to use month-first formats, such as English (United States) and Spanish (Panama). • `<DD>//` - Specifies to use day-first formats, such as Bulgarian and Dutch (Netherlands). • `<YYYY>//` - Specifies to use for year-first formats, such as Swedish and French (Canada).
/ec `<channelname>`	Specifies the event channel name triggered by the ONEVENT schedule type that matches a system event log criteria.
/it	Specifies to run the scheduled task only when the run as user (the user account under which the task runs) is logged on to the computer. This parameter has no effect on tasks that run with system permissions or tasks that already have the interactive-only property set. You can't use a change command to remove the interactive-only property from a task. By default, run as user is the current user of the local computer when the task is scheduled or the account specified by the **/u** parameter, if one is used. However, if the command includes the **/ru** parameter, then the run as user is the account specified by the **/ru** parameter.
/np	No password is stored. The task runs non-interactively as the given user. Only local resources are available.
/z	Specifies to delete the task upon the completion of its schedule.
/xml `<xmlfile>`	Creates a task specified in the XML file. Can be combined with the **/ru** and **/rp** parameters, or with the **/rp** parameter by itself if the XML file already contains the user account information.
/v1	Creates a task visible to pre-Vista operating systems. This is not compatible with the **/XML** parameter.
/f	Specifies to create the task and suppress warnings if the specified task already exists.
/rl `<level>`	Specifies the Run Level for the job. Acceptable values are **LIMITED** (scheduled tasks will be ran with the least level of privileges, such as Standard User accounts) and **HIGHEST** (scheduled tasks will be ran with the highest level of privileges, such as Superuser accounts). The default value is **Limited**.
/delay `<delaytime>`	Specifies the wait time to delay running the task after it's triggered in mmmm:ss format. This is only valid for the ONSTART, ONLOGON, and

Parameter	Description
	ONEVENT schedule types.
/hresult	Specifies the process exit code to be in HRESULT format.
/?	Displays help at the command prompt.

To schedule a task to run every `<n>` minutes

In a minute schedule, the **/sc minute** parameter is required. The **/mo** (modifier) parameter is optional and specifies the number of minutes between each run of the task. The default value for **/mo** is *1* (every minute). The **/et** (end time) and **/du** (duration) parameters are optional and can be used with or without the **/k** (end task) parameter.

Examples

- To schedule a security script, *Sec.vbs*, to run every 20 minutes, type:

  ```
  schtasks /create /sc minute /mo 20 /tn "Security Script" /tr
  \\central\data\scripts\sec.vbs
  ```

  Because this example doesn't include a starting date or time, the task starts 20 minutes after the command completes, and runs every 20 minutes thereafter whenever the system is running. Notice that the security script source file is located on a remote computer, but that the task is scheduled and executes on the local computer.

- To schedule a security script, *Sec.vbs*, to run on the local computer every 100 minutes between 5:00 P.M. and 7:59 A.M. each day, type:

  ```
  schtasks /create /tn "Security Script" /tr sec.vbs /sc minute /mo 100
  /st 17:00 /et 08:00 /k
  ```

  This example uses the **/sc** parameter to specify a minute schedule and the **/mo** parameter to specify an interval of 100 minutes. It uses the **/st** and **/et** parameters to specify the start time and end time of each day's schedule. It also uses the **/k** parameter to stop the script if it's still running at 7:59 A.M. Without **/k**, schtasks

wouldn't start the script after 7:59 A.M., but if the instance started at 6:20 A.M. was still running, it wouldn't stop it.

To schedule a task to run every `<n>` hours

In an hourly schedule, the **/sc hourly** parameter is required. The **/mo** (modifier) parameter is optional and specifies the number of hours between each run of the task. The default value for **/mo** is *1* (every hour). The **/k** (end task) parameter is optional and can be used with either **/et** (end at the specified time) or **/du** (end after the specified interval).

Examples

- To schedule the MyApp program to run every five hours, beginning on the first day of March 2002, type:

  ```
  schtasks /create /sc hourly /mo 5 /sd 03/01/2002 /tn MyApp /tr
  c:\apps\myapp.exe
  ```

  In this example, the local computer uses the **English (Zimbabwe)** option in **Regional and Language Options**, so the format for the start date is MM/DD/YYYY (03/01/2002).

- To schedule the MyApp program to run hourly, beginning at five minutes past midnight, type:

  ```
  schtasks /create /sc hourly /st 00:05 /tn MyApp /tr c:\apps\myapp.exe
  ```

- To schedule the MyApp program to run every 3 hours, for 10 hours total, type:

  ```
  schtasks /create /tn MyApp /tr MyApp.exe /sc hourly /mo 3 /st 00:00 /du
  0010:00
  ```

  In this example, the task runs at 12:00 A.M., 3:00 A.M., 6:00 A.M., and 9:00 A.M. Because the duration is 10 hours, the task isn't run again at 12:00 P.M. Instead, it starts again at 12:00 A.M. the next day. Also, because the program runs for just a

few minutes, the **/k** parameter, which stops the program if it's still running when the duration expires, isn't necessary.

To schedule a task to run every `<n>` days

In a daily schedule, the **/sc daily** parameter is required. The **/mo** (modifier) parameter is optional and specifies the number of days between each run of the task. The default value for **/mo** is *1* (every day).

Examples

- To schedule the MyApp program to run once a day, every day, at 8:00 A.M. until December 31, 2021, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc daily /st 08:00
  /ed 31/12/2021
  ```

  In this example, the local computer system is set to the **English (United Kingdom)** option in **Regional and Language Options**, so the format for the end date is DD/MM/YYYY (31/12/2021). Additionally, because this example doesn't include the **/mo** parameter, the default interval of *1* is used to run the command every day.

- To schedule the MyApp program to run every twelve days at 1:00 P.M. (13:00) beginning on December 31, 2021, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc daily /mo 12 /sd
  12/31/2002 /st 13:00
  ```

  In this example, the system is set to the **English (Zimbabwe)** option in **Regional and Language Options**, so the format for the end date is MM/DD/YYYY (12/31/2021).

- To schedule a security script, *Sec.vbs*, to run every 70 days, type:

  ```
  schtasks /create /tn "Security Script" /tr sec.vbs /sc daily /mo 70 /it
  ```

In this example, the **/it** parameter is used to specify that the task runs only when the user under whose account the task runs is logged onto the computer. Because the task runs with the permissions of a specific user account, this task only runs when that user is logged on.

> ⓘ **Note**
>
> To identify tasks with the interactive-only (**/it**) property, use a verbose query (**/query /v**). In a verbose query display of a task with /it, the **Logon Mode** field has a value of Interactive only.

To schedule a task to run every `<n>` weeks

In a weekly schedule, the **/sc weekly** parameter is required. The **/mo** (modifier) parameter is optional and specifies the number of weeks between each run of the task. The default value for **/mo** is *1* (every week).

Weekly schedules also have an optional **/d** parameter to schedule the task to run on specified days of the week, or on all days (). The default is *MON (Monday)*. The every day () option is equivalent to scheduling a daily task.

Examples

- To schedule the MyApp program to run on a remote computer every six weeks, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc weekly /mo 6 /s
  Server16 /u Admin01
  ```

  Because this example leaves out the **/d** parameter, the task runs on Mondays. This example also uses the **/s** parameter to specify the remote computer and the **/u** parameter to run the command with the permissions of the user's Administrator account. Additionally, because the **/p** parameter is left out, SchTasks.exe prompts the user for the Administrator account password, and because the command is run remotely, all paths in the command, including the path to MyApp.exe, refer to paths on the remote computer.

- To schedule a task to run every other Friday, type:

```
schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc weekly /mo 2 /d
FRI
```

This example uses the **/mo** parameter to specify the two-week interval and the **/d** parameter to specify the day of the week. To schedule a task that runs every Friday, leave out the **/mo** parameter or set it to *1*.

To schedule a task to run every `<n>` months

In this schedule type, the **/sc monthly** parameter is required. The **/mo** (modifier) parameter, which specifies the number of months between each run of the task, is optional and the default is *1* (every month). This schedule type also has an optional **/d** parameter to schedule the task to run on a specified date of the month. The default is *1* (the first day of the month).

Examples

- To schedule the MyApp program to run on the first day of every month, type:

  ```
  schtasks /create /tn MyApp /tr myapp.exe /sc monthly
  ```

  The default value for both the **/mo** (modifier) parameter and the **/d** (day) parameter is *1*, so you don't need to use either of those parameters for this example.

- To schedule the MyApp program to run every three months, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly /mo 3
  ```

  This example uses the **/mo** parameter to specify an interval of 3 months.

- To schedule the MyApp program to run every other month on the 21st day of the month at midnight for a year, from July 2, 2002 to June 30, 2003, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly /mo 2 /d
  ```

```
21 /st 00:00 /sd 2002/07/01 /ed 2003/06/30
```

This example uses the **/mo** parameter to specify the monthly interval (every two months), the **/d** parameter to specify the date, the **/st** parameter to specify the time, and the **/sd** and **/ed** parameters to specify the start date and end date, respectively. Also in this example, the local computer is set to the **English (South Africa)** option in **Regional and Language Options**, so the dates are specified in the local format, YYYY/MM/DD.

To schedule a task to run on a specific day of the week

The day of the week schedule is a variation of the weekly schedule. In a weekly schedule, the **/sc weekly** parameter is required. The **/mo** (modifier) parameter is optional and specifies the number of weeks between each run of the task. The default value for **/mo** is *1* (every week). The **/d** parameter, which is optional, schedules the task to run on specified days of the week, or on all days (*). The default is *MON (Monday)*. The every day option `(/d *)` is equivalent to scheduling a daily task.

Examples

- To schedule the MyApp program to run every week on Wednesday, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc weekly /d WED
  ```

  This example uses the **/d** parameter to specify the day of the week. Because the command leaves out the **/mo** parameter, the task runs every week.

- To schedule a task to run on Monday and Friday of every eighth week, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc weekly /mo 8 /d
  MON,FRI
  ```

  This example uses the **/d** parameter to specify the days and the **/mo** parameter to specify the eight-week interval.

To schedule a task to run on a specific week of the month

In this schedule type, the **/sc monthly** parameter, the **/mo** (modifier) parameter, and the **/d** (day) parameter are required. The **/mo** (modifier) parameter specifies the week on which the task runs. The **/d** parameter specifies the day of the week. You can specify only one day of the week for this schedule type. This schedule also has an optional **/m** (month) parameter that lets you schedule the task for particular months or every month (*). The default for the **/m** parameter is every month (*).

Examples

- To schedule the MyApp program to run on the second Sunday of every month, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly /mo SECOND
  /d SUN
  ```

  This example uses the **/mo** parameter to specify the second week of the month and the **/d** parameter to specify the day.

- To schedule the MyApp program to run on the first Monday in March and September, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly /mo FIRST
  /d MON /m MAR,SEP
  ```

  This example uses the **/mo** parameter to specify the first week of the month and the **/d** parameter to specify the day. It uses the **/m** parameter to specify the month, separating the month arguments with a comma.

To schedule a task to run on a specific day each month

In this schedule type, the **/sc monthly** parameter and the **/d** (day) parameter are required. The **/d** parameter specifies a date of the month (1 - 31), not a day of the week, and you can specify only one day in the schedule. The **/m** (month) parameter is optional,

with the default being every month *()*, while the **/mo** (modifier) parameter isn't valid with this schedule type.

Schtasks.exe won't let you schedule a task for a date that's not in a month specified by the **/m** parameter. For example, trying to schedule the 31st day of February. However, if you don't use the **/m** parameter, and schedule a task for a date that doesn't appear in every month, then the task won't run in the shorter months. To schedule a task for the last day of the month, use the last day schedule type.

Examples

- To schedule the MyApp program to run on the first day of every month, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly
  ```

  Because the default modifier is *none* (no modifier), this command uses the default day of *1*, and the default month of *every month*, without requiring any additional parameters.

- To schedule the MyApp program to run on May 15 and June 15 at 3:00 P.M. (15:00), type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly /d 15 /m
  MAY,JUN /st 15:00
  ```

  This example uses the **/d** parameter to specify the date and the **/m** parameter to specify the months. It also uses the **/st** parameter to specify the start time.

To schedule a task to run on the last day of a month

In the last day schedule type, the **/sc monthly** parameter, the **/mo LASTDAY** (modifier) parameter, and the **/m** (month) parameter are required. The **/d** (day) parameter isn't valid.

Examples

- To schedule the MyApp program to run on the last day of every month, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly /mo
  lastday /m *
  ```

  This example uses the **/mo** parameter to specify the last day and the **/m** parameter with the wildcard character (*) to indicate that the program runs every month.

- To schedule the MyApp program to run on the last day of February and the last day of March at 6:00 P.M., type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly /mo
  lastday /m FEB,MAR /st 18:00
  ```

  This example uses the **/mo** parameter to specify the last day, the **/m** parameter to specify the months, and the **/st** parameter to specify the start time.

To schedule to run once

In the run-once schedule type, the **/sc once** parameter is required. The **/st** parameter, which specifies the time that the task runs, is required. The **/sd** parameter, which specifies the date that the task runs, is optional, while the **/mo** (modifier) and **/ed** (end date) parameters aren't valid.

Schtasks won't let you schedule a task to run once if the date and time specified are in the past, based on the time of the local computer. To schedule a task that runs once on a remote computer in a different time zone, you must schedule it before that date and time occurs on the local computer.

Example

- To schedule the MyApp program to run at midnight on January 1, 2003, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc once /sd
  01/01/2003 /st 00:00
  ```

This example uses the **/sc** parameter to specify the schedule type and the **/sd** and **/st** parameters to specify the date and time. Also in this example, the local computer uses the **English (United States)** option in **Regional and Language Options**, the format for the start date is MM/DD/YYYY.

To schedule a task to run every time the system starts

In the on-start schedule type, the **/sc onstart** parameter is required. The **/sd** (start date) parameter is optional and the default is the current date.

Example

- To schedule the MyApp program to run every time the system starts, type:

```
schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc onstart
```

In this example, the local computer uses the **English (United States)** option in **Regional and Language Options**, the format for the start date is MM/DD/YYYY.

To schedule a task to run when a user logs on

The on logon schedule type schedules a task that runs whenever any user logs on to the computer. In the on logon schedule type, the **/sc onlogon** parameter is required. The **/sd** (start date) parameter is optional and the default is the current date.

Example

- To schedule a task that runs when a user logs on to a remote computer, type:

```
schtasks /create /tn "Start Web Site" /tr c:\myiis\webstart.bat /sc
onlogon /s Server23
```

This example schedules a batch file to run every time a user (any user) logs on to the remote computer. It uses the **/s** parameter to specify the remote computer.

Because the command is remote, all paths in the command, including the path to the batch file, refer to a path on the remote computer.

To schedule a task to run when the system is idle

The on idle schedule type schedules a task that runs whenever there is no user activity during the time specified by the **/i** parameter. In the on idle schedule type, the **/sc onidle** parameter and the **/i** parameter are required. The **/sd** (start date) is optional and the default is the current date.

Example

- To schedule the MyApp program to run whenever the computer is idle, type:

```
schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc onidle /i 10
```

This example uses the required **/i** parameter to specify that the computer must remain idle for ten minutes before the task starts.

To schedule a task to run now

Schtasks doesn't have a Run Now option, but you can simulate that option by creating a task that runs once and starts in a few minutes.

Example

- To schedule a task to run once, on November 13, 2020 at 2:18 P.M. local time, type:

```
schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc once /st 14:18 /sd
11/13/2002
```

In this example, the local computer uses the **English (United States)** option in **Regional and Language Options**, so the format for the start date is MM/DD/YYYY.

To schedule a task that runs with different permissions

You can schedule tasks of all types to run with permissions of an alternate account on both the local and a remote computer. In addition to the parameters required for the particular schedule type, the **/ru** parameter is required and the **/rp** parameter is optional.

Examples

- To run the MyApp program on the local computer, type:

  ```
  schtasks /create /tn MyApp /tr myapp.exe /sc weekly /d TUE /ru Admin06
  ```

  This example uses the **/ru** parameter to specify that the task should run with the permissions of the user's Administrator account (*Admin06*). Also in this example, the task is scheduled to run every Tuesday, but you can use any schedule type for a task run with alternate permissions.

  In response, SchTasks.exe prompts for the run as password for the *Admin06* account, and then displays a success message:

  ```
  Please enter the run as password for Admin06: ********
  SUCCESS: The scheduled task MyApp has successfully been created.
  ```

- To run the MyApp program on the *Marketing* computer every four days, type:

  ```
  schtasks /create /tn MyApp /tr myapp.exe /sc daily /mo 4 /s Marketing
  /u Marketing\Admin01 /ru Reskits\User01
  ```

  This example uses the **/sc** parameter to specify a daily schedule, and the **/mo** parameter to specify an interval of four days. Additionally, this example uses the **/s** parameter to provide the name of the remote computer and the **/u** parameter to specify an account with permission to schedule a task on the remote computer (*Admin01 on the Marketing computer*). Finally, this example uses the **/ru** parameter to specify that the task should run with the permissions of the user's non-

Administrator account (*User01* in the *Reskits* domain). Without the **/ru** parameter, the task would run with the permissions of the account specified by **/u**.

When running this example, Schtasks first requests the password of the user named by the **/u** parameter (to run the command) and then requests the password of the user named by the **/ru** parameter (to run the task). After authenticating the passwords, schtasks displays a message indicating that the task is scheduled:

```
Type the password for Marketing\Admin01:********
Please enter the run as password for Reskits\User01: ********
SUCCESS: The scheduled task MyApp has successfully been created.
```

- To run schedule the *AdminCheck.exe* program to run on the Public computer every Friday at 4:00 A.M.,, but only if the administrator of the computer is logged on, type:

```
schtasks /create /tn "Check Admin" /tr AdminCheck.exe /sc weekly /d FRI
/st 04:00 /s Public /u Domain3\Admin06 /ru Public\Admin01 /it
```

This example uses the **/sc** parameter to specify a weekly schedule, the **/d** parameter to specify the day, and the **/st** parameter to specify the start time. It also uses the **/s** parameter to provide the name of the remote computer, the **/u** parameter to specify an account with permission to schedule a task on the remote computer, the **/ru** parameter to configure the task to run with the permissions of the administrator of the Public computer (*Public\Admin01*), and the **/it** parameter to indicate that the task runs only when the *Public\Admin01* account is logged on.

> ⓘ **Note**
>
> To identify tasks with the interactive-only (**/it**) property, use a verbose query (`/query /v`). In a verbose query display of a task with **/it**, the **Logon Mode** field has a value of **Interactive only**.

To schedule a task that runs with system permissions

Tasks of all types can run with permissions of the **System** account on both the local and a remote computer. In addition to the parameters required for the particular schedule type, the **/ru system** (or **/ru**) parameter is required, while the **/rp** parameter isn't valid.

> **ⓘ Important**
>
> The **System** account doesn't have interactive logon rights. Users can't see or interact with programs or tasks run with system permissions. The **/ru** parameter determines the permissions under which the task runs, not the permissions used to schedule the task. Only Administrators can schedule tasks, regardless of the value of the **/ru** parameter.
>
> To identify tasks that run with system permissions, use a verbose query (`/query /v`). In a verbose query display of a system-run task, the **Run As User** field has a value of **NT AUTHORITY\SYSTEM** and the **Logon Mode** field has a value of **Background only**.

Examples

- To schedule the MyApp program to run on the local computer with permissions of the **System** account, type:

  ```
  schtasks /create /tn MyApp /tr c:\apps\myapp.exe /sc monthly /d 15 /ru
  System
  ```

  In this example, the task is scheduled to run on the fifteenth day of every month, but you can use any schedule type for a task run with system permissions. Additionally, this example uses the **/ru System** parameter to specify the system security context. Because system tasks don't use a password, the **/rp** parameter is left out.

  In response, SchTasks.exe displays an informational message and a success message, without prompting for a password:

  ```
  INFO: The task will be created under user name (NT AUTHORITY\SYSTEM).
  SUCCESS: The Scheduled task MyApp has successfully been created.
  ```

- To schedule the MyApp program to run on the *Finance01* computer every morning at 4:00 A.M., using system permissions, type:

```
schtasks /create /tn MyApp /tr myapp.exe /sc daily /st 04:00 /s
Finance01 /u Admin01 /ru System
```

This example uses the **/tn** parameter to name the task and the **/tr** parameter to specify the remote copy of the MyApp program, the **/sc** parameter to specify a daily schedule, but leaves out the **/mo** parameter because *1* (every day) is the default. This example also uses the **/st** parameter to specify the start time, which is also the time the task will run each day, the **/s** parameter to provide the name of the remote computer, the **/u** parameter to specify an account with permission to schedule a task on the remote computer, and the **/ru** parameter to specify that the task should run under the System account. Without the **/ru** parameter, the task would run using the permissions of the account specified by the **/u** parameter.

Schtasks.exe requests the password of the user named by the **/u** parameter and, after authenticating the password, displays a message indicating that the task is created and that it will run with permissions of the **System** account:

```
Type the password for Admin01:**********

INFO: The Schedule Task MyApp will be created under user name (NT
AUTHORITY\
SYSTEM).
SUCCESS: The scheduled task MyApp has successfully been created.
```

To schedule a task that runs more than one program

Each task runs only one program. However, you can create a batch file that runs multiple programs and then schedule a task to run the batch file.

1. Using a text editor, such as Notepad, create a batch file that includes the name and fully qualified path to the .exe file required to start the Event Viewer (Eventvwr.exe) and System Monitor (Perfmon.exe) programs.

```
C:\Windows\System32\Eventvwr.exe
C:\Windows\System32\Perfmon.exe
```

2. Save the file as *MyApps.bat*, open schtasks.exe, and then create a task to run *MyApps.bat* by typing:

```
schtasks /create /tn Monitor /tr C:\MyApps.bat /sc onlogon /ru
Reskit\Administrator
```

   This command creates the Monitor task, which runs whenever anyone logs on. It uses the **/tn** parameter to name the task, the **/tr** parameter to run MyApps.bat, the **/sc** parameter to indicate the OnLogon schedule type and the **/ru** parameter to run the task with the permissions of the user's Administrator account.

   As a result of this command, whenever a user logs on to the computer, the task starts both Event Viewer and System Monitor.

To schedule a task that runs on a remote computer

To schedule a task to run on a remote computer, you must add the task to the remote computer's schedule. Tasks of all types can be scheduled on a remote computer, but the following conditions must be met:

- You must have permission to schedule the task. As such, you must be logged on to the local computer with an account that is a member of the Administrators group on the remote computer, or you must use the **/u** parameter to provide the credentials of an Administrator of the remote computer.

- You can use the **/u** parameter only when the local and remote computers are in the same domain or the local computer is in a domain that the remote computer domain trusts. Otherwise, the remote computer cannot authenticate the user account specified and it cannot verify that the account is a member of the Administrators group.

- The task must have sufficient permission to run on the remote computer. The permissions required vary with the task. By default, the task runs with the permission of the current user of the local computer or, if the **/u** parameter is used, the task runs with the permission of the account specified by the **/u** parameter.

However, you can use the **/ru** parameter to run the task with permissions of a different user account or with system permissions.

Examples

- To schedule the MyApp program (as an administrator) to run on the *SRV01* remote computer every ten days starting immediately,type:

```
schtasks /create /s SRV01 /tn MyApp /tr c:\program
files\corpapps\myapp.exe /sc daily /mo 10
```

This example uses the **/s** parameter to provide the name of the remote computer. Because the local current user is an Administrator of the remote computer, the **/u** parameter, which provides alternate permissions for scheduling the task, isn't necessary.

> ⓘ **Note**
>
> When scheduling tasks on a remote computer, all parameters refer to the remote computer. Therefore, the file specified by the **/tr** parameter refers to the copy of MyApp.exe on the remote computer.

- To schedule the MyApp program (as a user) to run on the *SRV06* remote computer every three hours, type:

```
schtasks /create /s SRV06 /tn MyApp /tr c:\program
files\corpapps\myapp.exe /sc hourly /mo 3 /u reskits\admin01 /p
R43253@4$ /ru SRV06\user03 /rp MyFav!!Pswd
```

Because Administrator permissions are required to schedule a task, the command uses the **/u** and **/p** parameters to provide the credentials of the user's Administrator account (*Admin01* in the *Reskits* domain). By default, these permissions are also used to run the task. However, because the task does not need Administrator permissions to run, the command includes the **/u** and **/rp** parameters to override the default and run the task with permission of the user's non-Administrator account on the remote computer.

- To schedule the MyApp program (as a user) to run on the *SRV02* remote computer on the last day of every month.

```
schtasks /create /s SRV02 /tn MyApp /tr c:\program
files\corpapps\myapp.exe /sc monthly /mo LASTDAY /m * /u
reskits\admin01
```

Because the local current user (*user03*) isn't an Administrator of the remote computer, the command uses the **/u** parameter to provide the credentials of the user's Administrator account (*Admin01* in the *Reskits* domain). The Administrator account permissions will be used to schedule the task and to run the task.

Because the command did not include the **/p** (password) parameter, schtasks prompts for the password. Then it displays a success message and, in this case, a warning:

```
Type the password for reskits\admin01:********

SUCCESS: The scheduled task MyApp has successfully been created.
WARNING: The scheduled task MyApp has been created, but may not run
because the account information could not be set.
```

This warning indicates that the remote domain could not authenticate the account specified by the **/u** parameter. In this case, the remote domain could not authenticate the user account because the local computer isn't a member of a domain that the remote computer domain trusts. When this occurs, the task job appears in the list of scheduled tasks, but the task is actually empty and it won't run.

The following display from a verbose query exposes the problem with the task. In the display, note that the value of **Next Run Time** is **Never** and that the value of **Run As User** is **Could not be retrieved from the task scheduler database**.

Had this computer been a member of the same domain or a trusted domain, the task would have been successfully scheduled and would have run as specified.

```
HostName: SRV44
TaskName: MyApp
Next Run Time: Never
```

```
Status:
Logon mode: Interactive/Background
Last Run Time: Never
Last Result: 0
Creator: user03
Schedule: At 3:52 PM on day 31 of every month, start
starting 12/14/2001
Task To Run: c:\program files\corpapps\myapp.exe
Start In: myapp.exe
Comment: N/A
Scheduled Task State: Disabled
Scheduled Type: Monthly
Start Time: 3:52:00 PM
Start Date: 12/14/2001
End Date: N/A
Days: 31
Months: JAN,FEB,MAR,APR,MAY,JUN,JUL,AUG,SEP,OCT,NO
V,DEC
Run As User: Could not be retrieved from the task sched
uler database
Delete Task If Not Rescheduled: Enabled
Stop Task If Runs X Hours and X Mins: 72:0
Repeat: Every: Disabled
Repeat: Until: Time: Disabled
Repeat: Until: Duration: Disabled
Repeat: Stop If Still Running: Disabled
Idle Time: Disabled
Power Management: Disabled
```

Remarks

- To run the **/create** command with the permissions of a different user, use the **/u** parameter. The **/u** parameter is valid only for scheduling tasks on remote computers.
- To view more `schtasks /create` examples, type `schtasks /create /?` at a command prompt.
- To schedule a task that runs with permissions of a different user, use the **/ru** parameter. The **/ru** parameter is valid for tasks on local and remote computers.
- To use the **/u** parameter, the local computer must be in the same domain as the remote computer or it must be in a domain that the remote computer domain trusts. Otherwise, either the task isn't created, or the task job is empty and the task doesn't run.
- Schtasks always prompts for a password unless you provide one, even when you schedule a task on the local computer using the current user account. This is

normal behavior for schtasks.

- Schtasks doesn't verify program file locations or user account passwords. If you don't enter the correct file location or the correct password for the user account, the task is created, but it won't run. Also, if the password for an account changes or expires, and you don't change the password saved in the task, then the task won't run.
- The **System** account doesn't have interactive logon rights. Users don't see and can't interact with programs run with system permissions.
- Each task runs only one program. However, you can create a batch file that starts multiple tasks, and then schedule a task that runs the batch file.
- You can test a task as soon as you create it. Use the run operation to test the task and then check the SchedLgU.txt file (SystemRoot\SchedLgU.txt) for errors.

Related links

- Command-Line Syntax Key
- schtasks change command
- schtasks delete command
- schtasks end command
- schtasks query command
- schtasks run command

schtasks delete

Article • 02/03/2023

Deletes a scheduled task from the schedule. This command doesn't delete the program that the task runs or interrupt a running program.

Syntax

```
schtasks /delete /tn {<taskname> | *} [/f] [/s <computer> [/u [<domain>\]
<user> [/p <password>]]]
```

Parameters

Parameter	Description
/tn `{<taskname> | *}`	Identifies the task to be deleted. If you use the `*`, this command deletes all tasks scheduled for the computer, not just the tasks scheduled by the current user.
/f	Suppresses the confirmation message. The task is deleted without warning.
/s `<computer>`	Specifies the name or IP address of a remote computer (with or without backslashes). The default is the local computer.
/u `[<domain>]`	Runs this command with the permissions of the specified user account. By default, the command runs with the permissions of the current user of the local computer. The specified user account must be a member of the Administrators group on the remote computer. The **/u** and **/p** parameters are valid only when you use **/s**.
/p `<password>`	Specifies the password of the user account specified in the **/u** parameter. If you use the **/u** parameter without the **/p** parameter or the password argument, schtasks will prompt you for a password. The **/u** and **/p** parameters are valid only when you use **/s**.
/?	Displays help at the command prompt.

Examples

To delete the *Start Mail* task from the schedule of a remote computer.

```
schtasks /delete /tn Start Mail /s Svr16
```

This command uses the **/s** parameter to identify the remote computer.

To delete all tasks from the schedule of the local computer, including tasks scheduled by other users.

```
schtasks /delete /tn * /f
```

This command uses the **/tn** * parameter to represent all tasks on the computer and the **/f** parameter to suppress the confirmation message.

Related links

- Command-Line Syntax Key
- schtasks change command
- schtasks create command
- schtasks end command
- schtasks query command
- schtasks run command

schtasks end

Article • 02/03/2023

Stops only the instances of a program started by a scheduled task. To stop other processes, you must use the TaskKill command.

Syntax

```
schtasks /end /tn <taskname> [/s <computer> [/u [<domain>\]<user> [/p <password>]]]
```

Parameters

Parameter	Description
/tn `<taskname>`	Identifies the task that started the program. This parameter is required.
/s `<computer>`	Specifies the name or IP address of a remote computer (with or without backslashes). The default is the local computer.
/u `[<domain>]`	Runs this command with the permissions of the specified user account. By default, the command runs with the permissions of the current user of the local computer. The specified user account must be a member of the Administrators group on the remote computer. The **/u** and **/p** parameters are valid only when you use **/s**.
/p `<password>`	Specifies the password of the user account specified in the **/u** parameter. If you use the **/u** parameter without the **/p** parameter or the password argument, schtasks will prompt you for a password. The **/u** and **/p** parameters are valid only when you use **/s**.
/?	Displays help at the command prompt.

Examples

To stop the instance of Notepad.exe started by the *My Notepad* task, type:

```
schtasks /end /tn "My Notepad"
```

To stop the instance of Internet Explorer started by the *InternetOn* task on the remote computer, *Svr01*,type:

```
schtasks /end /tn InternetOn /s Svr01
```

Related links

- Command-Line Syntax Key
- schtasks change command
- schtasks create command
- schtasks delete command
- schtasks query command
- schtasks run command

schtasks query

Article • 02/16/2024

Lists all the tasks scheduled to run on the computer.

Syntax

```
schtasks [/query] [/fo {TABLE | LIST | CSV}] [/nh] [/v] [/s <computer> [/u
[<domain>\]<user> [/p <password>]]] [/tn <taskname>] [/xml] [/hresult]
```

Parameters

Expand table

Parameter	Description
/query	Optionally, specifies the name of the operation. Using this query without any parameters performs a query of all tasks on the system.
/fo `<format>`	Specifies the output format. The valid values are *TABLE*, *LIST*, or *CSV*.
/nh	Removes column headings from the table display. This parameter is valid with the *TABLE* or *CSV* output formats.
/v	Adds the advanced properties of the task to the display. This parameter is valid with the *LIST* or *CSV* output formats.
/s `<computer>`	Specifies the name or IP address of a remote computer (with or without backslashes). The default is the local computer.
/u `[<domain>]`	Runs this command with the permissions of the specified user account. By default, the command runs with the permissions of the current user of the local computer. The specified user account must be a member of the Administrators group on the remote computer. The **/u** and **/p** parameters are valid only when you use **/s**.
/p `<password>`	Specifies the password of the user account specified in the **/u** parameter. If you use the **/u** parameter without the **/p** parameter or the password argument, schtasks will prompt you for a password. The **/u** and **/p** parameters are valid only when you use **/s**.
/tn `<taskname>`	Queries a specific task by path and name. If **/tn** is used, `<taskname>` cannot be blank. Assumes from root directory "\" folder by default (thus \ is omittable if the

Parameter	Description
	task is located in the root directory). Does not accept wildcards. Use quotation marks to enclose names that include spaces.
/xml	Outputs all task definitions on the system to XML format. If **/tn** is specified, outputs the specific task name to XML format. The full path and name must be used.
/hresult	Specifies the process exit code to be in HRESULT format.
/?	Displays help at the command prompt.

Examples

To list all tasks scheduled for the local computer, type:

```
schtasks
schtasks /query
```

These commands produce the same result and can be used interchangeably.

To request a detailed display of the tasks on the local computer,type:

```
schtasks /query /fo LIST /v
```

This command uses the **/v** parameter to request a detailed (verbose) display and the **/fo LIST** parameter to format the display as a list for easy reading. You can use this command to verify that a task you created has the intended recurrence pattern.

To request a list of tasks scheduled for a remote computer and to add the tasks to a comma-separated log file on the local computer, type:

```
schtasks /query /s Reskit16 /fo csv /nh >> \\svr01\data\tasklogs\p0102.csv
```

You can use this command format to collect and track tasks that are scheduled for multiple computers. This command uses the **/s** parameter to identify the remote computer, *Reskit16*, the **/fo** parameter to specify the format and the **/nh** parameter to suppress the column headings. The >> append symbol redirects the output to the task

log, *p0102.csv*, on the local computer, *Svr01*. Because the command runs on the remote computer, the local computer path must be fully qualified.

To get information for the *Office Subscription Maintenance* task using the **/tn** parameter, which can also be viewed via Task Scheduler in the location *Microsoft**Office*\ with the root directory "****" seen under the **Task Scheduler Library** folder, type:

```
schtasks /query /tn "\Microsoft\Office\Office Subscription Maintenance"
```

Related links

- Command-Line Syntax Key
- schtasks change command
- schtasks create command
- schtasks delete command
- schtasks end command
- schtasks run command

schtasks run

Article • 02/03/2023

Starts a scheduled task immediately. The run operation ignores the schedule, but uses the program file location, user account, and password saved in the task to run the task immediately. Running a task does not affect the task schedule and does not change the next run time scheduled for the task.

Syntax

```
schtasks /run /tn <taskname> [/s <computer> [/u [<domain>\]<user> [/p
<password>]]]
```

Parameters

Parameter	Description
/tn `<taskname>`	Identifies the task to start. This parameter is required.
/s `<computer>`	Specifies the name or IP address of a remote computer (with or without backslashes). The default is the local computer.
/u `[<domain>]`	Runs this command with the permissions of the specified user account. By default, the command runs with the permissions of the current user of the local computer. The specified user account must be a member of the Administrators group on the remote computer. The **/u** and **/p** parameters are valid only when you use **/s**.
/p `<password>`	Specifies the password of the user account specified in the **/u** parameter. If you use the **/u** parameter without the **/p** parameter or the password argument, schtasks will prompt you for a password. The **/u** and **/p** parameters are valid only when you use **/s**.
/?	Displays help at the command prompt.

Remarks

- Use this operation to test your tasks. If a task doesn't run, check the Task Scheduler Service transaction log, `<Systemroot>\SchedLgU.txt` for errors.

- To run a task remotely, the task must be scheduled on the remote computer. When you run the task, it runs only on the remote computer. To verify that a task is running on a remote computer, use Task Manager or the Task Scheduler Service transaction log, `<Systemroot>\SchedLgU.txt`.

Examples

To start the *Security Script* task, type:

```
schtasks /run /tn Security Script
```

To start the *Update* task on a remote computer, Svr01, type:

```
schtasks /run /tn Update /s Svr01
```

Related links

- Command-Line Syntax Key
- schtasks change command
- schtasks create command
- schtasks delete command
- schtasks end command
- schtasks query command

scwcmd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2 and Windows Server 2012

The Scwcmd.exe command-line tool included with the Security Configuration Wizard (SCW) can be used to perform the following tasks:

- Analyze one or many servers with an SCW-generated policy.
- Configure one or many servers with an SCW-generated policy.
- Register a Security Configuration Database extension with SCW.
- Rollback SCW policies.
- Transform an SCW-generated policy into native files that are supported by Group Policy.
- View analysis results in HTML format.

> **Note**
>
> If you use **scwcmd** to configure, analyze, or roll back a policy on a remote server, SCW must be installed on the remote server.

Syntax

```
scwcmd analyze
scwcmd configure
scwcmd register
scwcmd rollback
scwcmd transform
scwcmd view
```

Parameters

Parameter	Description

Parameter	Description
scwcmd analyze	Determines whether a computer is in compliance with a policy.
scwcmd configure	Applies an SCW-generated security policy to a computer.
scwcmd register	Extends or customizes the SCW Security Configuration Database by registering a Security Configuration Database file that contains role, task, service, or port definitions.
scwcmd rollback	Applies the most recent rollback policy available, and then deletes that rollback policy.
scwcmd transform	Transforms a security policy file generated by using SCW into a new Group Policy object (GPO) in Active Directory Domain Services.
scwcmd view	Renders an .xml file by using a specified .xsl transform.

Related links

- Command-Line Syntax Key

scwcmd analyze

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2 and Windows Server 2012

Determines whether a computer is in compliance with a policy. Results are returned in an .xml file.

This command also accepts a list of computer names as input. To view the results in your browser, use **scwcmd view** and specify `%windir%\security\msscw\TransformFiles\scwanalysis.xsl` as the .xsl transform.

Syntax

```
scwcmd analyze [[[/m:<computername> | /ou:<OuName>] /p:<policy>] | /i:
<computerlist>] [/o:<resultdir>] [/u:<username>] [/pw:<password>] [/t:
<threads>] [/l] [/e]
```

Parameters

Parameter	Description
/m:`<computername>`	Specifies the NetBIOS name, DNS name, or IP address of the computer to analyze. If the **/m** parameter is specified, then the **/p** parameter must also be specified.
/ou:`<OuName>`	Specifies the fully qualified domain name (FQDN) of an organizational unit (OU) in Active Directory Domain Services. If the **/ou** parameter is specified, then the **/p** parameter must also be specified. All computers in the OU will be analyzed against the given policy.
/p:`<policy>`	Specifies the path and file name of the .xml policy file to be used to perform the analysis.
/i:`<computerlist>`	Specifies the path and file name of an .xml file that contains a list of computers along with their expected policy files. All computers in the .xml file will be analyzed against their corresponding policy files. A sample .xml file is `%windir%\security\SampleMachineList.xml`.

Parameter	Description
/o:`<resultdir>`	Specifies the path and directory where the analysis result files should be saved. The default is the current directory.
/u:`<username>`	Specifies an alternate user credential to use when performing the analysis on a remote computer. The default is the logged on user.
/pw:`<password>`	Specifies an alternate user credential to use when performing the analysis on a remote computer. The default is the password of the logged on user.
/t:`<threads>`	Specifies the number of simultaneous outstanding analysis operations that should be maintained during the analysis. The value range is 1-1000, with a default value of 40.
/l	Causes the analysis process to be logged. One log file will be generated for each computer being analyzed. The log files will be stored in the same directory as the result files. Use the **/o** option to specify the directory for the result files.
/e	Log an event to the Application Event log if a mismatch is found.
/?	Displays help at the command prompt.

Examples

To analyze a security policy against the file *webpolicy.xml*, type:

```
scwcmd analyze /p:webpolicy.xml
```

To analyze a security policy on the computer named *webserver* against the file *webpolicy.xml* by using the credentials of the *webadmin* account, type:

```
scwcmd analyze /m:webserver /p:webpolicy.xml /u:webadmin
```

To analyze a security policy against the file *webpolicy.xml*, with a *maximum of 100 threads*, and output the results to a file named results in the *resultserver* share, type:

```
scwcmd analyze /i:webpolicy.xml /t:100 /o:\\resultserver\results
```

To analyze a security policy for the *WebServers OU* against the file *webpolicy.xml* by using the *DomainAdmin* credentials, type:

```
scwcmd analyze /ou:OU=WebServers,DC=Marketing,DC=ABCCompany,DC=com
/p:webpolicy.xml /u:DomainAdmin
```

Related links

- Command-Line Syntax Key
- scwcmd configure command
- scwcmd register command
- scwcmd rollback command
- scwcmd transform command
- scwcmd view command

scwcmd configure

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2 and Windows Server 2012

Applies a Security Configuration Wizard (SCW)-generated security policy to a computer. This command-line tool also accepts a list of computer names as input.

Syntax

```
scwcmd configure [[[/m:<computername> | /ou:<OuName>] /p:<policy>] | /i:
<computerlist>] [/u:<username>] [/pw:<password>] [/t:<threads>]
```

Parameters

Parameter	Description
/m:`<computername>`	Specifies the NetBIOS name, DNS name, or IP address of the computer to configure. If the **/m** parameter is specified, then the **/p** parameter must also be specified.
/ou:`<OuName>`	Specifies the fully qualified domain name (FQDN) of an organizational unit (OU) in Active Directory Domain Services. If the **/ou** parameter is specified, then the **/p** parameter must also be specified. All computers in the OU will be configured against the given policy.
/p:`<policy>`	Specifies the path and file name of the .xml policy file to be used to perform the configuration.
/i:`<computerlist>`	Specifies the path and file name of an .xml file that contains a list of computers along with their expected policy files. All computers in the .xml file will be analyzed against their corresponding policy files. A sample .xml file is `%windir%\security\SampleMachineList.xml`.
/u:`<username>`	Specifies an alternate user credential to use when performing the configuration on a remote computer. The default is the logged on user.
/pw:`<password>`	Specifies an alternate user credential to use when performing the configuration on a remote computer. The default is the password of the logged on user.

Parameter	Description
/t:`<threads>`	Specifies the number of simultaneous outstanding configuration operations that should be maintained during the analysis. The value range is 1-1000, with a default value of 40.
/l	Causes the analysis process to be logged. One log file will be generated for each computer being analyzed. The log files will be stored in the same directory as the result files. Use the **/o** option to specify the directory for the result files.
/e	Log an event to the Application Event log if a mismatch is found.
/?	Displays help at the command prompt.

Examples

To configure a security policy against the file *webpolicy.xml*, type:

```
scwcmd configure /p:webpolicy.xml
```

To configure a security policy for the computer at *172.16.0.0* against the file *webpolicy.xml* by using the credentials of the *webadmin* account, type:

```
scwcmd configure /m:172.16.0.0 /p:webpolicy.xml /u:webadmin
```

To configure a security policy on all computers on the list *campusmachines.xml* with a *maximum of 100 threads*, type:

```
scwcmd configure /i:campusmachines.xml /t:100
```

To configure a security policy for the *WebServers OU* against the file *webpolicy.xml* by using the *DomainAdmin* credentials, type:

```
scwcmd configure /ou:OU=WebServers,DC=Marketing,DC=ABCCompany,DC=com
/p:webpolicy.xml /u:DomainAdmin
```

Related links

- Command-Line Syntax Key
- scwcmd analyze command
- scwcmd register command
- scwcmd rollback command
- scwcmd transform command
- scwcmd view command

scwcmd register

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2 and Windows Server 2012

Extends or customizes the Security Configuration Wizard (SCW) Security Configuration Database by registering a Security Configuration Database file that contains role, task, service, or port definitions.

Syntax

```
scwcmd register /kbname:<MyApp> [/kbfile:<kb.xml>] [/kb:<path>] [/d]
```

Parameters

Parameter	Description
/kbname:`<MyApp>`	Specifies the name under which the Security Configuration Database extension will be registered. This parameter must be specified.
/kbfile:`<kb.xml>`	Specifies the path and file name of the Security Configuration Database file used to extend or customize the base Security Configuration Database. To validate that the Security Configuration Database file is compliant with the SCW schema, use the `%windir%\security\KBRegistrationInfo.xsd` schema definition file. This option must be provided unless the **/d** parameter is specified.
/kb:`<path>`	Specifies the path to the directory that contains the SCW Security Configuration Database files to be updated. If this option is not specified, `%windir%\security\msscw\kbs` is used.
/d	Unregisters a Security Configuration Database extension from the Security Configuration Database. The extension to unregister is specified by the **/kbname** parameter. (The **/kbfile** parameter shouldn't be specified.) The Security Configuration Database to unregister the extension from is specified by the **/kb** parameter.
/?	Displays help at the command prompt.

Examples

To register the Security Configuration Database file named *SCWKBForMyApp.xml* under the name *MyApp* in the location `\\kbserver\kb`, type:

```
scwcmd register /kbfile:d:\SCWKBForMyApp.xml /kbname:MyApp /kb:\\kbserver\kb
```

To unregister the Security Configuration Database *MyApp*, located at `\\kbserver\kb`, type:

```
scwcmd register /d /kbname:MyApp /kb:\\kbserver\kb
```

Related links

- Command-Line Syntax Key
- scwcmd analyze command
- scwcmd configure command
- scwcmd rollback command
- scwcmd transform command
- scwcmd view command

scwcmd rollback

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2 and Windows Server 2012

Applies the most recent rollback policy available, and then deletes that rollback policy.

Syntax

```
scwcmd rollback /m:<computername> [/u:<username>] [/pw:<password>]
```

Parameters

Parameter	Description
/m:`<computername>`	Specifies the NetBIOS name, DNS name, or IP address of a computer where the rollback operation should be performed.
/u:`<username>`	Specifies an alternate user account to use when performing a remote rollback. The default is the logged on user.
/pw:`<password>`	Specifies an alternate user credential to use when performing a remote rollback. The default is the logged on user.
/?	Displays help at the command prompt.

Examples

To roll back the security policy on a computer at IP address *172.16.0.0*, type:

```
scwcmd rollback /m:172.16.0.0
```

Related links

- Command-Line Syntax Key

- scwcmd analyze command
- scwcmd configure command
- scwcmd register command
- scwcmd transform command
- scwcmd view command

scwcmd transform

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2 and Windows Server 2012

Transforms a security policy file generated by using the Security Configuration Wizard (SCW) into a new Group Policy Object (GPO) in Active Directory Domain Services. The transform operation does not change any settings on the server where it is performed. After the transform operation has completed, an administrator must link the GPO to the desired OUs to deploy the policy to servers.

> **ⓘ Important**
>
> Domain administrator credentials are needed to complete the transform operation.
>
> Internet Information Services (IIS) security policy settings can't be deployed by using Group Policy.
>
> Firewall policies that list approved apps shouldn't be deployed to servers unless the Windows Firewall service started automatically when the server was last started.

Syntax

```
scwcmd transform /p:<policyfile.xml> /g:<GPOdisplayname>
```

Parameters

Parameter	Description
/p:`<policyfile.xml>`	Specifies the path and file name of the .xml policy file that should be applied. This parameter must be specified.
/g:`<GPOdisplayname>`	Specifies the display name of the GPO. This parameter must be specified.
/?	Displays help at the command prompt.

Examples

To create a GPO named *FileServerSecurity* from a file named *FileServerPolicy.xml*, type:

```
scwcmd transform /p:FileServerPolicy.xml /g:FileServerSecurity
```

Related links

- Command-Line Syntax Key
- scwcmd analyze command
- scwcmd configure command
- scwcmd register command
- scwcmd rollback command
- scwcmd view command

scwcmd view

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2012 R2 and Windows Server 2012

Renders an .xml file by using a specified .xsl transform. This command can be useful for displaying Security Configuration Wizard (SCW) .xml files by using different views.

Syntax

```
scwcmd view /x:<Xmlfile.xml> [/s:<Xslfile.xsl>]
```

Parameters

Parameter	Description
/x:`<Xmlfile.xml>`	Specifies the .xml file to be viewed. This parameter must be specified.
/s:`<Xslfile.xsl>`	Specifies the .xsl transform to apply to the .xml file as part of the rendering process. This parameter is optional for SCW .xml files. When the **view** command is used to render a SCW .xml file, it will automatically try to load the correct default transform for the specified .xml file. If an .xsl transform is specified, the transform must be written under the assumption that the .xml file is in the same directory as the .xsl transform.
/?	Displays help at the command prompt.

Example

To view *Policyfile.xml* by using the *Policyview.xsl* transform, type:

```
scwcmd view /x:C:\policies\Policyfile.xml /s:C:\viewers\Policyview.xsl
```

Related links

- Command-Line Syntax Key
- scwcmd analyze command
- scwcmd configure command
- scwcmd register command
- scwcmd rollback command
- scwcmd transform command

secedit commands

Article • 02/03/2023

Configures and analyzes system security by comparing your current security configuration against specified security templates.

> **Note**
>
> The Microsoft Management Console (MMC) and the Security Configuration and Analysis snap-in are not available on Server Core.

Syntax

```
secedit /analyze
secedit /configure
secedit /export
secedit /generaterollback
secedit /import
secedit /validate
```

Parameters

Parameter	Description
secedit /analyze	Allows you to analyze current systems settings against baseline settings that are stored in a database. The analysis results are stored in a separate area of the database and can be viewed in the Security Configuration and Analysis snap-in.
secedit /configure	Allows you to configure a system with security settings stored in a database.
secedit /export	Allows you to export security settings stored in a database.
secedit /generaterollback	Allows you to generate a rollback template with respect to a configuration template.
secedit /import	Allows you to import a security template into a database so that the settings specified in the template can be applied to a system or analyzed against a system.

Parameter	Description
secedit /validate	Allows you to validate the syntax of a security template.

Remarks

- If there is no filepath specified, all filenames will default to the current directory.
- Your analysis results are stored in a separate area of the database and can be viewed in the Security Configuration and Analysis snap-in to the MMC.
- If your security templates are created by using the Security Template snap-in, and if you run the Security Configuration and Analysis snap-in against those templates, the following files are created:

File	Description
scesrv.log	○ **Location:** `%windir%\security\logs` ○ **Created by:** Operating system ○ **File type:** Text ○ **Refresh rate:** Overwritten when `secedit analyze`, `secedit configure`, `secedit export` or `secedit import` is run. ○ **Content:** Contains the results of the analysis grouped by policy type.
user-selected name.sdb	○ **Location:** `%windir%\<user account>\Documents\Security\Database` ○ **Created by:** Running the Security Configuration and Analysis snap-in ○ **File type:** Proprietary ○ **Refresh rate:** Updated whenever a new security template is created. ○ **Content:** Local security policies and user-created security templates.
user-selected name.log	○ **Location:** User-defined, but defaults to `%windir%\<user account>\Documents\Security\Logs` ○ **Created by:** Running the `secedit analyze` or `secedit configure` commands, or by using the Security Configuration and Analysis snap-in. ○ **File type:** Text ○ **Refresh rate:** Overwritten when `secedit analyze` or `secedit configure` is run, or by using the Security Configuration and Analysis snap-in. ○ **Content:** Log file name, date and time, and the results of the analysis or investigation.
user-selected name.inf	○ **Location:** `%windir%\*<user account>\Documents\Security\Templates` ○ **Created by:** Running the Security Template snap-in. ○ **File type:** Text ○ **Refresh rate:** Overwritten each time the security template is updated. ○ **Content:** Contains the set up information for the template for each policy selected using the snap-in.

Related links

- Command-Line Syntax Key

secedit /analyze

Article • 02/03/2023

Allows you to analyze current systems settings against baseline settings that are stored in a database.

Syntax

```
secedit /analyze /db <database file name> [/cfg <configuration file name>]
[/overwrite] [/log <log file name>] [/quiet}]
```

Parameters

Parameter	Description
/db	Required. Specifies the path and file name of the database containing the stored configuration against which the analysis is performed. If the file name specifies a database that hasn't had a security template (as represented by the configuration file) associated with it, the `/cfg <configuration file name>` option must also be specified.
/cfg	Specifies the path and file name for the security template that will be imported into the database for analysis. This option is only valid when used with the `/db <database file name>` parameter. If this parameter isn't also specified, the analysis is performed against any configuration already stored in the database.
/overwrite	Specifies whether the security template in the **/cfg** parameter should overwrite any template or composite template that is stored in the database, instead of appending the results to the stored template. This option is only valid when the `/cfg <configuration file name>` parameter is also used. If this parameter isn't also specified, the template in the **/cfg** parameter is appended to the stored template.
/log	Specifies the path and file name of the log file to be used in the process. If you don't specify a file location, the default log file, `<systemroot>\Documents and Settings\<UserAccount>\My Documents\Security\Logs\<databasename>.log` is used.
/quiet	Suppresses screen output. You can still view analysis results by using the Security Configuration and Analysis snap-in to the Microsoft Management Console (MMC).

Examples

To perform the analysis for the security parameters on the security database, *SecDbContoso.sdb*, and then direct the output to the file *SecAnalysisContosoFY11*, including prompts to verify the command ran correctly, type:

```
secedit /analyze /db C:\Security\FY11\SecDbContoso.sdb /log
C:\Security\FY11\SecAnalysisContosoFY11.log
```

To incorporate changes required by the analysis process on the *SecContoso.inf* file, and then to direct the output to the existing file, *SecAnalysisContosoFY11*, without prompting, type:

```
secedit /analyze /db C:\Security\FY11\SecDbContoso.sdb /cfg SecContoso.inf
/overwrite /log C:\Security\FY11\SecAnalysisContosoFY11.xml /quiet
```

Related links

- Command-Line Syntax Key
- secedit /configure
- secedit /export
- secedit /generaterollback
- secedit /import
- secedit /validate

secedit /configure

Article • 02/03/2023

Allows you to configure the current system settings using security settings stored in a database.

Syntax

```
secedit /configure /db <database file name> [/cfg <configuration file name>]
[/overwrite] [/areas [securitypolicy | group_mgmt | user_rights | regkeys |
filestore | services]] [/log <log file name>] [/quiet]
```

Parameters

Parameter	Description
/db	Required. Specifies the path and file name of the database containing the stored configuration. If the file name specifies a database that hasn't had a security template (as represented by the configuration file) associated with it, the `/cfg <configuration file name>` option must also be specified.
/cfg	Specifies the path and file name for the security template that will be imported into the database for analysis. This option is only valid when used with the `/db <database file name>` parameter. If this parameter isn't also specified, the analysis is performed against any configuration already stored in the database.
/overwrite	Specifies whether the security template in the **/cfg** parameter should overwrite any template or composite template that is stored in the database, instead of appending the results to the stored template. This option is only valid when the `/cfg <configuration file name>` parameter is also used. If this parameter isn't also specified, the template in the **/cfg** parameter is appended to the stored template.

Parameter	Description
/areas	Specifies the security areas to be applied to the system. If this parameter is not specified, all security settings defined in the database are applied to the system. To configure multiple areas, separate each area by a space. The following security areas are supported: • **securitypolicy:** Local policy and domain policy for the system, including account policies, audit policies, security options, and so on. • **group_mgmt:** Restricted group settings for any groups specified in the security template. • **user_rights:** User logon rights and granting of privileges. • **regkeys:** Security on local registry keys. • **filestore:** Security on local file storage. • **services:** Security for all defined services.
/log	Specifies the path and file name of the log file to be used in the process. If you don't specify a file location, the default log file, `<systemroot>\Documents and Settings\<UserAccount>\My Documents\Security\Logs\<databasename>.log` is used.
/quiet	Suppresses screen and log output. You can still view analysis results by using the Security Configuration and Analysis snap-in to the Microsoft Management Console (MMC).

Examples

To perform the analysis for the security parameters on the security database, *SecDbContoso.sdb*, and then direct the output to the file *SecAnalysisContosoFY11*, including prompts to verify the command ran correctly, type:

```
secedit /analyze /db C:\Security\FY11\SecDbContoso.sdb /log
C:\Security\FY11\SecAnalysisContosoFY11.log
```

To incorporate changes required by the analysis process on the *SecContoso.inf* file, and then to direct the output to the existing file, *SecAnalysisContosoFY11*, without prompting, type:

```
secedit /configure /db C:\Security\FY11\SecDbContoso.sdb /cfg SecContoso.inf
/overwrite /log C:\Security\FY11\SecAnalysisContosoFY11.xml /quiet
```

Related links

- Command-Line Syntax Key
- secedit /analyze
- secedit /export
- secedit /generaterollback
- secedit /import
- secedit /validate

secedit /export

Article • 02/16/2024

Exports security settings stored in a database configured with security templates. You can use this command to backup your security policies on a local computer, in addition to importing the settings to another computer.

Syntax

```
secedit /export [/db <database file name>] [/mergedpolicy] /cfg
<configuration file name> [/areas [securitypolicy | group_mgmt | user_rights
| regkeys | filestore | services]] [/log <log file name>] [/quiet]
```

Parameters

Expand table

Parameter	Description
/db	Requires that you specify the path and file name of the database containing the stored configuration when exporting to a location other than the default. If not specified, the system security database will be stored in **%windir%\security\database**. If the file name specifies a database that hasn't had a security template (as represented by the configuration file) associated with it, the `/cfg <configuration file name>` option must also be specified for the export.
/mergedpolicy	Merges and exports domain and local policy security settings.
/cfg	Required. Specifies the path and file name for the security template that will be imported into the database for analysis. This option is only valid when used with the `/db <database file name>` parameter. If this parameter isn't also specified, the analysis is performed against any configuration already stored in the database.
/areas	Specifies the security areas to be applied to the system. If this parameter is not specified, all security settings defined in the database are applied to the system. To configure multiple areas, separate each area by a space. The following security areas are supported: • **securitypolicy:** Local policy and domain policy for the system, including account policies, audit policies, security options, and so on.

Parameter	Description
	• **group_mgmt:** Restricted group settings for any groups specified in the security template. • **user_rights:** User logon rights and granting of privileges. • **regkeys:** Security on local registry keys. • **filestore:** Security on local file storage. • **services:** Security for all defined services.
/log	Specifies the path and file name of the log file to be used in the process. If you don't specify a file location, the default log file, `<systemroot>\Documents and Settings\<UserAccount>\My Documents\Security\Logs\<databasename>.log` is used.
/quiet	Suppresses screen and log output. You can still view analysis results by using the Security Configuration and Analysis snap-in to the Microsoft Management Console (MMC).

Examples

To export the security database and the domain security policies to an inf file, and then import that file to a different database in order to replicate the security policy settings on another computer, type:

```
secedit /export /db C:\Security\FY11\SecDbContoso.sdb /mergedpolicy /cfg
SecContoso.inf /log C:\Security\FY11\SecAnalysisContosoFY11.log /quiet
```

To import your example file to a different database on another computer, type:

```
secedit /import /db C:\Security\FY12\SecDbContoso.sdb /cfg SecContoso.inf
/log C:\Security\FY11\SecAnalysisContosoFY12.log /quiet
```

Related links

- Command-Line Syntax Key
- secedit /analyze
- secedit /configure
- secedit /generaterollback

- secedit /import
- secedit /validate

secedit /generaterollback

Article • 02/03/2023

Allows you to generate a rollback template for a specified configuration template. If an existing rollback template exists, running this command again will overwrite the existing information.

Successfully running this command logs the mismatches between the specified security template the security policy configuration into the scesrv.log file.

Syntax

```
secedit /generaterollback /db <database file name> /cfg <configuration file name> /rbk <rollback template file name> [/log <log file name>] [/quiet]
```

Parameters

Parameter	Description
/db	Required. Specifies the path and file name of the database containing the stored configuration against which the analysis is performed. If the file name specifies a database that hasn't had a security template (as represented by the configuration file) associated with it, the `/cfg <configuration file name>` option must also be specified.
/cfg	Required. Specifies the path and file name for the security template that will be imported into the database for analysis. This option is only valid when used with the `/db <database file name>` parameter. If this parameter isn't also specified, the analysis is performed against any configuration already stored in the database.
/rbk	Required. Specifies a security template into which the rollback information is written. Security templates are created using the Security Templates snap-in. Rollback files can be created with this command.
/log	Specifies the path and file name of the log file to be used in the process. If you don't specify a file location, the default log file, `<systemroot>\Documents and Settings\<UserAccount>\My Documents\Security\Logs\<databasename>.log` is used.
/quiet	Suppresses screen and log output. You can still view analysis results by using the Security Configuration and Analysis snap-in to the Microsoft Management Console (MMC).

Examples

To create the rollback configuration file, for the previously created *SecTmplContoso.inf* file, while saving the original settings, and then write out the action to the *SecAnalysisContosoFY11* log file, type:

```
secedit /generaterollback /db C:\Security\FY11\SecDbContoso.sdb /cfg
sectmplcontoso.inf /rbk sectmplcontosoRBK.inf /log
C:\Security\FY11\SecAnalysisContosoFY11.log
```

Related links

- Command-Line Syntax Key
- secedit /analyze
- secedit /configure
- secedit /export
- secedit /import
- secedit /validate

secedit /import

Article • 02/03/2023

Imports security settings (.inf file), previously exported from the database configured with security templates.

> **Important**
>
> Before you import an .inf file to another computer, you must run the `secedit /generaterollback` command on the database on which the import will be performed.
>
> You must also run the `secedit /validate` command on the import file to verify its integrity.

Syntax

```
secedit /import /db <database file name> /cfg <configuration file name>
[/overwrite] [/areas [securitypolicy | group_mgmt | user_rights | regkeys |
filestore | services]] [/log <log file name>] [/quiet]
```

Parameters

Parameter	Description
/db	Required. Specifies the path and file name of the database containing the stored configuration against which the import is performed. If the file name specifies a database that hasn't had a security template (as represented by the configuration file) associated with it, the `/cfg <configuration file name>` option must also be specified.
/overwrite	Specifies whether the security template in the **/cfg** parameter should overwrite any template or composite template that is stored in the database, instead of appending the results to the stored template. This option is only valid when the `/cfg <configuration file name>` parameter is also used. If this parameter isn't also specified, the template in the **/cfg** parameter is appended to the stored template.

Parameter	Description
/cfg	Required. Specifies the path and file name for the security template that will be imported into the database for analysis. This option is only valid when used with the `/db <database file name>` parameter. If this parameter isn't also specified, the analysis is performed against any configuration already stored in the database.
/areas	Specifies the security areas to be applied to the system. If this parameter is not specified, all security settings defined in the database are applied to the system. To configure multiple areas, separate each area by a space. The following security areas are supported: • **securitypolicy:** Local policy and domain policy for the system, including account policies, audit policies, security options, and so on. • **group_mgmt:** Restricted group settings for any groups specified in the security template. • **user_rights:** User logon rights and granting of privileges. • **regkeys:** Security on local registry keys. • **filestore:** Security on local file storage. • **services:** Security for all defined services.
/log	Specifies the path and file name of the log file to be used in the process. If you don't specify a file location, the default log file, `<systemroot>\Documents and Settings\<UserAccount>\My Documents\Security\Logs\<databasename>.log` is used.
/quiet	Suppresses screen and log output. You can still view analysis results by using the Security Configuration and Analysis snap-in to the Microsoft Management Console (MMC).

Examples

To export the security database and the domain security policies to an .inf file, and then to import that file to a different database to replicate the policy settings on another computer, type:

```
secedit /export /db C:\Security\FY11\SecDbContoso.sdb /mergedpolicy /cfg
NetworkShare\Policies\SecContoso.inf /log
C:\Security\FY11\SecAnalysisContosoFY11.log /quiet
```

To import just the security policies portion of the file to a different database on another computer, type:

```
secedit /import /db C:\Security\FY12\SecDbContoso.sdb /cfg
NetworkShare\Policies\SecContoso.inf /areas securitypolicy /log
C:\Security\FY11\SecAnalysisContosoFY12.log /quiet
```

Related links

- Command-Line Syntax Key
- secedit /analyze
- secedit /configure
- secedit /export
- secedit /generaterollback
- secedit /validate

secedit /validate

Article • 02/03/2023

Validates the security settings stored in a security template (.inf file). Validating security templates can help you determine if one is corrupted or inappropriately set. Corrupted or inappropriately set security templates aren't applied.

Syntax

```
secedit /validate <configuration file name>
```

Parameters

Parameter	Description
`<configuration file name>`	Required. Specifies the path and file name for the security template that will be validated. Log files aren't updated by this command.

Examples

To verify that the rollback .inf file, *secRBKcontoso.inf*, is still valid after rollback, type:

```
secedit /validate secRBKcontoso.inf
```

Related links

- Command-Line Syntax Key
- secedit /analyze
- secedit /configure
- secedit /export
- secedit /generaterollback

- secedit /import

serverceipoptin

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Allows you to participate in the Customer Experience Improvement Program (CEIP).

Syntax

```
serverceipoptin [/query] [/enable] [/disable]
```

Parameters

Parameter	Description
/query	Verifies your current setting.
/enable	Turns on your participation in CEIP.
/disable	Turns off your participation in CEIP.
/?	Displays help at the command prompt.

Examples

To verify your current settings, type:

```
serverceipoptin /query
```

To turn on your participation, type:

```
serverceipoptin /enable
```

To turn off your participation, type:

```
serverceipoptin /disable
```

Related links

- Command-Line Syntax Key

servermanagercmd

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Installs and removes roles, role services, and features. Also displays the list of all roles, role services, and features available, and shows which are installed on this computer.

> **ⓘ Important**
>
> This command, servermanagercmd, has been deprecated and it's not guaranteed to be supported in future releases of Windows. We recommend instead that you use the Windows PowerShell cmdlets that are available for Server Manager. For more information, see **Install or Uninstall Roles, Role Services, or Features**.

Syntax

```
servermanagercmd -query [[[<drive>:]<path>]<query.xml>] [-logpath
[[<drive>:]<path>]<log.txt>]
servermanagercmd -inputpath  [[[<drive>:]<path>]<answer.xml>] [-resultpath
<result.xml> [-restart] | -whatif] [-logpath [[<drive>:]<path>]<log.txt>]
servermanagercmd -install <id> [-allSubFeatures] [-resultpath [[<drive>:]
<path>]<result.xml> [-restart] | -whatif] [-logpath [[<Drive>:]<path>]
<log.txt>]
servermanagercmd -remove <id> [-resultpath <result.xml> [-restart] | -
whatif] [-logpath  [[<drive>:]<path>]<log.txt>]
servermanagercmd [-help | -?]
servermanagercmd -version
```

Parameters

Parameter	Description
-query `[[[<drive>:]<path>]<query.xml>]`	Displays a list of all roles, role services, and features installed and available for installation on the server. You can also use the short form of this parameter, **-q**. If you want the query results saved to an XML file, specify an XML file to replace `<query.xml>`.

Parameter	Description
-inputpath `[[<drive>:]<path>]<answer.xml>]`	Installs or removes the roles, role services, and features specified in an XML answer file represented by `<answer.xml>`. You can also use the short form of this parameter, **-p**.
-install `<id>`	Installs the role, role service, or feature specified by `<id>`. The identifiers are case-insensitive. Multiple roles, role services, and features must be separated by spaces. The following optional parameters are used with the **-install** parameter: • **-setting** `<SettingName>=<SettingValue>` - Specifies required settings for the installation. • **-allSubFeatures** - Specifies the installation of all subordinate services and features along with the parent role, role service, or feature named in the `<id>` value. **NOTE** Some role containers do not have a command line identifier to allow installation of all role services. This is the case when role services cannot be installed in the same instance of the Server Manager command. For example, the Federation Service role service of active directory Federation Services and the Federation Service Proxy role service cannot be installed by using the same Server Manager command instance. • **-resultpath** `<result.xml>` - Saves installation results to an XML file represented by `<result.xml>`. You can also use the short form of this parameter, **-r**. **NOTE** You can't run servermanagercmd with both the **-resultpath** parameter and the **-whatif** parameter specified. • **-restart** - Restarts the computer automatically when installation is complete (if restarting is required by the roles or features installed). • **-whatif** - Displays any operations specified for the **-install** parameter. You can also use the short form of the **-whatif** parameter, **-w**. You can't run **servermanagercmd** with both the **-resultpath** parameter and the **-whatif** parameter specified. • **-logpath** `<[[<drive>:]<path>]<log.txt>>` - Specifies a name and location for the log file, other than the default, `%windir%\temp\servermanager.log`.

Parameter	Description
-remove `<id>`	Removes the role, role service, or feature specified by `<id>`. The identifiers are case-insensitive. Multiple roles, role services, and features must be separated by spaces. The following optional parameters are used with the **-remove** parameter: • **-resultpath** `<[[<drive>:]<path>]result.xml>` - Saves removal results to an XML file represented by `<result.xml>`. You can also use the short form of this parameter, **-r**. **NOTE** You can't run servermanagercmd with both the **-resultpath** and the **-whatif** parameters specified. • **-restart** - Restarts the computer automatically when removal is complete (if restarting is required by remaining roles or features). • **-whatif** - Displays any operations specified for the -remove parameter. You can also use the short form of the -whatif parameter, **-w**. You can't run servermanagercmd with both the **-resultpath** and the **-whatif** parameters specified. • **-logpath** `<[[<Drive>:]<path>]<log.txt>>` - Specifies a name and location for the log file, other than the default, `%windir%\temp\servermanager.log`.
-version	Displays the Server Manager version number. You can also use the short form, **-v**.
-help	Displays help in the Command prompt window. You can also use the short form, **-?**.

Examples

To display a list of all roles, role services, and features available, and which roles, role services, and features are installed on the computer, type:

```
servermanagercmd -query
```

To install the Web Server (IIS) role, and save the installation results to an XML file represented by *installResult.xml*, type:

```
servermanagercmd -install Web-Server -resultpath installResult.xml
```

To display detailed information about the roles, role services, and features that would be installed or removed, based upon instructions that are specified in an XML answer file

represented by *install.xml*, type:

```
servermanagercmd -inputpath install.xml -whatif
```

Related links

- Command-Line Syntax Key
- Server Manager overview

serverweroptin

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Allows you to turn on error reporting.

Syntax

```
serverweroptin [/query] [/detailed] [/summary]
```

Parameters

Parameter	Description
/query	Verifies your current setting.
/detailed	Specifies to send detailed reports automatically.
/summary	Specifies to send summary reports automatically.
/?	Displays help at the command prompt.

Examples

To verify the current setting, type:

```
serverweroptin /query
```

To automatically send detailed reports, type:

```
serverweroptin /detailed
```

To automatically send summary reports, type:

```
serverweroptin /summary
```

Related links

- Command-Line Syntax Key

Services for Network File System command-line tools

Article • 02/03/2023

Services for Network File System (NFS) provides a file sharing solution that lets you transfer files between computers running Windows Server and UNIX operating systems using the NFS protocol.

Information and links to each of the associated NFS command-line tools:

Command	Description
mapadmin	Manage User Name Mapping for Microsoft Services for Network File System.
mount	Mount Network File System (NFS) network shares.
nfsadmin	Manage Server for NFS and Client for NFS.
nfsshare	Control Network File System (NFS) shares.
nfsstat	Display or reset counts of calls made to Server for NFS.
rpcinfo	List programs on remote computers.
showmount	Display mounted directories.

Related links

- Command-Line Syntax Key

set (environment variable)

Article • 09/06/2023

Displays, sets, or removes cmd.exe environment variables. If used without parameters, **set** displays the current environment variable settings.

> **Note**
>
> This command requires command extensions, which are enabled by default.

The **set** command can also run from the Windows Recovery Console, using different parameters. For more information, see Windows Recovery Environment (WinRE).

Syntax

```
set [<variable>=[<string>]]
set [/p] <variable>=[<promptString>]
set /a <variable>=<expression>
```

Parameters

Parameter	Description
`<variable>`	Specifies the environment variable to set or modify.
`<string>`	Specifies the string to associate with the specified environment variable.
/p	Sets the value of `<variable>` to a line of input entered by the user.
`<promptstring>`	Specifies a message to prompt the user for input. This parameter must be used with the **/p** parameter.
/a	Sets `<string>` to a numerical expression that is evaluated.
`<expression>`	Specifies a numerical expression.
/?	Displays help at the command prompt.

Remarks

- If command extensions are enabled (the default) and you run **set** with a value, it displays all of the variables that begin with that value.
- The characters `<`, `>`, `|`, `&`, and `^` are special command shell characters, and they must be preceded by the escape character (`^`) or enclosed in quotation marks when used in `<string>` (for example, "StringContaining&Symbol"). If you use quotation marks to enclose a string that contains one of the special characters, the quotation marks are set as part of the environment variable value.
- Use environment variables to control the behavior of some batch files and programs and to control the way Windows and the MS-DOS subsystem appears and works. The **set** command is often used in the **Autoexec.nt** file to set environment variables.
- If you use the **set** command without any parameters, the current environment settings are displayed. These settings usually include the **COMSPEC** and **PATH** environment variables, which are used to help find programs on disk. Two other environment variables used by Windows are **PROMPT** and **DIRCMD**.
- If you specify values for `<variable>` and `<string>`, the specified `<variable>` value is added to the environment and `<string>` is associated with that variable. If the variable already exists in the environment, the new string value replaces the old string value.
- If you specify only a variable and an equal sign (without `<string>`) for the **set** command, the `<string>` value associated with the variable is cleared (as if the variable isn't there).
- If you use the **/a** parameter, the following operators are supported, in descending order of precedence:

Operator	Operation performed
`( )`	Grouping
`! ~ -`	Unary
`* / %`	Arithmetic
`+ -`	Arithmetic
`<< >>`	Logical shift
`&`	Bitwise AND
`^`	Bitwise exclusive OR

Operator	Operation performed
`= *= /= %= += -= &= ^= <<= >>=`	
`,`	Expression separator

- If you use logical (`&&` or `||`) or modulus (%) operators, enclose the expression string in quotation marks. Any non-numeric strings in the expression are considered environment variable names, and their values are converted to numbers before they're processed. If you specify an environment variable name that isn't defined in the current environment, a value of zero is allotted, which allows you to perform arithmetic with environment variable values without using the % to retrieve a value.
- If you run **set /a** from the command line outside of a command script, it displays the final value of the expression.
- Numeric values are decimal numbers unless prefixed by 0× for hexadecimal numbers or 0 for octal numbers. Therefore, 0×12 is the same as 18, which is the same as 022.
- Delayed environment variable expansion support is disabled by default, but you can enable or disable it by using **cmd /v**.
- When creating batch files, you can use **set** to create variables, and then use them in the same way that you would use the numbered variables **%0** through **%9**. You can also use the variables **%0** through **%9** as input for **set**.
- If you call a variable value from a batch file, enclose the value with percent signs (%). For example, if your batch program creates an environment variable named *BAUD*, you can use the string associated with *BAUD* as a replaceable parameter by typing **%baud%** at the command prompt.

Examples

To set the value *TEST^1* for the environment variable named `testVar`, type:

```
set testVar=TEST^^1
```

The **set** command assigns everything that follows the equal sign (=) to the value of the variable. Therefore, if you type `set testVar=TEST^1`, you'll get the following result, `testVar=TEST1`.

To set the value *TEST&1* for the environment variable `testVar`, type:

```
set testVar=TEST^&1
```

To set an environment variable named *include* so the string *c:\directory* is associated with it, type:

```
set include=c:\directory
```

You can then use the string *c:\directory* in batch files by enclosing the name *include* with percent signs (%). For example, you can use `dir %include%` in a batch file to display the contents of the directory associated with the *include* environment variable. After this command is processed, the string c:\directory replaces **%include%**.

To use the **set** command in a batch program to add a new directory to the *path* environment variable, type:

```
@echo off
rem ADDPATH.BAT adds a new directory
rem to the path environment variable.
set path=%1;%path%
set
```

To display a list of all of the environment variables that begin with the letter *p*, type:

```
set p
```

To display a list of all of the environment variables on the current device, type:

```
set
```

Related links

- Command-Line Syntax Key

setlocal

Article • 02/03/2023

Starts localization of environment variables in a batch file. Localization continues until a matching **endlocal** command is encountered or the end of the batch file is reached.

Syntax

```
setlocal [enableextensions | disableextensions] [enabledelayedexpansion |
disabledelayedexpansion]
```

Parameters

Expand table

Parameter	Description
enableextensions	Enables the command extensions until the matching **endlocal** command is encountered, regardless of the setting before the **setlocal** command was run.
disableextensions	Disables the command extensions until the matching **endlocal** command is encountered, regardless of the setting before the **setlocal** command was run.
enabledelayedexpansion	Enables the delayed environment variable expansion until the matching **endlocal** command is encountered, regardless of the setting before the **setlocal** command was run.
disabledelayedexpansion	Disables the delayed environment variable expansion until the matching **endlocal** command is encountered, regardless of the setting before the **setlocal** command was run.
/?	Displays help at the command prompt.

Remarks

- If you use **setlocal** outside of a script or batch file, it has no effect.
- Use **setlocal** to change environment variables when you run a batch file. Environment changes made after you run **setlocal** are local to the batch file. The

Cmd.exe program restores previous settings when it encounters an **endlocal** command or reaches the end of the batch file.

- You can have more than one **setlocal** or **endlocal** command in a batch program (that is, nested commands).
- The **setlocal** command sets the ERRORLEVEL variable. If you pass {**enableextensions** | **disableextensions**} or {**enabledelayedexpansion** | **disabledelayedexpansion**}, the ERRORLEVEL variable is set to **0** (zero). Otherwise, it's set to **1**. You can use this information in batch scripts to determine whether the extensions are available, as shown in the following example:

  ```
  verify other 2>nul
  setlocal enableextensions
  if errorlevel 1 echo Unable to enable extensions
  ```

  Because **cmd** does not set the ERRORLEVEL variable when command extensions are disabled, the **verify** command initializes the ERRORLEVEL variable to a nonzero value when you use it with an invalid argument. Also, if you use the **setlocal** command with arguments {**enableextensions** | **disableextensions**} or {**enabledelayedexpansion** | **disabledelayedexpansion**} and it does not set the ERRORLEVEL variable to **1**, command extensions are not available.

Examples

To localize environment variables in a batch file, follow this sample script:

```
rem *******Begin Comment**************
rem This program starts the superapp batch program on the network,
rem directs the output to a file, and displays the file
rem in Notepad.
rem *******End Comment**************
@echo off
setlocal
path=g:\programs\superapp;%path%
call superapp>c:\superapp.out
endlocal
start notepad c:\superapp.out
```

Related links

- Command-Line Syntax Key

Feedback

Was this page helpful? Yes No

setx

Article • 02/03/2023

Creates or modifies environment variables in the user or system environment, without requiring programming or scripting. The **Setx** command also retrieves the values of registry keys and writes them to text files.

> **Note**
>
> This command provides the only command-line or programmatic way to directly and permanently set system environment values. System environment variables are manually configurable through **Control Panel** or through a registry editor. The **set** command, which is internal to the command interpreter (Cmd.exe), sets user environment variables for the current console window only.

Syntax

```
setx [/s <computer> [/u [<domain>\]<user name> [/p [<password>]]]]
<variable> <value> [/m]
setx [/s <computer> [/u [<domain>\]<user name> [/p [<password>]]]]
<variable>] /k <path> [/m]
setx [/s <computer> [/u [<domain>\]<user name> [/p [<password>]]]] /f
<filename> {[<variable>] {/a <X>,<Y> | /r <X>,<Y> <String>} [/m] | /x} [/d
<delimiters>]
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer. Do not use backslashes. The default value is the name of the local computer.
/u `[<domain>\]` `<user name>`	Runs the script with the credentials of the specified user account. The default value is the system permissions.
/p `[<password>]`	Specifies the password of the user account that is specified in the **/u** parameter.
`<variable>`	Specifies the name of the environment variable that you want to set.

Parameter	Description
`<value>`	Specifies the value to which you want to set the environment variable.
/k `<path>`	Specifies that the variable is set based on information from a registry key. The *path* uses the following syntax: `\\<HIVE>\<KEY>\...\<Value>`. For example, you might specify the following path: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\StandardName`
/f `<filename>`	Specifies the file that you want to use.
/a `<X>,<Y>`	Specifies absolute coordinates and offset as search parameters.
/r `<X>,<Y>` `<String>`	Specifies relative coordinates and offset from **String** as search parameters.
/m	Specifies to set the variable in the system environment. The default setting is the local environment.
/x	Displays file coordinates, ignoring the **/a**, **/r**, and **/d** command-line options.
/d `<delimiters>`	Specifies delimiters such as **,** or **** to be used in addition to the four built-in delimiters — SPACE, TAB, ENTER, and LINEFEED. Valid delimiters include any ASCII character. The maximum number of delimiters is 15, including built-in delimiters.
/?	Displays help at the command prompt.

Remarks

- This command is similar to the UNIX utility SETENV.
- You can use this command to set values for user and system environment variables from one of three sources (modes): Command Line Mode, Registry Mode, or File Mode.
- This command writes variables to the master environment in the registry. Variables set with **setx** variables are available in future command windows only, not in the current command window.
- **HKEY_CURRENT_USER** and **HKEY_LOCAL_MACHINE** are the only supported hives. REG_DWORD, REG_EXPAND_SZ, REG_SZ, and REG_MULTI_SZ are the valid **RegKey** data types.
- If you gain access to **REG_MULTI_SZ** values in the registry, only the first item is extracted and used.

- You can't use this command to remove values added to the local or system environments. You can use this command with a variable name and no value to remove a corresponding value from the local environment.
- REG_DWORD registry values are extracted and used in hexadecimal mode.
- File mode supports the parsing of carriage return and line feed (CRLF) text files only.
- Running this command on an existing variable removes any variable references and uses expanded values.

  For instance, if the variable %PATH% has a reference to %JAVADIR%, and %PATH% is manipulated using **setx**, %JAVADIR% is expanded and its value is assigned directly to the target variable %PATH%. This means that future updates to %JAVADIR% **will not** be reflected in the %PATH% variable.
- Be aware there's a limit of 1024 characters when assigning contents to a variable using **setx**.

  This means that the content is cropped if you go over 1024 characters, and that the cropped text is what's applied to the target variable. If this cropped text is applied to an existing variable, it can result in loss of data previously held by the target variable.

Examples

To set the *MACHINE* environment variable in the local environment to the value *Brand1*, type:

```
setx MACHINE Brand1
```

To set the *MACHINE* environment variable in the system environment to the value *Brand1 Computer*, type:

```
setx MACHINE Brand1 Computer /m
```

To set the *MYPATH* environment variable in the local environment to use the search path defined in the *PATH* environment variable, type:

```
setx MYPATH %PATH%
```

To set the *MYPATH* environment variable in the local environment to use the search path defined in the *PATH* environment variable after replacing ~ with %, type:

```
setx MYPATH ~PATH~
```

To set the *MACHINE* environment variable in the local environment to *Brand1* on a remote computer named *computer1*, type:

```
setx /s computer1 /u maindom\hiropln /p p@ssW23 MACHINE Brand1
```

To set the *MYPATH* environment variable in the local environment to use the search path defined in the *PATH* environment variable on a remote computer named *computer1*, type:

```
setx /s computer1 /u maindom\hiropln /p p@ssW23 MYPATH %PATH%
```

To set the *TZONE* environment variable in the local environment to the value found in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\StandardName** registry key, type:

```
setx TZONE /k
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\Stan
dardName
```

To set the *TZONE* environment variable in the local environment of a remote computer named *computer1* to the value found in the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\StandardName** registry key, type:

```
```

```
setx /s computer1 /u maindom\hiropln /p p@ssW23 TZONE /k
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation\Stan
dardName
```

To set the *BUILD* environment variable in the system environment to the value found in the **HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\CurrentBuildNumber** registry key, type:

```
setx BUILD /k
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\CurrentBuildN
umber /m
```

To set the BUILD environment variable in the system environment of a remote computer named Computer1 to the value found in the **HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\CurrentBuildNumber** registry key, type:

```
setx /s computer1 /u maindom\hiropln /p p@ssW23  BUILD /k
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\CurrentBuildNumber /m
```

To display the contents of a file named *Ipconfig.out*, along with the contents' corresponding coordinates, type:

```
setx /f ipconfig.out /x
```

To set the *IPADDR* environment variable in the local environment to the value found at the coordinate *5,11* in the *Ipconfig.out* file, type:

```
setx IPADDR /f ipconfig.out /a 5,11
```

To set the *OCTET1* environment variable in the local environment to the value found at the coordinate *5,3* in the *Ipconfig.out* file with delimiters **#$*.**, type:

```
```

```
setx OCTET1 /f ipconfig.out /a 5,3 /d #$*.
```

To set the *IPGATEWAY* environment variable in the local environment to the value found at the coordinate *0,7* with respect to the coordinate of *Gateway* in the *Ipconfig.out* file, type:

```
setx IPGATEWAY /f ipconfig.out /r 0,7 Gateway
```

To display the contents of the *Ipconfig.out* file, along with the contents' corresponding coordinates, on a computer named *computer1*, type:

```
setx /s computer1 /u maindom\hiropln /p p@ssW23 /f ipconfig.out /x
```

Related links

- Command-Line Syntax Key

sfc

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Scans and verifies the integrity of all protected system files and replaces incorrect versions with correct versions. If this command discovers that a protected file has been overwritten, it retrieves the correct version of the file from the **systemroot** folder, and then replaces the incorrect file.

> **ⓘ Important**
>
> You must be logged on as a member of the Administrators group to run this command.

Syntax

```
sfc [/scannow] [/verifyonly] [/scanfile=<file>] [/verifyfile=<file>]
[/offwindir=<offline windows directory> /offbootdir=<offline boot directory>
/offlogfile=<log file path>]
```

Parameters

Parameter	Description
/scannow	Scans the integrity of all protected system files and repairs files with problems when possible.
/verifyonly	Scans the integrity of all protected system files, without performing repairs.
/scanfile `<file>`	Scans the integrity of the specified file (full path and filename) and attempts to repair any problems if they're detected.
/verifyfile `<file>`	Verifies the integrity of the specified file (full path and filename), without performing repairs.

Parameter	Description
/offwindir `<offline windows directory>`	Specifies the location of the offline windows directory, for offline repair.
/offbootdir `<offline boot directory>`	Specifies the location of the offline boot directory for offline repair.
/offlogfile=`<log file path>`	Specifies a location to store the log file other than the default.
/?	Displays help at the command prompt.

Examples

To verify the *kernel32.dll file*, type:

```
sfc /verifyfile=c:\windows\system32\kernel32.dll
```

To set up the offline repair of the *kernel32.dll* file with an offline boot directory set to **D:** and an offline windows directory set to **D:\Windows**, type:

```
sfc /scanfile=D:\windows\system32\kernel32.dll /offbootdir=D:\
/offwindir=d:\windows
```

Related links

- Command-Line Syntax Key

shadow

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables you to remotely control an active session of another user on a Remote Desktop Session Host server.

Syntax

```
shadow {<sessionname> | <sessionID>} [/server:<servername>] [/v]
```

Parameters

Parameter	Description
`<sessionname>`	Specifies the name of the session that you want to remotely control.
`<sessionID>`	Specifies the ID of the session that you want to remotely control. Use **query user** to display the list of sessions and their session IDs.
/server:`<servername>`	Specifies the Remote Desktop Session Host server containing the session that you want to remotely control. By default, the current Remote Desktop Session Host4 server is used.
/v	Displays information about the actions being performed.
/?	Displays help at the command prompt.

Remarks

- You can either view or actively control the session. If you choose to actively control a user's session, you will be able to input keyboard and mouse actions to the session.
- You can always remotely control your own sessions (except the current session), but you must have Full Control permission or remote Control special access permission to remotely control another session.

- You can also initiate remote control by using Remote Desktop Services Manager.
- Before monitoring begins, the server warns the user that the session is about to be remotely controlled, unless this warning is disabled. Your session might appear to be frozen for a few seconds while it waits for a response from the user. To configure remote control for users and sessions, use the Remote Desktop Services Configuration tool or the Remote Desktop Services extensions to Local Users and Groups and active directory Users and computers.
- Your session must be capable of supporting the video resolution used at the session that you are remotely controlling or the operation fails.
- The console session can neither remotely control another session nor can it be remotely controlled by another session.
- When you want to end remote control (shadowing), press CTRL+`*` (by using `*` from the numeric keypad only).

Examples

To shadow *session 93*, type:

```
shadow 93
```

To shadow the session *ACCTG01*, type:

```
shadow ACCTG01
```

Related links

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

shift

Article • 02/03/2023

Changes the position of batch parameters in a batch file.

Syntax

```
shift [/n <N>]
```

Parameters

Parameter	Description
/n `<N>`	Specifies to start shifting at the *N*th argument, where *N* is any value from *0* to *8*. Requires command extensions, which are enabled by default.
/?	Displays help at the command prompt.

Remarks

- The **shift** command changes the values of the batch parameters **%0** through **%9** by copying each parameter into the previous one—the value of **%1** is copied to **%0**, the value of **%2** is copied to **%1**, and so on. This is useful for writing a batch file that performs the same operation on any number of parameters.
- If command extensions are enabled, the **shift** command supports the **/n** command-line option. The **/n** option specifies to start shifting at the Nth argument, where **N** is any value from 0 to 8. For example, **SHIFT /2** would shift **%3** to **%2**, **%4** to **%3**, and so on, and leave **%0** and **%1** unaffected. Command extensions are enabled by default.
- You can use the **shift** command to create a batch file that can accept more than 10 batch parameters. If you specify more than 10 parameters on the command line, those that appear after the tenth (**%9**) will be shifted one at a time into **%9**.
- The **shift** command has no effect on the **%*** batch parameter.
- There's no backward **shift** command. After you implement the **shift** command, you can't recover the batch parameter (**%0**) that existed before the shift.

Examples

To use a batch file, called *Mycopy.bat*, to copy a list of files to a specific directory, type:

```
@echo off
rem MYCOPY.BAT copies any number of files
rem to a directory.
rem The command uses the following syntax:
rem mycopy dir file1 file2 ...
set todir=%1
:getfile
shift
if "%1"=="" goto end
copy %1 %todir%
goto getfile
:end
set todir=
echo All done
```

Related links

- Command-Line Syntax Key

showmount

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

You can use **showmount** to display information about mounted file systems exported by Server for NFS on a specified computer. If you don't specify a server, this command displays information about the computer on which the **showmount** command is run.

Syntax

```
showmount {-e|-a|-d} <server>
```

Parameters

Parameter	Description
-e	Displays all the file systems exported on the server.
-a	Displays all Network File System (NFS) clients and the directories on the server each has mounted.
-d	Displays all directories on the server that are currently mounted by NFS clients.

Related links

- Command-Line Syntax Key
- Services for Network File System Command Reference

shutdown

Article • 10/05/2023

Enables you to shut down or restart local or remote computers, one at a time.

Syntax

```
shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o] [/hybrid]
[/soft] [/fw] [/f] [/m \\computer][/t xxx][/d [p|u:]xx:yy [/c "comment"]]
```

Parameters

Parameter	Description
/i	Displays the **Remote Shutdown** box. The **/i** option must be the first parameter following the command. If **/i** is specified, all other options are ignored.
/l	Logs off the current user immediately, with no time-out period. You can't use **/l** with **/m** or **/t**.
/s	Shuts down the computer.
/sg	Shuts down the computer. On the next boot, if **Automatic Restart Sign-On** is enabled, the device automatically signs in and locks based on the last interactive user. After sign in, it restarts any registered applications.
/r	Restarts the computer after shutdown.
/g	Fully shuts down and restarts the computer. On restart, if **Automatic Restart Sign-On** is enabled, the device automatically signs in and locks based on the last interactive user. After sign in, it restarts any registered applications.
/a	Aborts a system shutdown. Can only be used during the time-out period. Combine with /fw to clear any pending boots to firmware.
/p	Turns off the local computer only (not a remote computer)—with no time-out period or warning. You can use **/p** only with **/d** or **/f**. If your computer doesn't support power-off functionality, it shuts down when you use **/p**, but the power to the computer remains on.
/h	Puts the local computer into hibernation, if hibernation is enabled. The **/f** switch can be used with the **/h** switch.

Parameter	Description
/hybrid	Shuts down the device and prepares it for fast startup. This option must be used with the **/s** option.
/soft	Allows running processes and applications to gracefully close instead of forcibly terminating.
/fw	Combining this option with a shutdown option causes the next restart to go to the firmware user interface.
/e	Enables you to document the reason for an unexpected shutdown of a computer in the Shutdown Event Tracker.
/o	Goes to the **Advanced boot options** menu and restarts the device. This option must be used with the **/r** option.
/f	Forces running applications to close without warning users. **Caution:** Using the **/f** option might result in loss of unsaved data.
/m `\\ <computername>`	Specifies the target computer. Can't be used with the **/l** option.
/t `<xxx>`	Sets the time-out period before shutdown to *xxx* seconds. The valid range is 0-315360000 (10 years), with a default of 30. If the timeout period is greater than 0, the **/f** parameter is implied.
/d `[p | u:] <xx>:<yy>`	Lists the reason for the system restart or shutdown. The supported parameter values are: • **P** - Indicates that the restart or shutdown is planned. • **U** - Indicates that the reason is user-defined. If **p** or **u** aren't specified, the restart or shutdown is unplanned. • *xx* - Specifies the major reason number (a positive integer, less than 256). • *yy* Specifies the minor reason number (a positive integer, less than 65536).
/c `<comment>`	Enables you to create a custom reason for the system shutdown or restart, which must be enclosed in double quotation marks. You can use a maximum of 512 characters. Can also be used with the **/d** parameter.
/?	Displays help at the command prompt, including a list of the major and minor reasons that are defined on your local computer.

Remarks

- Users must be assigned the **Shut down the system** user right to shut down a local or remotely administered computer that is using the **shutdown** command.
- Users must be members of the **Administrators** group to annotate an unexpected shutdown of a local or remotely administered computer. If the target computer is joined to a domain, members of the **Domain Admins** group might be able to perform this procedure. For more information, see:
  - Default local groups
  - Default groups
- If you want to shut down more than one computer at a time, you can call **shutdown** for each computer by using a script, or you can use **shutdown /i** to display the **Remote Shutdown** box.
- If you specify major and minor reason codes, you must first define these reason codes on each computer where you plan to use the reasons. If the reason codes aren't defined on the target computer, Shutdown Event Tracker can't log the correct reason text.
- Remember to indicate that a shutdown is planned by using the **/p** parameter. Not using the **/p** parameter, indicates that the shutdown was unplanned.
  - Using the **/p** parameter, along the reason code for an unplanned shutdown, causes the shutdown to fail.
  - Not using the **/p** parameter, and only providing the reason code for a planned shutdown, also causes the shutdown to fail.

The shutdown or restart reasons uses the following legend:

- **E**: Expected - An expected shutdown or restart that is planned and communicated in advance.
- **U**: Unexpected - An unexpected shutdown or restart occurs where the system stops working due to an error, such as a system crash, power failure or other.
- **P**: Planned - A planned shutdown or restart scheduled in advance, such as system maintenance, software installation or other.
- **C**: Customer Defined - Specify a custom reason for the system shutdown or restart.

Reason type	Major	Minor	Description
U	0	0	Other (Unplanned)
E	0	0	Other (Unplanned)

Reason type	Major	Minor	Description
E or P	0	0	Other (Planned)
U	0	5	Other Failure: System Unresponsive
E	1	1	Hardware: Maintenance (Unplanned)
E or P	1	1	Hardware: Maintenance (Planned)
E	1	2	Hardware: Installation (Unplanned)
E or P	1	2	Hardware: Installation (Planned)
E	2	2	Operating System: Recovery (Unplanned)
E or P	2	2	Operating System: Recovery (Planned)
P	2	3	Operating System: Upgrade (Planned)
E	2	4	Operating System: Reconfiguration (Unplanned)
E or P	2	4	Operating System: Reconfiguration (Planned)
P	2	16	Operating System: Service pack (Planned)
	2	17	Operating System: Hot fix (Unplanned)
P	2	17	Operating System: Hot fix (Planned)
	2	18	Operating System: Security fix (Unplanned)
P	2	18	Operating System: Security fix (Planned)
E	4	1	Application: Maintenance (Unplanned)
E or P	4	1	Application: Maintenance (Planned)
E or P	4	2	Application: Installation (Planned)
E	4	5	Application: Unresponsive
E	4	6	Application: Unstable
U	5	15	System Failure: Stop error
U	5	19	Security issue (Unplanned)
E	5	19	Security issue (Unplanned)
E or P	5	19	Security issue (Planned)
E	5	20	Loss of network connectivity (Unplanned)

Reason type	Major	Minor	Description
U	6	11	Power Failure: Cord Unplugged
U	6	12	Power Failure: Environment
P	7	0	Legacy API shutdown

Examples

To force apps to close and to restart the local computer after a one-minute delay, with the reason *Application: Maintenance (Planned)* and the comment "Reconfiguring myapp.exe", type:

```
shutdown /r /t 60 /c "Reconfiguring myapp.exe" /f /d p:4:1
```

To restart the remote computer *myremoteserver* with the same parameters as the previous example, type:

```
shutdown /r /m \\myremoteserver /t 60 /c "Reconfiguring myapp.exe" /f /d
p:4:1
```

To restart the remote computer *myremoteserver* in 5 minutes due to a security update and include a custom reason in the shutdown event tracker, type:

```
shutdown /r /t 300 /e /c "Security Update" /m \\myremoteserver
```

Related links

- Command-Line Syntax Key

Simulate restore

Article • 02/03/2023

Tests whether writer involvement in restore sessions will be successful on the computer without issuing **PreRestore** or **PostRestore** events to writers.

> **Note**
>
> A DiskShadow metadata file must be selected for the **simulate restore** command to succeed. Use the **load metadata command** to load the selected writers and components for the restore.

Syntax

```
simulate restore
```

Related links

- Command-Line Syntax Key
- load metadata command

sort

Article • 02/03/2023

Reads input, sorts data, and writes the results to the screen, to a file, or to another device.

Syntax

```
sort [/r] [/+<N>] [/m <kilobytes>] [/l <locale>] [/rec <characters>]
[[<drive1>:][<path1>]<filename1>] [/t [<drive2>:][<path2>]] [/o [<drive3>:]
[<path3>]<filename3>]
```

Parameters

Parameter	Description
/r	Reverses the sort order (that is, sorts from Z to A and from 9 to 0).
`/+<N>`	Specifies the character position number where **sort** will begin each comparison. *N* can be any valid integer.
/m `<kilobytes>`	Specifies the amount of main memory to use for the sort in kilobytes (KB).
/l <locale>	Overrides the sort order of characters that are defined by the system default locale (that is, the language and Country/Region selected during installation).
/rec `<characters>`	Specifies the maximum number of characters in a record or a line of the input file (the default value is 4,096 and the maximum is 65,535).
`[<drive1>:]` `[<path1>]` `<filename1>`	Specifies the file to be sorted. If no file name is specified, the standard input is sorted. Specifying the input file is faster than redirecting the same file as standard input.
/t `[<drive2>:]` `[<path2>]`	Specifies the path of the directory to hold the **sort** command's working storage if the data does not fit in the main memory. By default, the system temporary directory is used.
/o `[<drive3>:]` `[<path3>]` `<filename3>`	Specifies the file where the sorted input is to be stored. If not specified, the data is written to the standard output. Specifying the output file is faster than redirecting standard output to the same file.

Parameter	Description
/unique	Only returns unique results.
/?	Displays help at the command prompt.

Remarks

- By default, comparisons start at the first character of each line. The **/+** command-line option starts comparisons at the character that is specified by *N*. For example, `/+3` indicates that each comparison should begin at the third character of each line. Lines with fewer than *N* characters collate before other lines.
- The memory used is always a minimum of 160 KB. If the memory size is specified, the exact specified amount is used for the sort (must be at least 160 KB), regardless of how much main memory is available.
- The default maximum memory size when no size is specified is 90% of the available main memory, if both the input and output are files, or 45% of main memory otherwise. The default setting usually gives the best performance.
- Currently, the only alternative to the default locale is the C locale, which is faster than natural language sorting (it sorts characters according to their binary encodings).
- You can use the pipe symbol (`|`) to direct input data to the **sort** command from another command or to direct sorted output to another command. You can specify input and output files by using redirection symbols (`<` or `>`). It can be faster and more efficient (especially with large files) to specify the input file directly (as defined by *filename1* in the command syntax), and then specify the output file using the **/o** parameter.
- The **sort** command doesn't distinguish between uppercase and lowercase letters and has no limit on file size.
- The sort program uses the collating-sequence table that corresponds to the **Country/Region** code and code-page settings. Characters greater than ASCII code 127 are sorted based on information in the Country.sys file or in an alternate file specified by the **country** command in your Config.nt file.
- If the sort fits within the maximum memory size (as set by default or as specified by the **/m** parameter), the sort is performed in a single pass. Otherwise, the sort is performed in two separate sort and merge passes, and the amounts of memory

used for both passes are equal. When two passes are performed, the partially sorted data is stored in a temporary file on disk. If there is not enough memory to perform the sort in two passes, a run-time error is issued. If the **/m** command-line option is used to specify more memory than is truly available, performance degradation or a run-time error can occur.

Examples

- To sort and display, in reverse order, the lines in a file named *expenses.txt*, type:

```
sort /r expenses.txt
```

- To search a large file named *maillist.txt* for the text *Jones*, and to sort the results of the search using the pipe (`|`) to direct the output of a **find** command to the **sort** command, type:

```
find Jones maillist.txt | sort
```

  The command produces a sorted list of lines that contain the specified text.

- To sort keyboard input and display the results alphabetically on the screen, you can first use the **sort** command with no parameters, by typing:

```
sort
```

  Then type the text that you want sorted, and press ENTER at the end of each line. When you have finished typing text, press CTRL+Z, and then press ENTER. The **sort** command displays the text you typed, sorted alphabetically.

Related links

- Command-Line Syntax Key

start

Article • 10/02/2023

Starts a separate Command Prompt window to run a specified program or command.

Syntax

```
start <"title"> [/d <path>] [/i] [{/min | /max}] [{/separate | /shared}]
[{/low | /normal | /high | /realtime | /abovenormal | /belownormal}] [/node
<NUMA node>] [/affinity <hexaffinity>] [/wait] [/b] [/machine
<x86|amd64|arm|arm64>] [<command> [<parameter>... ] | <program>
[<parameter>... ]]
```

> **Note**
>
> The **machine** parameter is currently in PREVIEW for Windows 11 only. The parameter is available beginning with the **Windows 11 Insider Preview Build 22557**. This information relates to a prerelease product that may be substantially modified before it's released. Microsoft makes no warranties, expressed or implied, with respect to the information provided here.

Parameters

Parameter	Description
`"title"`	Specifies the title to display in the **Command Prompt** window title bar.
/d `<path>`	Specifies the startup directory.
/i	Passes the Cmd.exe startup environment to the new **Command Prompt** window. If `/i` isn't specified, the current environment is used.
`{/min | /max}`	Specifies to minimize (`/min`) or maximize (`/max`) the new **Command Prompt** window.
`{/separate | /shared}`	Starts 16-bit programs in a separate memory space (`/separate`) or shared memory space (**/shared**). These options aren't supported on 64-bit platforms.
`{/low | /normal | /high | /realtime |`	Starts an application in the specified priority class.

Parameter	Description
`/abovenormal | /belownormal}`	
/node `<NUMA node>`	Leverages memory locality on NUMA (Non-Uniform Memory Architecture) nodes as a decimal integer. Two processes that communicate with each other through shared memory on the preferred NUMA node can minimize memory latencies while allocating memory from the same NUMA node when possible. They're free to run on processors outside the specified node.
/affinity `<hexaffinity>`	Applies the specified processor affinity mask (expressed as a hexadecimal number) to the new application. Two programs are able to run on specific processor cores within the same NUMA node. This number can be changed to the processor-specific supported amount without having to change the affinity mask.
/wait	Starts an application and waits for it to end.
/b	Starts an application without opening a new **Command Prompt** window. CTRL+C handling is ignored unless the application enables CTRL+C processing. Use CTRL+BREAK to interrupt the application.
/machine `<x86 | amd64 | arm | arm64>`	Specifies the machine architecture of the application process.
`[<command> [<parameter>... ] | <program> [<parameter>... ]]`	Specifies the command or program to start.
`<parameter>`	Specifies parameters to pass to either the command or the program.
/?	Displays help at the command prompt.

Remarks

- You can run non-executable files through their file association by typing the name of the file as a command.
- If you run a command that contains the string CMD as the first token without an extension or path qualifier, CMD is replaced with the value of the COMSPEC variable. This prevents users from picking up `cmd` from the current directory.
- If you run a 32-bit graphical user interface (GUI) application, `cmd` doesn't wait for the application to quit before returning to the command prompt. This behavior doesn't occur if you run the application from a command script.

- If you're running on a 64-bit platform, the `/separate` and `/shared` parameters aren't supported.
- If you run a command that uses a first token that isn't a command or the file path to an existing file with an extension, `Cmd.exe` uses the value of the PATHEXT environment variable to determine which extensions to look for and in what order. The default value for the PATHEXT variable is `.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC`

  Note the syntax is the same as the PATH variable, with semicolons (;) separating each extension.
- **start** searches for a specified executable file, and if found, the executable launches regardless of the current working directory. When searching for an executable file, if there's no match on any extension, **start** checks to see if the name matches a directory name. If it does, **start** opens `Explorer.exe` on that path.

Examples

To start the *Myapp* program at the command prompt and retain use of the current **Command Prompt** window, type:

Windows Command Prompt

```
start Myapp
```

To view the **start** command-line help information in a separate maximized **Command Prompt** window, type:

Windows Command Prompt

```
start /max start /?
```

Related links

- Command-Line Syntax Key

subst

Article • 02/03/2023

Associates a path with a drive letter. If used without parameters, **subst** displays the names of the virtual drives in effect.

Syntax

```
subst [<drive1>: [<drive2>:]<path>]
subst <drive1>: /d
```

Parameters

Parameter	Description
`<drive1>:`	Specifies the virtual drive to which you want to assign a path.
`[<drive2>:]<path>`	Specifies the physical drive and path that you want to assign to a virtual drive.
/d	Deletes a substituted (virtual) drive.
/?	Displays help at the command prompt.

Remarks

- The following commands don't work and must not be used on drives specified in the **subst** command:
  - chkdsk command

    diskcomp command

    diskcopy command

    format command

    label command

    recover command

- The `<drive1>` parameter must be within the range that is specified by the **lastdrive** command. If not, **subst** displays the following error message: `Invalid parameter - drive1:`

Examples

To create a virtual drive z for the path b:\user\betty\forms, type:

```
subst z: b:\user\betty\forms
```

Instead of typing the full path, you can reach this directory by typing the letter of the virtual drive followed by a colon as follows:

```
z:
```

Related links

- Command-Line Syntax Key

sxstrace

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Diagnoses side-by-side problems.

Syntax

```
sxstrace [{[trace -logfile:<filename> [-nostop]|[parse -logfile:<filename> -
outfile:<parsedfile>  [-filter:<appname>]}]
```

Parameters

Parameter	Description
trace	Enables tracing for side-by-side.
-logfile	Specifies the raw log file.
`<filename>`	Saves tracing log to `<filename>`.
-nostop	Specifies that you shouldn't receive a prompt to stop tracing.
parse	Translates the raw trace file.
-outfile	Specifies the output filename.
`<parsedfile>`	Specifies the filename of the parsed file.
-filter	Allows the output to be filtered.
`<appname>`	Specifies the name of the application.
stoptrace	Stops the trace, if it wasn't stopped before.
-?	Displays help at the command prompt.

Examples

To enable tracing and to save the trace file to *sxstrace.etl*, type:

```
sxstrace trace -logfile:sxstrace.etl
```

To translate the raw trace file into a human readable format and to save the result to *sxstrace.txt*, type:

```
sxstrace parse -logfile:sxstrace.etl -outfile:sxstrace.txt
```

Related links

- Command-Line Syntax Key

sysocmgr

Article • 03/03/2021

The sysocmger command has been deprecated and isn't guaranteed to be supported in future releases of Windows.

systeminfo

Article • 02/03/2023

Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties (such as RAM, disk space, and network cards).

Syntax

```
systeminfo [/s <computer> [/u <domain>\<username> [/p <password>]]] [/fo
{TABLE | LIST | CSV}] [/nh]
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
/u `<domain>\` `<username>`	Runs the command with the account permissions of the specified user account. If **/u** is not specified, this command uses the permissions of the user who is currently logged on to the computer that is issuing the command.
/p `<password>`	Specifies the password of the user account that is specified in the **/u** parameter.
/fo `<format>`	Specifies the output format with one of the following values: • **TABLE** - Displays output in a table. • **LIST** - Displays output in a list. • **CSV** - Displays output in comma-separated values (.csv) format.
/nh	Suppresses column headers in the output. Valid when the **/fo** parameter is set to TABLE or CSV.
/?	Displays help at the command prompt.

Examples

To view configuration information for a computer named *Srvmain*, type:

```
systeminfo /s srvmain
```

To remotely view configuration information for a computer named *Srvmain2* that is located on the *Maindom* domain, type:

```
systeminfo /s srvmain2 /u maindom\hiropln
```

To remotely view configuration information (in list format) for a computer named *Srvmain2* that is located on the *Maindom* domain, type:

```
systeminfo /s srvmain2 /u maindom\hiropln /p p@ssW23 /fo list
```

Related links

- Command-Line Syntax Key

takeown

Article • 02/03/2023

Enables an administrator to recover access to a file that previously was denied, by making the administrator the owner of the file. This command is typically used on batch files.

Syntax

```
takeown [/s <computer> [/u [<domain>\]<username> [/p [<password>]]]] /f
<filename> [/a] [/r [/d {Y|N}]]
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer (do not use backslashes). The default value is the local computer. This parameter applies to all of the files and folders specified in the command.
/u `[<domain>\]` `<username>`	Runs the script with the permissions of the specified user account. The default value is system permissions.
/p `[<[password>]`	Specifies the password of the user account that is specified in the **/u** parameter.
/f `<filename>`	Specifies the file name or directory name pattern. You can use the wildcard character `*` when specifying the pattern. You can also use the syntax `<sharename>\<filename>`.
/a	Gives ownership to the Administrators group instead of the current user. If you don't specify this option, file ownership is given to the user who is currently logged on to the computer.
/r	Performs a recursive operation on all files in the specified directory and subdirectories.

Parameter	Description
/d `{Y | N}`	Suppresses the confirmation prompt that is displayed when the current user does not have the **List Folder** permission on a specified directory, and instead uses the specified default value. Valid values for the **/d** option are: • **Y** - Take ownership of the directory. • **N** - Skip the directory. **NOTE** You must use this option in conjunction with the **/r** option.
/?	Displays help at the command prompt.

Remarks

- Mixed patterns using (**?** and ***) aren't supported by **takeown** command.
- After deleting the lock with **takeown**, you might have to use Windows Explorer to give yourself full permissions to the files and directories before you can delete them.

Examples

To take ownership of a file named *Lostfile*, type:

```
takeown /f lostfile
```

Related links

- Command-Line Syntax Key

tapicfg

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates, removes, or displays a TAPI application directory partition, or sets a default TAPI application directory partition. TAPI 3.1 clients can use the information in this application directory partition with the directory service locator service to find and communicate with TAPI directories. You can also use **tapicfg** to create or remove service connection points, which enable TAPI clients to efficiently locate TAPI application directory partitions in a domain.

This command-line tool can be run on any computer that is a member of the domain.

Syntax

```
tapicfg install
tapicfg remove
tapicfg publishscp
tapicfg removescp
tapicfg show
tapicfg makedefault
```

Parameters

Parameters	Description
tapicfg install	Creates a TAPI application directory partition.
tapicfg remove	Removes a TAPI application directory partition.
tapicfg publishscp	Creates a service connection point to publish a TAPI application directory partition.
tapicfg removescp	Removes a service connection point for a TAPI application directory partition.
tapicfg show	Displays the names and locations of the TAPI application directory partitions in the domain.

Parameters	Description
tapicfg makedefault	Sets the default TAPI application directory partition for the domain.

Remarks

- You must be a member of the **Enterprise Admins** group in Active Directory to run either **tapicfg install** (to create a TAPI application directory partition) or **tapicfg remove** (to remove a TAPI application directory partition).
- User-supplied text (such as the names of TAPI application directory partitions, servers, and domains) with International or Unicode characters are only displayed correctly if appropriate fonts and language support are installed.
- You can still use Internet Locator Service (ILS) servers in your organization, if ILS is needed to support certain applications, because TAPI clients running Windows XP or a Windows Server 2003 operating system can query either ILS servers or TAPI application directory partitions.
- You can use **tapicfg** to create or remove service connection points. If the TAPI application directory partition is renamed for any reason (for example, if you rename the domain in which it resides), you must remove the existing service connection point and create a new one that contains the new DNS name of the TAPI application directory partition to be published. Otherwise, TAPI clients are unable to locate and access the TAPI application directory partition. You can also remove a service connection point for maintenance or security purposes (for example, if you do not want to expose TAPI data on a specific TAPI application directory partition).

Related links

- Command-Line Syntax Key
- tapicfg install
- tapicfg remove
- tapicfg publishscp
- tapicfg removescp
- tapicfg show

- tapicfg makedefault

tapicfg install

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates a TAPI application directory partition.

> **ⓘ Important**
>
> You must be a member of the Enterprise Admins group in active directory to run this command.

Syntax

```
tapicfg install /directory:<partitionname> [/server:<DCname>]
[/forcedefault]
```

Parameters

Parameter	Description
install `/directory:` `<partitionname>`	Required. Specifies the DNS name of the TAPI application directory partition to be created. This name must be a fully-qualified domain name.
/server: `<DCname>`	Specifies the DNS name of the domain controller on which the TAPI application directory partition is created. If the domain controller name isn't specified, the name of the local computer is used.
/forcedefault	Specifies that this directory is the default TAPI application directory partition for the domain. There can be multiple TAPI application directory partitions in a domain. if this directory is the first TAPI application directory partition created on the domain, it's automatically set as the default, regardless of whether you use the **/forcedefault** option.
/?	Displays help at the command prompt.

Remarks

- This command-line tool can be run on any computer that is a member of the domain.
- User-supplied text (such as the names of TAPI application directory partitions, servers, and domains) with International or Unicode characters are only displayed correctly if appropriate fonts and language support are installed.
- You can still use Internet Locator Service (ILS) servers in your organization, if ILS is needed to support certain applications, because TAPI clients running Windows XP or a Windows Server 2003 operating system can query either ILS servers or TAPI application directory partitions.
- You can use **tapicfg** to create or remove service connection points. If the TAPI application directory partition is renamed for any reason (for example, if you rename the domain in which it resides), you must remove the existing service connection point and create a new one that contains the new DNS name of the TAPI application directory partition to be published. Otherwise, TAPI clients are unable to locate and access the TAPI application directory partition. You can also remove a service connection point for maintenance or security purposes (for example, if you do not want to expose TAPI data on a specific TAPI application directory partition).

Examples

To create a TAPI application directory partition named *tapifiction.testdom.microsoft.com* on a server named *testdc.testdom.microsoft.com*, and then set it as the default TAPI application directory partition for the new domain, type:

```
tapicfg install /directory:tapifiction.testdom.microsoft.com
/server:testdc.testdom.microsoft.com /forcedefault
```

Related links

- Command-Line Syntax Key
- tapicfg remove
- tapicfg publishscp

- tapicfg removescp
- tapicfg show
- tapicfg makedefault

tapicfg remove

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes a TAPI application directory partition.

> **ⓘ Important**
>
> You must be a member of the Enterprise Admins group in active directory to run this command.

Syntax

```
tapicfg remove /directory:<partitionname>
```

Parameters

Parameter	Description
remove `/directory:<partitionname>`	Required. Specifies the DNS name of the TAPI application directory partition to be removed. Note that this name must be a fully-qualified domain name.
/?	Displays help at the command prompt.

Remarks

- This command-line tool can be run on any computer that is a member of the domain.
- User-supplied text (such as the names of TAPI application directory partitions, servers, and domains) with International or Unicode characters are only displayed correctly if appropriate fonts and language support are installed.

- You can still use Internet Locator Service (ILS) servers in your organization, if ILS is needed to support certain applications, because TAPI clients running Windows XP or a Windows Server 2003 operating system can query either ILS servers or TAPI application directory partitions.
- You can use **tapicfg** to create or remove service connection points. If the TAPI application directory partition is renamed for any reason (for example, if you rename the domain in which it resides), you must remove the existing service connection point and create a new one that contains the new DNS name of the TAPI application directory partition to be published. Otherwise, TAPI clients are unable to locate and access the TAPI application directory partition. You can also remove a service connection point for maintenance or security purposes (for example, if you do not want to expose TAPI data on a specific TAPI application directory partition).

Related links

- Command-Line Syntax Key
- tapicfg install
- tapicfg publishscp
- tapicfg removescp
- tapicfg show
- tapicfg makedefault

tapicfg publishscp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates a service connection point to publish a TAPI application directory partition.

Syntax

```
tapicfg publishscp /directory:<partitionname> [/domain:<domainname>]
[/forcedefault]
```

Parameters

Parameter	Description
publishscp `/directory:<partitionname>`	Required. Specifies the DNS name of the TAPI application directory partition that the service connection point will publish.
/domain: `<domainname>`	Specifies the DNS name of the domain in which the service connection point is created. If the domain name is not specified, the name of the local domain is used.
/forcedefault	Specifies that this directory is the default TAPI application directory partition for the domain. There can be multiple TAPI application directory partitions in a domain.
/?	Displays help at the command prompt.

Remarks

- This command-line tool can be run on any computer that is a member of the domain.
- User-supplied text (such as the names of TAPI application directory partitions, servers, and domains) with International or Unicode characters are only displayed correctly if appropriate fonts and language support are installed.

- You can still use Internet Locator Service (ILS) servers in your organization, if ILS is needed to support certain applications, because TAPI clients running Windows XP or a Windows Server 2003 operating system can query either ILS servers or TAPI application directory partitions.
- You can use **tapicfg** to create or remove service connection points. If the TAPI application directory partition is renamed for any reason (for example, if you rename the domain in which it resides), you must remove the existing service connection point and create a new one that contains the new DNS name of the TAPI application directory partition to be published. Otherwise, TAPI clients are unable to locate and access the TAPI application directory partition. You can also remove a service connection point for maintenance or security purposes (for example, if you do not want to expose TAPI data on a specific TAPI application directory partition).

Related links

- Command-Line Syntax Key
- tapicfg install
- tapicfg remove
- tapicfg removescp
- tapicfg show
- tapicfg makedefault

tapicfg removescp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes a service connection point for a TAPI application directory partition.

Syntax

```
tapicfg removescp /directory:<partitionname> [/domain:<domainname>]
```

Parameters

Parameter	Description
removescp `/directory:<partitionname>`	Required. Specifies the DNS name of the TAPI application directory partition for which a service connection point is removed.
/domain: `<domainname>`	Specifies the DNS name of the domain from which the service connection point is removed. If the domain name isn't specified, the name of the local domain is used.
/?	Displays help at the command prompt.

Remarks

- This command-line tool can be run on any computer that is a member of the domain.
- User-supplied text (such as the names of TAPI application directory partitions, servers, and domains) with International or Unicode characters are only displayed correctly if appropriate fonts and language support are installed.
- You can still use Internet Locator Service (ILS) servers in your organization, if ILS is needed to support certain applications, because TAPI clients running Windows XP or a Windows Server 2003 operating system can query either ILS servers or TAPI application directory partitions.

- You can use **tapicfg** to create or remove service connection points. If the TAPI application directory partition is renamed for any reason (for example, if you rename the domain in which it resides), you must remove the existing service connection point and create a new one that contains the new DNS name of the TAPI application directory partition to be published. Otherwise, TAPI clients are unable to locate and access the TAPI application directory partition. You can also remove a service connection point for maintenance or security purposes (for example, if you do not want to expose TAPI data on a specific TAPI application directory partition).

Related links

- Command-Line Syntax Key
- tapicfg install
- tapicfg remove
- tapicfg publishscp
- tapicfg show
- tapicfg makedefault

tapicfg show

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the names and locations of the TAPI application directory partitions in the domain.

Syntax

```
tapicfg show [/defaultonly] [/domain:<domainname>]
```

Parameters

Parameter	Description
/default only	Displays the names and locations of only the default TAPI application directory partition in the domain.
/domain: `<domainname>`	Specifies the DNS name of the domain for which the TAPI application directory partitions are displayed. If the domain name isn't specified, the name of the local domain is used.
/?	Displays help at the command prompt.

Remarks

- This command-line tool can be run on any computer that is a member of the domain.
- User-supplied text (such as the names of TAPI application directory partitions, servers, and domains) with International or Unicode characters are only displayed correctly if appropriate fonts and language support are installed.
- You can still use Internet Locator Service (ILS) servers in your organization, if ILS is needed to support certain applications, because TAPI clients running Windows XP or a Windows Server 2003 operating system can query either ILS servers or TAPI application directory partitions.

- You can use **tapicfg** to create or remove service connection points. If the TAPI application directory partition is renamed for any reason (for example, if you rename the domain in which it resides), you must remove the existing service connection point and create a new one that contains the new DNS name of the TAPI application directory partition to be published. Otherwise, TAPI clients are unable to locate and access the TAPI application directory partition. You can also remove a service connection point for maintenance or security purposes (for example, if you do not want to expose TAPI data on a specific TAPI application directory partition).

Example

To display the name of the default TAPI application directory partition for the new domain, type:

```
tapicfg show /defaultonly
```

Related links

- Command-Line Syntax Key
- tapicfg install
- tapicfg remove
- tapicfg publishscp
- tapicfg removescp
- tapicfg makedefault

tapicfg makedefault

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets the default TAPI application directory partition for the domain.

Syntax

```
tapicfg makedefault /directory:<partitionname> [/domain:<domainname>]
```

Parameters

Parameter	Description
makedefault `/directory:` `<partitionname>`	Required. Specifies the DNS name of the TAPI application directory partition set as the default partition for the domain. This name must be a fully-qualified domain name.
/domain: `<domainname>`	Specifies the DNS name of the domain for which the TAPI application directory partition is set as the default. If the domain name is not specified, the name of the local domain is used.
/?	Displays help at the command prompt.

Remarks

- This command-line tool can be run on any computer that is a member of the domain.
- User-supplied text (such as the names of TAPI application directory partitions, servers, and domains) with International or Unicode characters are only displayed correctly if appropriate fonts and language support are installed.
- You can still use Internet Locator Service (ILS) servers in your organization, if ILS is needed to support certain applications, because TAPI clients running Windows XP or a Windows Server 2003 operating system can query either ILS servers or TAPI application directory partitions.

- You can use **tapicfg** to create or remove service connection points. If the TAPI application directory partition is renamed for any reason (for example, if you rename the domain in which it resides), you must remove the existing service connection point and create a new one that contains the new DNS name of the TAPI application directory partition to be published. Otherwise, TAPI clients are unable to locate and access the TAPI application directory partition. You can also remove a service connection point for maintenance or security purposes (for example, if you do not want to expose TAPI data on a specific TAPI application directory partition).

Related links

- Command-Line Syntax Key
- tapicfg install
- tapicfg remove
- tapicfg publishscp
- tapicfg removescp
- tapicfg show

taskkill

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Ends one or more tasks or processes. Processes can be ended by process ID or image name. You can use the tasklist command command to determine the process ID (PID) for the process to be ended.

> **Note**
>
> This command replaces the **kill** tool.

Syntax

```
taskkill [/s <computer> [/u [<domain>\]<username> [/p [<password>]]]] {[/fi
<filter>] [...] [/pid <processID> | /im <imagename>]} [/f] [/t]
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
/u `<domain>\` `<username>`	Runs the command with the account permissions of the user who is specified by `<username>` or by `<domain>\<username>`. The **/u** parameter can be specified only if **/s** is also specified. The default is the permissions of the user who is currently logged on to the computer that is issuing the command.
/p `<password>`	Specifies the password of the user account that is specified in the **/u** parameter.
/fi `<filter>`	Applies a filter to select a set of tasks. You can use more than one filter or use the wildcard character (`*`) to specify all tasks or image names. The valid filters are listed in the **Filter names, operators, and values** section of this article.

Parameter	Description
/pid `<processID>`	Specifies the process ID of the process to be terminated.
/im `<imagename>`	Specifies the image name of the process to be terminated. Use the wildcard character (`*`) to specify all image names.
/f	Specifies that processes be forcefully ended. This parameter is ignored for remote processes; all remote processes are forcefully ended.
/t	Ends the specified process and any child processes started by it.

Filter names, operators, and values

Filter Name	Valid Operators	Valid Value(s)
STATUS	eq, ne	`RUNNING | NOT RESPONDING | UNKNOWN`
IMAGENAME	eq, ne	Image name
PID	eq, ne, gt, lt, ge, le	PID value
SESSION	eq, ne, gt, lt, ge, le	Session number
CPUtime	eq, ne, gt, lt, ge, le	CPU time in the format *HH:MM:SS*, where *MM* and *SS* are between 0 and 59 and *HH* is any unsigned number
MEMUSAGE	eq, ne, gt, lt, ge, le	Memory usage in KB
USERNAME	eq, ne	Any valid user name (`<user>` or `<domain\user>`)
SERVICES	eq, ne	Service name
WINDOWTITLE	eq, ne	Window title
MODULES	eq, ne	DLL name

Remarks

- The **WINDOWTITLE** and **STATUS** filters aren't supported when a remote system is specified.

- The wildcard character (`*`) is accepted for the `*/im` option, only when a filter is applied.
- Ending a remote process is always carried out forcefully, regardless whether the **/f** option is specified.
- Providing a computer name to the hostname filter causes a shutdown, stopping all processes.

Examples

To end the processes with process IDs *1230*, *1241*, and *1253*, type:

```
taskkill /pid 1230 /pid 1241 /pid 1253
```

To forcefully end the process *Notepad.exe* if it was started by the system, type:

```
taskkill /f /fi "USERNAME eq NT AUTHORITY\SYSTEM" /im notepad.exe
```

To end all processes on the remote computer *Srvmain* with an image name beginning with *note*, while using the credentials for the user account *Hiropln*, type:

```
taskkill /s srvmain /u maindom\hiropln /p p@ssW23 /fi "IMAGENAME eq note*"
/im *
```

To end the process with the process ID *2134* and any child processes that it started, but only if those processes were started by the Administrator account, type:

```
taskkill /pid 2134 /t /fi "username eq administrator"
```

To end all processes that have a process ID *greater than or equal to 1000*, regardless of their image names, type:

```
taskkill /f /fi "PID ge 1000" /im *
```

Related links

- Command-Line Syntax Key
- tasklist command

tasklist

Article • 02/03/2023

Displays a list of currently running processes on the local computer or on a remote computer. **Tasklist** replaces the **tlist** tool.

> **Note**
>
> This command replaces the **tlist** tool.

Syntax

```
tasklist [/s <computer> [/u [<domain>\]<username> [/p <password>]]] [{/m
<module> | /svc | /v}] [/fo {table | list | csv}] [/nh] [/fi <filter> [/fi
<filter> [ ... ]]]
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.
/u `<domain>\<username>`	Runs the command with the account permissions of the user who is specified by `<username>` or by `<domain>\<username>`. The **/u** parameter can be specified only if **/s** is also specified. The default is the permissions of the user who is currently logged on to the computer that is issuing the command.
/p `<password>`	Specifies the password of the user account that is specified in the **/u** parameter.
/m `<module>`	Lists all tasks with DLL modules loaded that match the given pattern name. If the module name is not specified, this option displays all modules loaded by each task.
svc	Lists all the service information for each process without truncation. Valid when the **/fo** parameter is set to **table**.
/v	Displays verbose task information in the output. For complete verbose output without truncation, use **/v** and **/svc** together.

Parameter	Description
/fo `{table | list | csv}`	Specifies the format to use for the output. Valid values are **table**, **list**, and **csv**. The default format for output is **table**.
/nh	Suppresses column headers in the output. Valid when the **/fo** parameter is set to **table** or **csv**.
/fi `<filter>`	Specifies the types of processes to include in or exclude from the query. You can use more than one filter or use the wildcard character (`\`) to specify all tasks or image names. The valid filters are listed in the **Filter names, operators, and values** section of this article.
/?	Displays help at the command prompt.

Filter names, operators, and values

Filter Name	Valid Operators	Valid Value(s)
STATUS	eq, ne	`RUNNING | NOT RESPONDING | UNKNOWN`. This filter isn't supported if you specify a remote system.
IMAGENAME	eq, ne	Image name
PID	eq, ne, gt, lt, ge, le	PID value
SESSION	eq, ne, gt, lt, ge, le	Session number
SESSIONNAME	eq, ne	Session name
CPUtime	eq, ne, gt, lt, ge, le	CPU time in the format *HH:MM:SS*, where *MM* and *SS* are between 0 and 59 and *HH* is any unsigned number
MEMUSAGE	eq, ne, gt, lt, ge, le	Memory usage in KB
USERNAME	eq, ne	Any valid user name (`<user>` or `<domain\user>`)
SERVICES	eq, ne	Service name
WINDOWTITLE	eq, ne	Window title. This filter isn't supported if you specify a remote system.
MODULES	eq, ne	DLL name

Examples

To list all tasks with a *process ID greater than 1000*, and *display them in csv format*, type:

```
tasklist /v /fi "PID gt 1000" /fo csv
```

To list the system processes that are currently running, type:

```
tasklist /fi "USERNAME ne NT AUTHORITY\SYSTEM" /fi "STATUS eq running"
```

To list detailed information for all processes that are currently running, type:

```
tasklist /v /fi "STATUS eq running"
```

To list all the service information for processes on the remote computer *srvmain*, which has a DLL name *beginning with ntdll*, type:

```
tasklist /s srvmain /svc /fi "MODULES eq ntdll*"
```

To list the processes on the remote computer *srvmain*, using the credentials of your currently logged-on user account, type:

```
tasklist /s srvmain
```

To list the processes on the remote computer *srvmain*, using the credentials of the *user account Hiropln*, type:

```
tasklist /s srvmain /u maindom\hiropln /p p@ssW23
```

Related links

- Command-Line Syntax Key

tcmsetup

Article • 02/03/2023

Sets up or disables the TAPI client. For TAPI to function correctly, you must run this command to specify the remote servers that will be used by TAPI clients.

> **ⓘ Important**
>
> To use this command, you must be a member of the **Administrators** group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the **Domain Admins** group might be able to perform this procedure. As a security best practice, consider using **Run as** to perform this procedure.

Syntax

```
tcmsetup [/q] [/x] /c <server1> [<server2> …]
tcmsetup  [/q] /c /d
```

Parameters

Parameter	Description
/q	Prevents the display of message boxes.
/x	Specifies that connection-oriented callbacks will be used for heavy traffic networks where packet loss is high. When this parameter is omitted, connectionless callbacks will be used.
/c	Required. Specifies client setup.
`<server1>`	Required. Specifies the name of the remote server that has the TAPI service providers that the client will use. The client will use the service providers' lines and phones. The client must be in the same domain as the server or in a domain that has a two-way trust relationship with the domain that contains the server.
`<server2>…`	Specifies any additional server or servers that will be available to this client. If you specify a list of servers is, use a space to separate the server names.

Parameter	Description
/d	Clears the list of remote servers. Disables the TAPI client by preventing it from using the TAPI service providers that are on the remote servers.
/?	Displays help at the command prompt.

Remarks

- Before a client user can use a phone or line on a TAPI server, the telephony server administrator must assign the user to the phone or line.
- The list of telephony servers that is created by this command replaces any existing list of telephony servers available to the client. You can't use this command to add to the existing list.

Related links

- Command-Line Syntax Key
- Command shell overview
- Specify telephony servers on a client computer
- Assign a telephony user to a line or phone

telnet

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Communicates with a computer running the telnet server service. Running this command without any parameters, lets you enter the telnet context, as indicated by the telnet prompt (**Microsoft telnet>**). From the telnet prompt, you can use telnet commands to manage the computer running the telnet client.

> **ⓘ Important**
>
> You must install the telnet client software before you can run this command. For more information, see **Installing telnet**.

Syntax

```
telnet [/a] [/e <escapechar>] [/f <filename>] [/l <username>] [/t {vt100 | vt52 | ansi | vtnt}] [<host> [<port>]] [/?]
```

Parameters

Parameter	Description
/a	Attempts automatic logon. Same as **/l** option, except that it uses the currently logged on user's name.
/e `<escapechar>`	Specifies the escape character used to enter the telnet client prompt.
/f `<filename>`	Specifies the file name used for client side logging.
/l `<username>`	Specifies the user name to log on with on the remote computer.
/t `{vt100 | vt52 | ansi | vtnt}`	Specifies the terminal type. Supported terminal types are **vt100**, **vt52**, **ansi**, and **vtnt**.
`<host> [<port>]`	Specifies the hostname or IP address of the remote computer to connect to, and optionally the TCP port to use (default is TCP port 23).

Parameter	Description
/?	Displays help at the command prompt.

Examples

To use telnet to connect to the computer running the telnet Server Service at *telnet.microsoft.com*, type:

```
telnet telnet.microsoft.com
```

To use telnet to connect to the computer running the telnet Server Service at *telnet.microsoft.com* on TCP port 44 and to log the session activity in a local file called *telnetlog.txt*, type:

```
telnet /f telnetlog.txt telnet.microsoft.com 44
```

Related links

- Command-Line Syntax Key
- Installing telnet
- telnet Technical Reference

telnet: close

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Closes the current connection.

Syntax

```
c[lose]
```

Examples

To close the current telnet connection, type:

```
c
```

Related links

- Command-Line Syntax Key

telnet: display

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays operating parameters.

Syntax

```
d[isplay]
```

Examples

To display operating parameters, type:

```
d
```

Related links

- Command-Line Syntax Key

telnet: open

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Connects to a telnet server.

Syntax

```
o[pen] <hostname> [<port>]
```

Parameters

Parameter	Description
`<hostname>`	Specifies the computer name or IP address.
`[<port>]`	Specifies the TCP port that the telnet server is listening on. The default is TCP port 23.

Examples

To connect to a telnet server at *telnet.microsoft.com*, type:

```
o telnet.microsoft.com
```

Related links

- Command-Line Syntax Key

telnet: quit

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Exits telnet.

Syntax

```
q[uit]
```

Examples

To exit telnet, type:

```
q
```

Related links

- Command-Line Syntax Key

telnet: send

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sends telnet commands to the telnet server.

Syntax

```
sen {ao | ayt | brk | esc | ip | synch | <string>} [?]
```

Parameters

Parameter	Description
ao	Sends the telnet command **Abort Output**.
ayt	Sends the telnet command **Are You There?**
brk	Sends the telnet command **brk**.
esc	Sends the current telnet escape character.
ip	Sends the telnet command **Interrupt Process**.
synch	Sends the telnet command synch.
`<string>`	Sends whatever string you type to the telnet server.
?	Displays help associated with this command.

Example

To send the **Are you there?** command to the telnet server, type:

```
sen ayt
```

Related links

- Command-Line Syntax Key

telnet: set

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets options. You can use the telnet unset command to turn off an option that was previously set.

Syntax

```
set [bsasdel] [crlf] [delasbs] [escape <char>] [localecho] [logfile
<filename>] [logging] [mode {console | stream}] [ntlm] [term {ansi | vt100 |
vt52 | vtnt}] [?]
```

Parameters

Parameter	Description
bsasdel	Sends **backspace** as a **delete**.
crlf	Sends CR & LF (0x0D, 0x 0A) when the **Enter** key is pressed. Known as **New line mode**.
delasbs	Sends **delete** as a **backspace**.
escape `<character>`	Sets the escape character used to enter the telnet client prompt. The escape character can be a single character, or it can be a combination of the **CTRL** key plus a character. To set a control-key combination, hold down the **CTRL** key while you type the character that you want to assign.
localecho	Turns on local echo.
logfile `<filename>`	Logs the current telnet session to the local file. Logging begins automatically when you set this option.
logging	Turns on logging. If no log file is set, an error message appears.
mode `{console | stream}`	Sets the operation mode.

Parameter	Description
ntlm	Turns on NTLM authentication.
term `{ansi | vt100 | vt52 | vtnt}`	Sets the terminal type.
?	Displays help for this command.

Remarks

- On non-English versions of telnet, the **codeset** `<option>` is available. **Codeset** `<option>` sets the current code set to an option, which can be any one of the following: **shift JIS**, **Japanese EUC**, **JIS Kanji**, **JIS Kanji (78)**, **DEC Kanji**, **NEC Kanji**. You should set the same code set on the remote computer.

Example

To set the log file and to begin logging to the local file *tnlog.txt*, type:

```
set logfile tnlog.txt
```

Related links

- Command-Line Syntax Key

telnet: status

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays status information.

Syntax

```
st[atus]
```

Example

To display status information, type:

```
st
```

Related links

- Command-Line Syntax Key

telnet: unset

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Turns off previously set options.

Syntax

```
u {bsasdel | crlf | delasbs | escape | localecho | logging | ntlm} [?]
```

Parameters

Parameter	Description
bsasdel	Sends **backspace** as a **backspace**.
crlf	Sends the **Enter** key as a CR. Also known as line feed mode.
delasbs	Sends **delete** as **delete**.
escape	Removes the escape character setting.
localecho	Turns off localecho.
logging	Turns off logging.
ntlm	Turns off NTLM authentication.
?	Displays help for this command.

Example

Turn off logging.

```
u logging
```

Related links

- Command-Line Syntax Key

tftp

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Transfers files to and from a remote computer, typically a computer running UNIX, that is running the Trivial File Transfer Protocol (tftp) service or daemon. tftp is typically used by embedded devices or systems that retrieve firmware, configuration information, or a system image during the boot process from a tftp server.

> [IMPORTANT] The tftp protocol doesn't support any authentication or encryption mechanism, and as such can introduce a security risk when present. Installing the tftp client is not recommended for systems connected to the Internet. A tftp server service is no longer provided by Microsoft for security reasons.

Syntax

```
tftp [-i] [<host>] [{get | put}] <source> [<destination>]
```

Parameters

Parameter	Description
-i	Specifies binary image transfer mode (also called octet mode). In binary image mode, the file is transferred in one-byte units. Use this mode when transferring binary files. If you don't use the **-i** option, the file is transferred in ASCII mode. This is the default transfer mode. This mode converts the end-of-line (EOL) characters to an appropriate format for the specified computer. Use this mode when transferring text files. If a file transfer is successful, the data transfer rate is displayed.
`<host>`	Specifies the local or remote computer.
get	Transfers the file *destination* on the remote computer to the file *source* on the local computer.

Parameter	Description
put	Transfers the file *source* on the local computer to the file *destination* on the remote computer. Because the tftp protocol doesn't support user authentication, the user must be logged onto the remote computer, and the files must be writable on the remote computer.
`<source>`	Specifies the file to transfer.
`<destination>`	Specifies where to transfer the file.

Examples

To copy the file *boot.img* from the remote computer *Host1*, type:

```
tftp  -i Host1 get boot.img
```

Related links

- Command-Line Syntax Key

time

Article • 02/03/2023

Displays or sets the system time. If used without parameters, **time** displays the current system time and prompts you to enter a new time.

> **Note**
>
> You must be an administrator to change the current time.

Syntax

```
time [/t | [<HH>[:<MM>[:<SS>]] [am|pm]]]
```

Parameters

Parameter	Description
`<HH>[:<MM>[:<SS>[.<NN>]]] [am | pm]`	Sets the system time to the new time specified, where *HH* is in hours (required), *MM* is in minutes, and *SS* is in seconds. *NN* can be used to specify hundredths of a second. You must separate values for *HH*, *MM*, and *SS* with colons (:). *SS* and *NN* must be separated with a period (.). If **am** or **pm** isn't specified, **time** uses the 24-hour format by default.
/t	Displays the current time without prompting you for a new time.
/?	Displays help at the command prompt.

Remarks

- Valid *HH* values are 0 through 24.
- Valid *MM* and *SS* values are 0 through 59.

Examples

If command extensions are enabled, to display the current system time, type:

```
time /t
```

To change the current system time to 5:30 PM, type either of the following:

```
time 17:30:00
time 5:30 pm
```

To display the current system time, followed by a prompt to enter a new time, type:

```
The current time is: 17:33:31.35
Enter the new time:
```

To keep the current time and return to the command prompt, press ENTER. To change the current time, type the new time and then press ENTER.

Related links

- Command-Line Syntax Key

timeout

Article • 02/03/2023

Pauses the command processor for the specified number of seconds. This command is typically used in batch files.

Syntax

```
timeout /t <timeoutinseconds> [/nobreak]
```

Parameters

Parameter	Description
/t `<timeoutinseconds>`	Specifies the decimal number of seconds (between -1 and 99999) to wait before the command processor continues processing. The value **-1** causes the computer to wait indefinitely for a keystroke.
/nobreak	Specifies to ignore user key strokes.
/?	Displays help at the command prompt.

Remarks

- A user keystroke resumes the command processor execution immediately, even if the timeout period has not expired.
- When used in conjunction with the resource kit's **Sleep** tool, **timeout** is similar to the **pause** command.

Examples

To pause the command processor for ten seconds, type:

```
timeout /t 10
```

To pause the command processor for 100 seconds and ignore any keystroke, type:

```
timeout /t 100 /nobreak
```

To pause the command processor indefinitely until a key is pressed, type:

```
timeout /t -1
```

Related links

- Command-Line Syntax Key

title

Article • 02/03/2023

Creates a title for the Command Prompt window.

Syntax

```
title [<string>]
```

Parameters

Parameter	Description
`<string>`	Specifies the text to appear as the title of the Command Prompt window.
/?	Displays help at the command prompt.

Remarks

- To create window title for batch programs, include the **title** command at the beginning of a batch program.
- After a window title is set, you can reset it only by using the **title** command.

Examples

To change the Command Prompt window title to *Updating Files* while the batch file executes the **copy** command, and then to return the title back to *Command Prompt*, type the following script:

```
@echo off
title Updating Files
copy \\server\share\*.xls c:\users\common\*.xls
echo Files Updated.
title Command Prompt
```

Related links

- Command-Line Syntax Key

tlntadmn

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Administers a local or remote computer that is running the telnet Server Service. If used without parameters, **tlntadmn** displays the current server settings.

This command requires you to log on to the local computer with administrative credentials. To administer a remote computer, you must also provide administrative credentials for the remote computer. You can do so by logging on to the local computer with an account that has administrative credentials for both the local computer and the remote computer. If you can't use this method, you can use the **-u** and **-p** parameters to provide administrative credentials for the remote computer.

Syntax

```
tlntadmn [<computername>] [-u <username>] [-p <password>] [{start | stop | pause | continue}] [-s {<sessionID> | all}] [-k {<sessionID> | all}] [-m {<sessionID> | all}  <message>] [config [dom = <domain>] [ctrlakeymap = {yes | no}] [timeout = <hh>:<mm>:<ss>] [timeoutactive = {yes | no}] [maxfail = <attempts>] [maxconn = <connections>] [port = <number>] [sec {+ | -}NTLM {+ | -}passwd] [mode = {console | stream}]] [-?]
```

Parameters

Parameter	Description
`<computername>`	Specifies the name of the server to connect to. The default is the local computer.
-u `<username>` -p `<password>`	Specifies administrative credentials for a remote server that you want to administer. This parameter is required if you want to administer a remote server to which you are not logged on with administrative credentials.
start	starts the telnet Server Service.
stop	Stops the telnet Server Service
pause	Pauses the telnet Server Service. No new connections will be accepted.

Parameter	Description
continue	Resumes the telnet Server Service.
-s `{<sessionID> | all}`	Displays active telnet sessions.
-k `{<sessionID> | all}`	Ends telnet sessions. Type the Session ID to end a specific session, or type all to end all the sessions.
-m `{<sessionID> | all} <message>`	Sends a message to one or more sessions. Type the session ID to send a message to a specific session, or type all to send a message to all sessions. type the message that you want to send between quotation marks.
config dom = `<domain>`	Configures the default domain for the server.
config ctrlakeymap = `{yes | no}`	Specifies if you want the telnet server to interpret CTRL+A as ALT. Type **yes** to map the shortcut key, or type **no** to prevent the mapping.
config timeout = `<hh>:<mm>:<ss>`	Sets the time-out period in hours, minutes, and seconds.
config timeoutactive = `{yes | no}`	Enables the idle session timeout.
config maxfail = `<attempts>`	Sets the maximum number of failed logon attempts before disconnecting.
config maxconn = `<connections>`	Sets the maximum number of connections.
config port = `<number>`	Sets the telnet port. You must specify the port with an integer smaller than 1024.
config sec `{+ | -}NTLM {+ | -}passwd`	Specifies whether you want to use NTLM, a password, or both to authenticate logon attempts. To use a particular type of authentication, type a plus sign (+) before that type of authentication. To prevent using a particular type of authentication, type a minus sign (-) before that type of authentication.
config mode = `{console | stream}`	Specifies the mode of operation.
-?	Displays help at the command prompt.

Examples

To configure the idle session timeout to 30 minutes, type:

```
tlntadmn config timeout=0:30:0
```

To display active telnet sessions, type:

```
tlntadmn -s
```

Related links

- Command-Line Syntax Key
- telnet Operations Guide

tpmtool

Article • 02/03/2023

This utility can be used to get information about the Trusted Platform Module (TPM).

> **ⓘ Important**
>
> Some information may relate to the pre-released product, which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

Syntax

```
tpmtool /parameter [<arguments>]
```

Parameters

Parameter	Description
getdeviceinformation	Displays the basic information of the TPM. See the Win32_Tpm::IsReadyInformation method parameters article for details about the information flag values.
gatherlogs [output directory path]	Collects TPM logs and places them in the specified directory. If that directory doesn't exist, it's created. By default, the log files are placed in the current directory. The possible files generated are: • TpmEvents.evtx • TpmInformation.txt • SRTMBoot.dat • SRTMResume.dat • DRTMBoot.dat • DRTMResume.dat
drivertracing `[start | stop]`	Starts or stops collecting TPM driver traces. The trace log, *TPMTRACE.etl*, is created and placed in the current directory.
/?	Displays help at the command prompt.

Examples

To display the basic information of the TPM, type:

```
tpmtool getdeviceinformation
```

To collect TPM logs and place them in the current directory, type:

```
tpmtool gatherlogs
```

To collect TPM logs and place them in `C:\Users\Public`, type:

```
tpmtool gatherlogs C:\Users\Public
```

To collect TPM driver traces, type:

```
tpmtool drivertracing start
# Run scenario
tpmtool drivertracing stop
```

Related links

- Command-Line Syntax Key
- COM Error Codes (TPM, PLA, FVE)

tpmvscmgr

Article • 02/03/2023

The tpmvscmgr command-line tool allows users with Administrative credentials to create and delete TPM virtual smart cards on a computer.

Syntax

```
tpmvscmgr create [/name] [/adminkey DEFAULT | PROMPT | RANDOM] [/PIN DEFAULT
| PROMPT] [/PUK DEFAULT | PROMPT] [/generate] [/machine] [/?]
```

```
tpmvscmgr destroy [/instance <instanceID>] [/?]
```

Create parameters

The **Create** command sets up new virtual smart cards on the user's system. It also returns the instance ID of the newly-created card for later reference, if deletion is required. The instance ID is in the format **ROOT\SMARTCARDREADER\000n** where **n** starts from 0 and is increased by 1 each time you create a new virtual smart card.

Parameter	Description
/name	Required. Indicates the name of the new virtual smart card.
/adminkey	Indicates the desired administrator key that can be used to reset the PIN of the card if the user forgets the PIN. This can include: • **DEFAULT** - Specifies the default value of *010203040506070801020304050607080102030405060708*. • **PROMPT** - Prompts the user to enter a value for the administrator key. • **RANDOM** - Results in a random setting for the administrator key for a card that is not returned to the user. This creates a card that might not be manageable by using smart card management tools. When using the RANDOM option, the administrator key must be entered as 48 hexadecimal characters.

Parameter	Description
/PIN	Indicates desired user PIN value. • **DEFAULT** - Specifies the default PIN of 12345678. • **PROMPT** - Prompts the user to enter a PIN at the command line. The PIN must be a minimum of eight characters, and it can contain numerals, characters, and special characters.
/PUK	Indicates the desired PIN Unlock Key (PUK) value. The PUK value must be a minimum of eight characters, and it can contain numerals, characters, and special characters. If the parameter is omitted, the card is created without a PUK. The options include: • **DEFAULT** - Specifies the default PUK of *12345678*. • **PROMPT** - Prompts to the user to enter a PUK at the command line.
/generate	Generates the files in storage that are necessary for the virtual smart card to function. If you don't use the **/generate** parameter, it's like you created the card without the underlying file system. A card without a file system can be managed only by a smart card management system such as Microsoft Configuration Manager.
/machine	Allows you to specify the name of a remote computer on which the virtual smart card can be created. This can be used in a domain environment only, and it relies on DCOM. For the command to succeed in creating a virtual smart card on a different computer, the user running this command must be a member in the local administrators group on the remote computer.
/?	Displays Help for this command.

Destroy parameters

The **Destroy** command securely deletes a virtual smart card from the user's computer.

> ⚠ **Warning**
>
> If a virtual smart card is deleted, it cannot be recovered.

Parameter	Description
/instance	Specifies the instance ID of the virtual smart card to be removed. The instanceID was generated as output by tpmvscmgr.exe when the card was created. The **/instance** parameter is a required field for the **Destroy** command.
/?	Displays help at the command prompt.

Remarks

- For alphanumeric inputs, the full 127 character ASCII set is allowed.

Examples

To create a virtual smart card that can be later managed by a smart card management tool launched from another computer, type:

```
tpmvscmgr.exe create /name VirtualSmartCardForCorpAccess /AdminKey DEFAULT
/PIN PROMPT
```

Alternatively, instead of using a default administrator key, you can create an administrator key at the command line. The following command shows how to create an administrator key.

```
tpmvscmgr.exe create /name VirtualSmartCardForCorpAccess /AdminKey PROMPT
/PIN PROMPT
```

To create an unmanaged virtual smart card that can be used to enroll certificates, type:

```
tpmvscmgr.exe create /name VirtualSmartCardForCorpAccess /AdminKey RANDOM
/PIN PROMPT /generate
```

A virtual smart card is created with a randomized administrator key. The key is automatically discarded after the card is created. This means that if the user forgets the PIN or wants to the change the PIN, the user needs to delete the card and create it again.

To delete the card, type:

```
tpmvscmgr.exe destroy /instance <instance ID>
```

Where `<instanceID>` is the value printed on the screen when the user created the card. Specifically, for the first card created, the instance ID is

ROOT\SMARTCARDREADER\0000.

Related links

- Command-Line Syntax Key

tracerpt

Article • 02/03/2023

The **tracerpt** command parses Event Trace Logs, log files generated by Performance Monitor, and real-time Event Trace providers. It also generates dump files, report files, and report schemas.

Syntax

```
tracerpt <[-l] <value [value [...]]>|-rt <session_name [session_name
[...]]>> [options]
```

Parameters

Parameters	Description
-config `<filename>`	Specifies which settings file to load, which includes your command options.
-y	Specifies to answer **yes** to all questions, without prompting.
-f `<XML | HTML>`	Specifies the report file format.
-of `<CSV | EVTX | XML>`	Specifies the dump file format. The default is **XML*.
-df `<filename>`	Specifies to create a Microsoft-specific counting/reporting schema file.
-int `<filename>`	Specifies to dump the interpreted event structure to the specified file.
-rts	Specifies to add the report raw timestamp in the event trace header. Can only be used with **-o**. It's not supported with **-report** or **-summary**.
-tmf `<filename>`	Specifies which Trace Message Format definition file to use.
-tp `<value>`	Specifies the TMF file search path. Multiple paths may be used, separated by a semicolon (;).
-i `<value>`	Specifies the provider image path. The matching PDB will be located in the Symbol Server. Multiple paths can be used, separated by a semicolon (;).
-pdb `<value>`	Specifies the symbol server path. Multiple paths can be used, separated by a semicolon (;).

Parameters	Description
-gmt	Specifies to convert WPP payload timestamps to Greenwich Mean Time.
-rl `<value>`	Specifies the System Report Level from 1 to 5. Default is *1*.
-summary [filename]	Specifies to create a summary report text file. The filename, if not specified, is *summary.txt*.
-o [filename]	Specifies to create a text output file. The filename, if not specified, is *dumpfile.xml*.
-report [filename]	Specifies to create a text output report file. The filename, if not specified, is *workload.xml*.
-lr	Specifies to be less restrictive. This uses best efforts for events that don't match the events schema.
-export [filename]	Specifies to create an Event Schema export file. The filename, if not specified, is *schema.man*.
[-l] `<value [value […]]>`	Specifies the Event Trace log file to process.
-rt `<session_name [session_name […]]>`	Specifies the Real-time Event Trace Session data sources.
-?	Displays help at the command prompt.

Examples

To create a report based on the two event logs *logfile1.etl* and *logfile2.etl*, and to create the dump file *logdump.xml* in *XML* format, type:

```
tracerpt logfile1.etl logfile2.etl -o logdump.xml -of XML
```

To create a report based on the event log *logfile.etl*, to create the dump file *logdmp.xml* in XML format, to use best efforts to identify events not in the schema, and to produce a summary report file *logdump.txt* and a report file, *logrpt.xml*, type:

```
tracerpt logfile.etl -o logdmp.xml -of XML -lr -summary logdmp.txt -report
logrpt.xml
```

To use the two event logs *logfile1.etl* and *logfile2.etl* to produce a dump file, and to report file with the default filenames, type:

```
tracerpt logfile1.etl logfile2.etl -o -report
```

To use the event log *logfile.etl* and the performance log *counterfile.blg* to produce the report file *logrpt.xml* and the Microsoft-specific XML schema file *schema.xml*, type:

```
tracerpt logfile.etl counterfile.blg -report logrpt.xml -df schema.xml
```

To read the real-time Event Trace Session NT Kernel Logger and to produce the dump file *logfile.csv* in *CSV* format, type:

```
tracerpt -rt NT Kernel Logger -o logfile.csv -of CSV
```

Related links

- Command-Line Syntax Key

tracert

Article • 09/28/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This diagnostic tool determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to live (TTL) field values. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP time Exceeded message to the source computer.

This command determines the path by sending the first echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the **/h** parameter.

The path is determined by examining the ICMP time Exceeded messages returned by intermediate routers and the echo Reply message returned by the destination. However, some routers don't return time Exceeded messages for packets with expired TTL values and are invisible to the **tracert** command. In this case, a row of asterisks (`*`) is displayed for that hop. The path displayed is the list of near/side router interfaces of the routers in the path between a source host and a destination. The near/side interface is the interface of the router that is closest to the sending host in the path.

> **Important**
>
> This command is available only if the Internet Protocol (TCP/IP) protocol is installed as a component in the properties of a network adapter in Network Connections.
>
> To trace a path and provide network latency and packet loss for each router and link in the path, use the **pathping command** command.

Syntax

```
tracert [/d] [/h <maximumhops>] [/j <hostlist>] [/w <timeout>] [/R] [/S
```

```
<srcaddr>] [/4][/6] <targetname>
```

Parameters

Parameter	Description
/d	Stops attempts to resolve the IP addresses of intermediate routers to their names. This can speed up the return of results.
/h `<maximumhops>`	Specifies the maximum number of hops in the path to search for the target (destination). The default is 30 hops.
/j `<hostlist>`	Specifies that echo Request messages use the Loose Source Route option in the IP header with the set of intermediate destinations specified in `<hostlist>`. With loose source routing, successive intermediate destinations can be separated by one or multiple routers. The maximum number of addresses or names in the list is *9*. The `<hostlist>` is a series of IP addresses (in dotted decimal notation) separated by spaces. Use this parameter only when tracing IPv4 addresses.
/w `<timeout>`	Specifies the amount of time in milliseconds to wait for the ICMP time Exceeded or echo Reply message corresponding to a given echo Request message to be received. If not received within the time-out, an asterisk (`*`) is displayed. The default time-out is 4000 (4 seconds).
/R	Specifies that the IPv6 Routing extension header be used to send an echo Request message to the local host, using the destination as an intermediate destination and testing the reverse route.
/S `<srcaddr>`	Specifies the source address to use in the echo Request messages. Use this parameter only when tracing IPv6 addresses.
/4	Specifies that tracert.exe can use only IPv4 for this trace.
/6	Specifies that tracert.exe can use only IPv6 for this trace.
`<targetname>`	Specifies the destination, identified either by IP address or host name.
/?	Displays help at the command prompt.

Examples

To trace the path to the host named `www.microsoft.com`, type:

```

tracert www.microsoft.com
```

Here's an example output:

Output

```
Tracing route to e13678.dscb.akamaiedge.net [23.216.93.114]
over a maximum of 30 hops:

 1     1 ms     1 ms    <1 ms  <devicename>.mshome.net [172.26.96.1]
 2    11 ms    13 ms     6 ms  192.168.191.20
 3    20 ms    11 ms    18 ms  192.168.1.1
 4    44 ms    41 ms    35 ms  10.228.0.1
 5    32 ms    31 ms    46 ms  10.41.0.49
 6    36 ms    39 ms    30 ms  10.41.0.221
 7    35 ms    36 ms    39 ms  10.41.0.225
 8    54 ms    45 ms    50 ms  204.111.0.147
 9    50 ms    52 ms    47 ms  ae-39.a02.atlnga05.us.bb.gin.ntt.net
[128.241.219.117]
10    53 ms    51 ms    61 ms  ae-5.r24.atlnga05.us.bb.gin.ntt.net
[129.250.4.192]
11    64 ms    45 ms    44 ms  ae-0.a03.atlnga05.us.bb.gin.ntt.net
[129.250.2.20]
12    49 ms    67 ms    46 ms  ae-0.akamai-onnet.atlnga05.us.bb.gin.ntt.net
[128.241.1.122]
13    67 ms   287 ms     *
ae20.r03.border101.atl02.fab.netarch.akamai.com [23.203.144.21]
14     *        *        *     Request timed out.
15     *        *        *     Request timed out.
16     *        *        *     Request timed out.
17   204 ms    58 ms    51 ms  a23-216-93-
114.deploy.static.akamaitechnologies.com [23.216.93.114]

Trace complete.
```

The beginning column displays the hop number starting from 1 and incrementing with each hop along the route from your device to the destination. Each hop represents an intermediate device, such as a router, that the packet passes through while traveling to the final destination.

The three center columns display the round-trip time in milliseconds (ms) for a packet to travel from your device to the router, at that specific hop, and back to your device. It's known as the "ping time" or "ping latency" and measures the delay in milliseconds for data to travel to the router and return. Network latency can be affected by factors such as network congestion, the quality of network links, and the distance between hops.

The end column displays either the IP address or the hostname of the router or intermediate device at that specific hop in the network path. In most cases, you'll see the IP address, but if reverse DNS lookup is successful, it displays the hostnames, which can help identify routers by name.

To trace the path to the host named `www.microsoft.com` and prevent the resolution of each IP address to its name, type:

```
tracert /d www.microsoft.com
```

To trace the path to the host named `www.microsoft.com` and use the loose source route *10.12.0.1/10.29.3.1/10.1.44.1*, type:

```
tracert /j 10.12.0.1 10.29.3.1 10.1.44.1 www.microsoft.com
```

Related links

- Command-Line Syntax Key
- pathping command

tree

Article • 02/03/2023

Displays the directory structure of a path or of the disk in a drive graphically. The structure displayed by this command depends upon the parameters that you specify at the command prompt. If you don't specify a drive or path, this command displays the tree structure beginning with the current directory of the current drive.

Syntax

```
tree [<drive>:][<path>] [/f] [/a]
```

Parameters

Parameter	Description
`<drive>:`	Specifies the drive that contains the disk for which you want to display the directory structure.
`<path>`	Specifies the directory for which you want to display the directory structure.
/f	Displays the names of the files in each directory.
/a	Specifies to use text characters instead of graphic characters to show the lines that link subdirectories.
/?	Displays help at the command prompt.

Examples

To display the names of all the subdirectories on the disk in your current drive, type:

```
tree \
```

To display, one screen at a time, the files in all the directories on drive C, type:

```
```

```
tree c:\ /f | more
```

To print a list of all the directories on drive C to a file, type:

```

tree c:\ /f > <driveletter>:\<filepath>\filename.txt
```

Related links

- Command-Line Syntax Key

tscon

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Connects to another session on a Remote Desktop Session Host server.

> **ⓘ Important**
>
> You must have **Full Control access** permission or **Connect special access** permission to connect to another session.

> **ⓘ Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
tscon {<sessionID> | <sessionname>} [/dest:<sessionname>] [/password:<pw> | /password:*] [/v]
```

Parameters

Parameter	Description
`<sessionID>`	Specifies the ID of the session to which you want to connect. If you use the optional `/dest:<sessionname>` parameter, you can also specify the name of the current session.
`<sessionname>`	Specifies the name of the session to which you want to connect.
/dest:`<sessionname>`	Specifies the name of the current session. This session will disconnect when you connect to the new session. You can also use this parameter to connect the session of another user to a different session.

Parameter	Description
/password:`<pw>`	Specifies the password of the user who owns the session to which you want to connect. This password is required when the connecting user does not own the session.
/password:`*`	Prompts for the password of the user who owns the session to which you want to connect.
/v	Displays information about the actions being performed.
/?	Displays help at the command prompt.

Remarks

- This command fails if you don't specify a password in the **/password** parameter, and the target session belongs to a user other than the current one.
- You can't connect to the console session.

Examples

To connect to *Session 12* on the current Remote Desktop Services Session Host server, and to disconnect the current session, type:

```
tscon 12
```

To connect to *Session 23* on the current Remote Desktop Services Session Host server using the password *mypass*, and to disconnect the current session, type:

```
tscon 23 /password:mypass
```

To connect the session named *TERM03* to the session named *TERM05*, and then to disconnect session *TERM05*, type:

```
tscon TERM03 /v /dest:TERM05
```

Related links

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

tsdiscon

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Disconnects a session from a Remote Desktop Session Host server. If you don't specify a session ID or session name, this command disconnects the current session.

> **ⓘ Important**
>
> You must have **Full Control access** permission or **Disconnect special access** permission to disconnect another user from a session.

> **ⓘ Note**
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
tsdiscon [<sessionID> | <sessionname>] [/server:<servername>] [/v]
```

Parameters

Parameter	Description
`<sessionID>`	Specifies the ID of the session to disconnect.
`<sessionname>`	Specifies the name of the session to disconnect.
/server:`<servername>`	Specifies the terminal server that contains the session that you want to disconnect. Otherwise, the current Remote Desktop Session Host server is used. This parameter is required only if you run the **tsdiscon** command from a remote server.
/v	Displays information about the actions being performed.

Parameter	Description
/?	Displays help at the command prompt.

Remarks

- Any applications running when you disconnected the session are automatically running when you reconnect to that session with no loss of data. You can use the reset session command to end the running applications of the disconnected session, but this may result in loss of data at the session.
- The console session can't be disconnected.

Examples

To disconnect the current session, type:

```
tsdiscon
```

To disconnect *Session 10*, type:

```
tsdiscon 10
```

To disconnect the session named *TERM04*, type:

```
tsdiscon TERM04
```

Related links

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference
- reset session command

tsecimp

Article • 02/03/2023

Imports assignment information from an Extensible Markup Language (XML) file into the TAPI server security file (Tsec.ini). You can also use this command to display the list of TAPI providers and the lines devices associated with each of them, validate the structure of the XML file without importing the contents, and check domain membership.

Syntax

```
tsecimp /f <filename> [{/v | /u}]
tsecimp /d
```

Parameters

Parameter	Description
/f `<filename>`	Required. Specifies the name of the XML file that contains the assignment information that you want to import.
/v	Validates the structure of the XML file without importing the information into the Tsec.ini file.
/u	Checks whether each user is a member of the domain specified in the XML file. The computer on which you use this parameter must be connected to the network. This parameter might significantly slow performance if you are processing a large amount of user assignment information.
/d	Displays a list of installed telephony providers. For each telephony provider, the associated line devices are listed, as well as the addresses and users associated with each line device.
/?	Displays help at the command prompt.

Remarks

The XML file from which you want to import assignment information must follow the structure described below:

```
XML
```

```
<UserList>
  <User>
    <LineList>
      <Line>
```

- `<Userlist element>` - The top element of the XML file.
- `<User element>` - Contains information about a user who is a member of a domain. Each user might be assigned one or more line devices. Additionally, each **User** element might have an attribute named **NoMerge**. When this attribute is specified, all current line device assignments for the user are removed before new ones are made. You can use this attribute to easily remove unwanted user assignments. By default, this attribute is not set. The **User** element must contain a single **DomainUserName** element, which specifies the domain and user name of the user. The **User** element might also contain one **FriendlyName** element, which specifies a friendly name for the user. The **User** element might contain one **LineList** element. If a **LineList** element is not present, all line devices for this user are removed.
- `<LineList element>` - Contains information about each line or device that might be assigned to the user. Each **LineList** element can contain more than one **Line** element.
- `<Line element>` - Specifies a line device. You must identify each line device by adding either an **Address** element or a **PermanentID** element under the **Line** element. For each **Line** element, you can set the **Remove** attribute. If you set this attribute, the user is no longer assigned that line device. If this attribute is not set, the user gains access to that line device. No error is given if the line device is not available to the user.

Sample output for /d parameter

This sample output appears after running the **/d** parameter to display the current TAPI configuration. For each telephony provider, the associated line devices are listed, as well as the addresses and users associated with each line device.

```
NDIS Proxy TAPI Service Provider
  Line: WAN Miniport (L2TP)
    Permanent ID: 12345678910

NDIS Proxy TAPI Service Provider
  Line: LPT1DOMAIN1\User1
    Permanent ID: 12345678910
```

```
Microsoft H.323 Telephony Service Provider
  Line: H323 Line
    Permanent ID: 123456
    Addresses:
      BLDG1-TAPI32
```

Examples

To remove all line devices assigned to *User1*, type:

XML

```
<UserList>
  <User NoMerge=1>
    <DomainUser>domain1\user1</DomainUser>
  </User>
</UserList>
```

To remove all line devices assigned to *User1*, before assigning one line with address *99999*, type:

XML

```
<UserList>
  <User NoMerge=1>
  <DomainUser>domain1\user1</DomainUser>
  <FriendlyName>User1</FriendlyName>
  <LineList>
    <Line>
      <Address>99999</Address>
    </Line>
  </LineList>
  </User>
</UserList>
```

In this example, *User1* has no other line devices assigned, regardless of whether any line devices were assigned previously.

To add one line device for *User1*, without deleting any previously assigned line devices, type:

XML

```
<UserList>
  <User>
  <DomainUser>domain1\user1</DomainUser>
```

```
  <FriendlyName>User1</FriendlyName>
  <LineList>
    <Line>
      <Address>99999</Address>
    </Line>
  </LineList>
  </User>
</UserList>
```

To add line address *99999* and to remove line address *88888* from *User1's* access, type:

XML

```
<UserList>
  <User>
  <DomainUser>domain1\user1</DomainUser>
  <FriendlyName>User1</FriendlyName>
  <LineList>
    <Line>
      <Address>99999</Address>
    </Line>
    <Line Remove=1>
      <Address>88888</Address>
    </Line>
  </LineList>
  </User>
</UserList>
```

To add permanent device *1000* and to remove line *88888* from *User1's* access, type:

XML

```
<UserList>
  <User>
  <DomainUser>domain1\user1</DomainUser>
  <FriendlyName>User1</FriendlyName>
  <LineList>
    <Line>
    <PermanentID>1000</PermanentID>
    </Line>
    <Line Remove=1>
    <Address>88888</Address>
    </Line>
  </LineList>
  </User>
</UserList>
```

Related links

- Command-Line Syntax Key
- Command shell overview

tskill

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Ends a process running in a session on a Remote Desktop Session Host server.

> **Note**
>
> You can use this command to end only those processes that belong to you, unless you are an administrator. Administrators have full access to all **tskill** functions and can end processes that are running in other user sessions.
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
tskill {<processID> | <processname>} [/server:<servername>] [/id:<sessionID>
| /a] [/v]
```

Parameters

Parameter	Description
`<processID>`	Specifies the ID of the process that you want to end.
`<processname>`	Specifies the name of the process that you want to end. This parameter can include wildcard characters.
/server:`<servername>`	Specifies the terminal server that contains the process that you want to end. If **/server** isn't specified, the current Remote Desktop Session Host server is used.
/id:`<sessionID>`	Ends the process that is running in the specified session.
/a	Ends the process that is running in all sessions.

Parameter	Description
/v	Displays information about the actions being performed.
/?	Displays help at the command prompt.

Remarks

- When all processes that are running in a session end, the session also ends.
- If you use the `<processname>` and the `/server:<servername>` parameters, you must also specify either the `/id:<sessionID>` or the **/a** parameter.

Examples

To end process 6543, type:

```
tskill 6543
```

To end the process explorer running on session 5, type:

```
tskill explorer /id:5
```

Related links

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

tsprof

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies the Remote Desktop Services user configuration information from one user to another. The Remote Desktop Services user configuration information appears in the Remote Desktop Services extensions to Local Users and Groups and active directory Users and computers.

> **Note**
>
> You can also use the **tsprof command** to set the profile path for a user.
>
> To find out what's new in the latest version, see **What's New in Remote Desktop Services in Windows Server**.

Syntax

```
tsprof /update {/domain:<Domainname> | /local} /profile:<path> <username>
tsprof /copy {/domain:<Domainname> | /local} [/profile:<path>] <src_user>
<dest_user>
tsprof /q {/domain:<Domainname> | /local} <username>
```

Parameters

Parameter	Description
/update	Updates profile path information for `<username>` in domain `<domainname>` to `<profilepath>`.
/domain:`<Domainname>`	Specifies the name of the domain in which the operation is applied.
/local	Applies the operation only to local user accounts.
/profile:`<path>`	Specifies the profile path as displayed in the Remote Desktop Services extensions in Local Users and Groups and active directory Users and computers.

Parameter	Description
`<username>`	Specifies the name of the user for whom you want to update or query the server profile path.
/copy	Copies user configuration information from `<src_user>` to `<dest_user>` and updates the profile path information for `<dest_user>` to `<profilepath>`. Both `<src_user>` and `<dest_user>` must either be local or must be in domain `<domainname>`.
`<src_user>`	Specifies the name of the user from whom you want to copy the user configuration information. Also known as the source user.
`<dest_user>`	Specifies the name of the user to whom you want to copy the user configuration information. Also known as the destination user.
/q	Displays the current profile path of the user for whom you want to query the server profile path.
/?	Displays help at the command prompt.

Examples

To copy user configuration information from *LocalUser1* to *LocalUser2*, type:

```
tsprof /copy /local LocalUser1 LocalUser2
```

To set the Remote Desktop Services profile path for *LocalUser1* to a directory called *c:\profiles*, type:

```
tsprof /update /local /profile:c:\profiles LocalUser1
```

Related links

- Command-Line Syntax Key
- Remote Desktop Services (Terminal Services) Command Reference

type

Article • 02/03/2023

In the Windows Command shell, **type** is a built in command which displays the contents of a text file. Use the **type** command to view a text file without modifying it.

In PowerShell, **type** is a built-in alias to the Get-Content cmdlet, which also displays the contents of a file, but using a different syntax.

Syntax

```
type [<drive>:][<path>]<filename>
```

Parameters

Parameter	Description
`[<drive>:][<path>]<filename>`	Specifies the location and name of the file or files that you want to view. If your `<filename>` contains spaces, you must enclose it in quotation marks (for example, "Filename Containing Spaces.txt"). You can also add multiple filenames by adding spaces between them.
/?	Displays help at the command prompt.

Remarks

- If you display a binary file or a file that is created by a program, you may see strange characters on the screen, including formfeed characters and escape-sequence symbols. These characters represent control codes that are used in the binary file. In general, avoid using the **type** command to display binary files.

Examples

To display the contents of a file named *holiday.mar*, type:

```
type holiday.mar
```

To display the contents of a lengthy file named *holiday.mar* one screen at a time, type:

```
type holiday.mar | more
```

Related links

- Command-Line Syntax Key

typeperf

Article • 06/16/2023

The **typeperf** command writes performance data to the command window or to a log file. To stop **typeperf**, press CTRL+C.

Syntax

```
typeperf <counter [counter ...]> [options]
typeperf -cf <filename> [options]
typeperf -q [object] [options]
typeperf -qx [object] [options]
```

Parameters

Parameter	Description
`<counter [counter [...]]>`	Specifies performance counters to monitor. The `<counter>` parameter is the full name of a performance counter in \Computer\Object(Instance)\Counter format, such as `\\Server1\Processor(0)\% User Time`.

Options

Option	Description
-f `<CSV | TSV | BIN | SQL>`	Specifies the output file format. The default is CSV.
-cf `<filename>`	Specifies a file containing a list of performance counters to monitor, with one counter per line.
-si `<[[hh:]mm:]ss>`	Specifies the sample interval. The default is one second.
-o `<filename>`	Specifies the path for the output file, or the SQL database. The default is STDOUT (written to the command window).
-q `[object]`	Display a list of installed counters (no instances). To list counters for one object, include the object name.

Option	Description
-qx `[object]`	Display a list of installed counters with instances. To list counters for one object, include the object name.
-sc `<samples>`	Specifies the number of samples to collect. The default is to collect data until CTRL+C is pressed.
-config `<filename>`	Specifies a settings file containing command options.
-s `<computer_name>`	Specifies a remote computer to monitor if no computer is specified in the counter path.
-y	Answer *yes* to all questions without prompting.
/?	Displays help at the command prompt.

Examples

To write the values for the local computer's performance counter `\Processor(_Total)\% Processor Time` to the command window at a default sample interval of 1 second until CTRL+C is pressed, type:

```
typeperf \Processor(_Total)\% Processor Time
```

To write the values for the list of counters in the file *counters.txt* to the tab-delimited file *domain2.tsv* at a sample interval of 5 seconds until 50 samples have been collected, type:

```
typeperf -cf counters.txt -si 5 -sc 50 -f TSV -o domain2.tsv
```

To query installed counters with instances for the counter object *PhysicalDisk* and writes the resulting list to the file *counters.txt*, type:

```
typeperf -qx PhysicalDisk -o counters.txt
```

Related links

- Command-Line Syntax Key

tzutil

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the Windows Time Zone utility.

Syntax

```
tzutil [/?] [/g] [/s <timezoneID>[_dstoff]] [/l]
```

Parameters

Parameter	Description
/g	Displays the current time zone ID.
/s `<timezoneID>` `[_dstoff]`	Sets the current time zone using the specified time zone ID. The **_dstoff** suffix disables Daylight Saving time adjustments for the time zone (where applicable). Your value must be surrounded by quotes.
/l	Lists all valid time zone IDs and display names. The output appears as: • `<display name>` • `<time zone ID>`
/?	Displays help at the command prompt.

Remarks

An exit code of **0** indicates the command completed successfully.

Examples

To display the current time zone ID, type:

```
```

```
tzutil /g
```

To set the current time zone to Pacific Standard time, type:

```

tzutil /s "Pacific Standard time"
```

To set the current time zone to Pacific Standard time and disable Daylight Saving time adjustments, type:

```

tzutil /s "Pacific Standard time_dstoff"
```

Related links

- Command-Line Syntax Key

unlodctr

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes **Performance counter names** and **Explain text** for a service or device driver from the system registry.

> **⚠ Warning**
>
> Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

Syntax

```
unlodctr <drivername>
```

Parameters

Parameter	Description
`<drivername>`	Removes the **Performance counter name** settings and **Explain text** for driver or service `<drivername>` from the Windows Server registry. If your `<drivername>` includes spaces, you must use quotation marks around the text, for example "Driver name".
/?	Displays help at the command prompt.

Examples

To remove the current **Performance counter names** and **Explain text** for the Simple Mail Transfer Protocol (SMTP) service, type:

```
unlodctr SMTPSVC
```

Related links

- Command-Line Syntax Key

ver

Article • 02/03/2023

Displays the operating system version number. This command is supported in the Windows Command prompt (Cmd.exe), but not in any version of PowerShell.

Syntax

```
ver
```

Parameters

Parameter	Description
/?	Displays help at the command prompt.

Examples

To obtain the version number of the operating system from the Command shell (cmd.exe), type:

```
ver
```

If you want to get the operating system version number through Windows PowerShell, type:

```PowerShell
$PSVersionTable.BuildVersion
```

If you want to get the operating system version number through PowerShell 7.x.x, type:

```PowerShell
$PSVersionTable.OS
```

Related links

- Command-Line Syntax Key

verifier

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Driver Verifier monitors Windows kernel-mode drivers and graphics drivers to detect illegal function calls or actions that might corrupt the system. Driver Verifier can subject Windows drivers to a variety of stresses and tests to find improper behavior. You can configure which tests to run, which allows you to put a driver through heavy stress loads or through more streamlined testing. You can also run Driver Verifier on multiple drivers simultaneously, or on one driver at a time.

> **ⓘ Important**
>
> You must be in the Administrators group on the computer to use Driver Verifier. Running Driver Verifier can cause the computer to crash, so you should only run this utility on computers used for testing and debugging.

Syntax

```
verifier /standard /all
verifier /standard /driver NAME [NAME ...]
verifier /flags <options> /all
verifier /flags <options> /driver NAME [NAME ...]
verifier /rules [OPTION ...]
verifier /query
verifier /querysettings
verifier /bootmode [persistent | disableafterfail | oneboot]
verifier /reset
verifier /faults [Probability] [PoolTags] [Applications] [DelayMins]
verifier /faultssystematic [OPTION ...]
verifier /log LOG_FILE_NAME [/interval SECONDS]
verifier /volatile /flags <options>
verifier /volatile /adddriver NAME [NAME ...]
verifier /volatile /removedriver NAME [NAME ...]
verifier /volatile /faults [Probability] [PoolTags] [Applications]
[DelayMins]
verifier /domain <types> <options> /driver ... [/logging | /livedump]
verifier /logging
verifier /livedump
```

```
verifier /?
verifier /help
```

Parameters

Parameter	Description
/all	Directs the Driver Verifier utility to verify all installed drivers after the next boot.
/bootmode `[persistent | disableafterfail | oneboot | resetonunusualshutdown]`	Controls whether the settings for the Driver Verifier utility are enabled after a reboot. To set or change this option, you must reboot the computer. The following modes are available: • **persistent** - Ensures that the Driver Verifier settings persist (stay in effect) over many reboots. This is the default setting. • **disableafterfail** - If Windows fails to start, this setting disables the Driver Verifier utility for subsequent reboots. • **oneboot** - Only enables the Driver Verifier settings for the next time the computer starts. The Driver Verifier utility is disabled for subsequent reboots. • **resetonunusualshutdown** - The Driver Verifier utility will persist until an unusual shutdown occurs. Its abbrevation, 'rous', can be used.
/driver `<driverlist>`	Specifies one or more drivers that will be verified. The **driverlist** parameter is a list of drivers by binary name, such as *driver.sys*. Use a space to separate each driver name. Wildcard values, such as `n*.sys`, aren't supported.
/driver.exclude `<driverlist>`	Specifies one or more drivers that will be excluded from verification. This parameter is applicable only if all drivers are selected for verification. The **driverlist** parameter is a list of drivers by binary name, such as *driver.sys*. Use a space to separate each driver name. Wildcard values, such as `n*.sys`, aren't supported.

Parameter	Description
/faults	Enables the **Low Resources Simulation** feature in the Driver Verifier utility. You can use **/faults** in place of `/flags 0x4`. However, you can't use `/flags 0x4` with the **/faults** subparameters. You can use the following subparameters of the /faults parameter to configure the Low Resources Simulation: • **Probability** - Specifies the probability that the Driver Verifier utility will fail a given allocation. Type a number (in decimal or hexadecimal) to represent the number of chances in 10,000 that the Driver Verifier utility will fail the allocation. The default value, 600, means 600/10000 or 6%. • **Pool Tags** - Limits the allocations that the Driver Verifier utility can fail to allocations with the specified pool tags. You can use a wildcard character (*) to represent multiple pool tags. To list multiple pool tags, separate the tags with spaces. By default, all allocations can fail. • **Applications** - Limits the allocations that the Driver Verifier utility can fail to allocations for the specified program. Type the name of an executable file. To list programs, separate the program names with spaces. By default, all allocations can fail. • **DelayMins** - Specifies the number of minutes after booting during which the Driver Verifier utility does not intentionally fail any allocations. This delay allows the drivers to load and the system to stabilize before the test begins. Type a number (in decimal or hexadecimal). The default value is 7 (minutes).

Parameter	Description
/faultssystematic	Specifies the options for **Systematic Low Resources** simulation. Use the `0x40000` flag to select the **Systematic Low Resources** simulation option. The following options are available: • **enableboottime** - Enables fault injections across computer reboots. • **disableboottime** - Disables fault injections across computer reboots (this is the default setting). • **recordboottime** - Enables fault injections in what if mode across computer reboots. • **resetboottime** - Disables fault injections across computer reboots and clears the stack exclusion list. • **enableruntime** - Dynamically enables fault injections. • **disableruntime** - Dynamically disables fault injections. • **recordruntime** - Dynamically enables fault injections in what if mode. • **resetruntime** - Dynamically disables fault injections and clears the previously faulted stack list. • **querystatistics** - Shows the current fault injection statistics. • **incrementcounter** - Increments the test pass counter used to identify when a fault was injected. • **getstackid COUNTER** - Retrieves the indicated injected stack identifier. • **excludestack STACKID** - Excludes the stack from fault injection.

Parameter	Description
/flags `<options>`	Activates the specified options after the next reboot. This number can be entered in decimal or in hexadecimal (with an 0x prefix) format. Any combination of the following values is allowed: • **Value: 1 or 0x1 (bit 0)** - Special pool checking • **Value: 2 or 0x2 (bit 1)** - Force IRQL Checking • **Value: 4 or 0x4 (bit 2)** - Low Resources Simulation • **Value: 8 or 0x8 (bit 3)** - Pool Tracking • **Value: 16 or 0x10 (bit 4)** - I/O Verification • **Value: 32 or 0x20 (bit 5)** - Deadlock Detection • **Value: 64 or 0x40 (bit 6)** - Enhanced I/O Verification. This option is automatically activated when you select **I/O Verification**. • **Value: 128 or 0x80 (bit 7)** - DMA Verification • **Value: 256 or 0x100 (bit 8)** - Security Checks • **Value: 512 or 0x200 (bit 9)** - Force Pending I/O Requests • **Value: 1024 or 0x400 (bit 10)** - IRP Logging • **Value: 2048 or 0x800 (bit 11)** - Miscellaneous Checks • **Value: 8192 or 0x2000 (bit 13)** - Invariant MDL Checking for Stack • **Value: 16384 or 0x4000 (bit 14)** - Invariant MDL Checking for Driver • **Value: 32768 or 0x8000 (bit 15)** - Power Framework Delay Fuzzing • **Value: 65536 or 0x10000 (bit 16)** - Port/miniport interface checking • **Value: 131072 or 0x20000 (bit 17)** - DDI compliance checking • **Value: 262144 or 0x40000 (bit 18)** - Systematic low resources simulation • **Value: 524288 or 0x80000 (bit 19)** - DDI compliance checking (additional) • **Value: 2097152 or 0x200000 (bit 21)** - NDIS/WIFI verification • **Value: 8388608 or 0x800000 (bit 23)** - Kernel synchronization delay fuzzing • **Value: 16777216 or 0x1000000 (bit 24)** - VM switch verification • **Value: 33554432 or 0x2000000 (bit 25)** - Code integrity checks. You can't use this method to activate the SCSI Verification or Storport Verification options. For more information, see SCSI Verification and Storport Verification.
/flags `<volatileoptions>`	Specifies the the Driver Verifier utility options that are changed immediately without rebooting.This number can be entered in decimal or in hexadecimal (with an 0x prefix) format. Any combination of the following values is allowed: • **Value: 1 or 0x1 (bit 0)** - Special pool • **Value: 2 or 0x2 (bit 1)** - Force IRQL Checking • **Value: 4 or 0x4 (bit 2)** - Low Resources Simulation

Parameter	Description
`<probability>`	Number between 1 and 10,000 specifying the fault injection probability. For example, specifying 100 means a fault injection probability of 1% (100/10,000). if this parameter isn't specified, the default probability of 6% is used.
`<tags>`	Specifies the pool tags that will be injected with faults, separated by space characters. If this parameter is not specified, then any pool allocation can be injected with faults.
`<apps>`	Specifies the image file name of the apps that will be injected with faults, separated by space characters. If this parameter isn't specified, then low resources simulation can take place in any application.
`<minutes>`	A positive number specifying the length of the period after rebooting, in minutes, during which no fault injection will occur. If this parameter isn't specified, then the default length of *8 minutes* is used.
/iolevel `<level>`	Specifies the level of I/O Verification. The value of [level] can be **1** - Enables Level 1 I/O Verification (default) or **2** - Enables Level 1 I/O Verification and Level 2 I/O Verification. If I/O Verification isn't enabled (by using `/flags 0x10`), **/iolevel** is ignored.
/log `<logfilename>` `[/intervalseconds]`	Creates a log file using the specified name. The Driver Verifier utility periodically writes statistics to this file, based on the interval you optionally set. The default interval is *30 seconds*. If a verifier **/log** command is typed at the command line, the command prompt doesn't return. To close the log file and return a prompt, use the **CTRL+C** key. After a reboot, to create a log, you must submit the verifier **/log** command again.
/rules `<option>`	Options for rules that can be disabled, including: • **query** - Shows current status of controllable rules. • **reset** - Resets all rules to their default state. • **default ID** - Sets rule ID to its default state. For the supported rules, the rule ID is the Bug Check 0xC4 (DRIVER_VERIFIER_DETECTED_VIOLATION) parameter 1 value. • **disable ID** - Disables specified rule ID. For the supported rules, the rule ID is the Bug Check 0xC4 (DRIVER_VERIFIER_DETECTED_VIOLATION) parameter 1 value.

Parameter	Description
/standard	Activates the "standard" or default Driver Verifier options after the next restart. The standard options are Special Pool, Force IRQL Checking, Pool Tracking, I/O Verification, Deadlock Detection, DMA Verification, Security Checks, Miscellaneous Checks, and DDI compliance checking. This is equivalent to `/flags 0x209BB`. [!NOTE] Starting in Windows 10 versions after 1803, using `/flags 0x209BB` will no longer automatically enable WDF verification. Use the **/standard** syntax to enable standard options, with WDF verification included.
/volatile	Changes the settings without rebooting the computer. Volatile settings take effect immediately. You can use the **/volatile** parameter with the **/flags** parameter to enable and disable some options without rebooting. You can also use **/volatile** with the **/adddriver** and **/removedriver** parameters to start or stop the verification of a driver without rebooting, even if the Driver Verifier utility isn't running. For more information, see Using Volatile Settings.
/adddriver `<volatiledriverlist>`	Adds the specified drivers from the volatile settings. To specify multiple drivers, list their names, separated by spaces. Wildcard values, such as *n.sys*, aren't supported.
/removedriver `<volatiledriverlist>`	Removes the specified drivers from the volatile settings. To specify multiple drivers, list their names, separated by spaces. Wildcard values, such as *n.sys*, aren't supported.
/reset	Clears all the Driver Verifier utility settings. After the next restart, no drivers will be verified.
/querysettings	Displays a summary of the options that will be activated and drivers that will be verified after the next boot. The display doesn't include drivers and options added by using the **/volatile** parameter. For other ways to view these settings, see Viewing Driver Verifier Settings.
/query	Displays a summary of the Driver Verifier utility's current activity. The **Level** field in the display is the hexadecimal value of options set with the **/volatile** parameter. For explanations of each statistic, see Monitoring Global Counters and Monitoring Individual Counters.

Parameter	Description
/domain `<types> <options>`	Controls the verifier extension settings. The following verifier extension types are supported: • **wdm** - Enables verifier extension for WDM drivers. • **ndis** - Enables verifier extension for networking drivers. • **ks** - Enables verifier extension for kernel mode streaming drivers. • **audio** - Enables verifier extension for audio drivers. . The following extension options are supported: • **rules.default** - Enables default validation rules for the selected verifier extension. • **rules.all** - Enables all validation rules for the selected verifier extension.
/logging	Enables logging for violated rules detected by the selected verifier extensions.
/livedump	Enables live memory dump collection for violated rules detected by the selected verifier extensions.
/?	Displays command-line help.

Return Codes

The following values are returned after driver verifier has run:

- 0: EXIT_CODE_SUCCESS
- 1: EXIT_CODE_ERROR
- 2: EXIT_CODE_REBOOT_NEEDED

Remarks

- You can use the **/volatile** parameter with some of the Driver Verifier utility **/flags** options and with **/standard**. You can't use **/volatile** with the **/flags** options for DDI compliance checking, Power Framework Delay Fuzzing, Storport Verification, or SCSI Verification. For more information, see Using Volatile Settings.

Related links

- Command-Line Syntax Key

- Driver Verifier
- Controlling Driver Verifier
- Monitoring Driver Verifier
- Using Volatile Settings

verify

Article • 02/03/2023

Tells the Command Prompt tool (cmd.exe) whether to verify your files are written correctly to a disk.

Syntax

```
verify [on | off]
```

Parameters

Parameter	Description
`[on | off]`	Switches the **verify** setting on or off.
/?	Displays help at the command prompt.

Examples

To display the current **verify** setting, type:

```
verify
```

To turn the **verify** setting on, type:

```
verify on
```

Related links

- Command-Line Syntax Key

vol

Article • 02/03/2023

Displays the disk volume label and serial number, if they exist. If used without parameters, **vol** displays information for the current drive.

Syntax

```
vol [<drive>:]
```

Parameters

Parameter	Description
`<drive>:`	Specifies the drive that contains the disk for which you want to display the volume label and serial number.
/?	Displays help at the command prompt.

Related links

- Command-Line Syntax Key

vssadmin

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Windows 8.1, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

Displays current volume shadow copy backups and all installed shadow copy writers and providers. Select a command name in the following table view its command syntax.

Command	Description	Availability
vssadmin delete shadows	Deletes volume shadow copies.	Client and Server
vssadmin list shadows	Lists existing volume shadow copies.	Client and Server
vssadmin list writers	Lists all subscribed volume shadow copy writers on the system.	Client and Server
vssadmin resize shadowstorage	Resizes the maximum size for a shadow copy storage association.	Client and Server

Related links

- Command-Line Syntax Key

vssadmin delete shadows

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Windows 8.1, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

Deletes a specified volume's shadow copies. You can only delete shadow copies with the *client-accessible* type.

Syntax

```
vssadmin delete shadows /for=<ForVolumeSpec> [/oldest | /all | /shadow=
<ShadowID>] [/quiet]
```

Parameters

Parameter	Description
/for=`<ForVolumeSpec>`	Specifies which volume's shadow copy will be deleted.
/oldest	Deletes only the oldest shadow copy.
/all	Deletes all of the specified volume's shadow copies.
/shadow=`<ShadowID>`	Deletes the shadow copy specified by ShadowID. To get the shadow copy ID, use the vssadmin list shadows command. When you enter a shadow copy ID, use the following format, where each *X* represents a hexadecimal character: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
/quiet	Specifies that the command won't display messages while running.

Examples

To delete the oldest shadow copy of volume C, type:

```
```

```
vssadmin delete shadows /for=c: /oldest
```

Related links

- Command-Line Syntax Key
- vssadmin command
- vssadmin list shadows command

vssadmin list shadows

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Windows 8.1, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

Lists all existing shadow copies of a specified volume. If you use this command without parameters, it displays all volume shadow copies on the computer in the order dictated by **Shadow Copy Set**.

Syntax

```
vssadmin list shadows [/for=<ForVolumeSpec>] [/shadow=<ShadowID>]
```

Parameters

Parameter	Description
/for=`<ForVolumeSpec>`	Specifies which volume the shadow copies will be listed for.
/shadow=`<ShadowID>`	Lists the shadow copy specified by ShadowID. To get the shadow copy ID, use the vssadmin list shadows command. When you type a shadow copy ID, use the following format, where each *X* represents a hexadecimal character: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

Related links

- Command-Line Syntax Key
- vssadmin command
- vssadmin list shadows command

vssadmin list writers

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Windows 8.1, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

Lists subscribed volume shadow copy writers.

Syntax

```
vssadmin list writers
```

Related links

- Command-Line Syntax Key
- vssadmin command

vssadmin resize shadowstorage

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows 10, Windows 8.1, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008

Resizes the maximum amount of storage space that can be used for shadow copy storage.

The minimum amount of storage space that can be used for shadow copy storage can be specified by using the **MinDiffAreaFileSize** registry value. For more information, see MinDiffAreaFileSize.

> ⚠ **Warning**
>
> Resizing the storage association may cause shadow copies to disappear.

Syntax

```
vssadmin resize shadowstorage /for=<ForVolumeSpec> /on=<OnVolumeSpec>
[/maxsize=<MaxSizeSpec>]
```

Parameters

Parameter	Description
/for=`<ForVolumeSpec>`	Specifies the volume for which the maximum amount of storage space is to be resized.
/on=`<OnVolumeSpec>`	Specifies the storage volume.
[/maxsize=`<MaxSizeSpec>`]	Specifies the maximum amount of space that can be used for storing shadow copies. If no value is specified for **/maxsize**, there's no limit placed on the amount of storage space that can be used. The **MaxSizeSpec** value must be 1 MB or greater and must be expressed in one of the following units: KB, MB, GB, TB, PB, or EB. If no unit is specified, **MaxSizeSpec** uses bytes by default.

Examples

To resize shadow copy of volume C on volume D, with a maximum size of 900MB, type:

```
vssadmin resize shadowstorage /For=C: /On=D: /MaxSize=900MB
```

To resize shadow copy of volume C on volume D, with no maximum size, type:

```
vssadmin resize shadowstorage /For=C: /On=D: /MaxSize=UNBOUNDED
```

To resize shadow copy of volume C by 20%, type:

```
vssadmin resize shadowstorage /For=C: /On=C: /MaxSize=20%
```

Related links

- Command-Line Syntax Key
- vssadmin command

waitfor

Article • 02/03/2023

Sends or waits for a signal on a system. This command is used to synchronize computers across a network.

Syntax

```
waitfor [/s <computer> [/u [<domain>\]<user> [/p [<password>]]]] /si
<signalname>
waitfor [/t <timeout>] <signalname>
```

Parameters

Parameter	Description
/s `<computer>`	Specifies the name or IP address of a remote computer (don't use backslashes). The default is the local computer. This parameter applies to all files and folders specified in the command. If you don't use this parameter, the signal is broadcast to all the systems in a domain. If you do use this parameter, the signal is sent only to the specified system.
/u `[<domain>]` `<user>`	Runs the script using the credentials of the specified user account. By default, **waitfor** uses the current user's credentials.
/p `[\` `<password>]`	Specifies the password of the user account that is specified in the **/u** parameter.
/si	Sends the specified signal across the network. This parameter also lets you manually activate a signal.
/t `<timeout>`	Specifies the number of seconds to wait for a signal. By default, **waitfor** waits indefinitely.
`<signalname>`	Specifies the signal that **waitfor** waits for or sends. This parameter isn't case-sensitive and can't exceed 225 characters. Valid characters include a-z, A-Z, 0-9, and the ASCII extended character set (128-255).
/?	Displays help at the command prompt.

Remarks

- You can run multiple instances of **waitfor** on a single computer, but each instance of **waitfor** must wait for a different signal. Only one instance of **waitfor** can wait for a given signal on a given computer.
- Computers can only receive signals if they are in the same domain as the computer sending the signal.
- You can use this command when you test software builds. For example, the compiling computer can send a signal to several computers running **waitfor** after the compile has completed successfully. On receipt of the signal, the batch file that includes **waitfor** can instruct the computers to immediately start installing software or running tests on the compiled build.

Examples

To wait until the *espresso\build007* signal is received, type:

```
waitfor espresso\build007
```

By default, **waitfor** waits indefinitely for a signal.

To wait *10 seconds* for the *espresso\compile007* signal to be received before timing out, type:

```
waitfor /t 10 espresso\build007
```

To manually activate the *espresso\build007* signal, type:

```
waitfor /si espresso\build007
```

Related links

- Command-Line Syntax Key

wbadmin

Article • 02/03/2023

Enables you to back up and restore your operating system, volumes, files, folders, and applications from a command prompt.

To configure a regularly scheduled backup using this command, you must be a member of the **Administrators** group. To perform all other tasks with this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions.

You must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

Parameters

Parameter	Description
wbadmin delete catalog	Deletes the backup catalog on the local computer. Use this command only if the backup catalog on this computer is corrupted and you have no backups stored at another location that you can use to restore the catalog.
wbadmin delete systemstatebackup	Deletes one or more system state backups.
wbadmin disable backup	Disables your daily backups.
wbadmin enable backup	Configures and enables a regularly scheduled backup.
wbadmin get disks	Lists disks that are currently online.
wbadmin get items	Lists the items included in a backup.
wbadmin get status	Shows the status of the currently running backup or recovery operation.
wbadmin get versions	Lists details of backups recoverable from the local computer or, if another location is specified, from another computer.
wbadmin restore catalog	Recovers a backup catalog from a specified storage location in the case where the backup catalog on the local computer has been corrupted.
wbadmin start backup	Runs a one-time backup. If used with no parameters, uses the settings from the daily backup schedule.

Parameter	Description
wbadmin start recovery	Runs a recovery of the volumes, applications, files, or folders specified.
wbadmin start sysrecovery	Runs a recovery of the full system (at least all the volumes that contain the operating system's state). This command is only available if you are using the Windows Recovery Environment.
wbadmin start systemstatebackup	Runs a system state backup.
wbadmin start systemstaterecovery	Runs a system state recovery.
wbadmin stop job	Stops the currently running backup or recovery operation.

Related links

- Command-Line Syntax Key
- Windows Server Backup Cmdlets in Windows PowerShell
- Windows Recovery Environment (WinRE)

wbadmin delete catalog

Article • 02/03/2023

Deletes the backup catalog that is stored on the local computer. Use this command when the backup catalog has been corrupted and you can't restore it using the wbadmin restore catalog command.

To delete a backup catalog using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

Syntax

```
wbadmin delete catalog [-quiet]
```

Parameters

Parameter	Description
-quiet	Runs the command without prompts to the user.

Remarks

- If you delete the backup catalog of a computer, you'll no longer be able to get to any backups created for that computer using the Windows Server Backup snap-in. However, if you can get to another backup location and run the wbadmin restore catalog command, you can restore the backup catalog from that location.
- We strongly recommend you create a new backup after you delete a backup catalog.

Related links

- Command-Line Syntax Key

- wbadmin command
- wbadmin restore catalog command
- Remove-WBCatalog

wbadmin delete systemstatebackup

Article • 02/03/2023

Deletes the system state backups that you specify. If the specified volume contains backups other than system state backups of your local server, those backups will not be deleted.

To delete a system state backup using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

> **Note**
>
> Windows Server Backup does not back up or recover registry user hives (HKEY_CURRENT_USER) as part of system state backup or system state recovery.

Syntax

```
wbadmin delete systemstatebackup {-keepVersions:<numberofcopies> | -version:
<versionidentifier> | -deleteoldest} [-backupTarget:<volumename>] [-machine:
<backupmachinename>] [-quiet]
```

> **Important**
>
> You must only specify one of these parameters: **-keepVersions**, **-version**, or **-deleteOldest**.

Parameters

Parameter	Description
-keepVersions	Specifies the number of the latest system state backups to keep. The value must be a positive integer. The parameter value **-keepversions:0** deletes all the system state backups.

Parameter	Description
-version	Specifies the version identifier of the backup in MM/DD/YYYY-HH:MM format. If you don't know the version identifier, run the wbadmin get versions command. Versions made up of exclusively system state backups can be deleted using this command. Run the wbadmin get items command to view the version type.
-deleteOldest	Deletes the oldest system state backup.
-backupTarget	Specifies the storage location for the backup that you want to delete. The storage location for disk backups can be a drive letter, a mount point, or a GUID-based volume path. This value only needs to be specified for locating backups that are not on the local computer. Information about backups for the local computer is available in the backup catalog on the local computer.
-machine	Specifies the computer whose system state backup you want to delete. Useful when multiple computers were backed up to the same location. Should be used when the **-backupTarget** parameter is specified.
-quiet	Runs the command without prompts to the user.

Examples

To delete the system state backup created on March 31, 2013 at 10:00 AM, type:

```
wbadmin delete systemstatebackup -version:03/31/2013-10:00
```

To delete all system state backups, except the three most recent, type:

```
wbadmin delete systemstatebackup -keepVersions:3
```

To delete the oldest system state backup stored on disk f:, type:

```
wbadmin delete systemstatebackup -backupTarget:f:\ -deleteOldest
```

Related links

- Command-Line Syntax Key
- wbadmin command
- wbadmin get versions command
- wbadmin get items command

wbadmin disable backup

Article • 02/03/2023

Stops running the existing scheduled daily backups.

To disable a scheduled daily backup using this command, you must be a member of the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

Syntax

```
wbadmin disable backup [-quiet]
```

Parameters

Parameter	Description
-quiet	Runs the command without prompts to the user.

Related links

- Command-Line Syntax Key
- wbadmin command
- wbadmin enable backup command

wbadmin enable backup

Article • 02/03/2023

Creates and enables a daily backup schedule or modifies an existing backup schedule. With no parameters specified, it displays the currently scheduled backup settings.

To configure or modify a daily backup schedule using this command, you must be a member of the **Backup Operators** group or the **Administrators** group. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

To view the disk identifier value for your disks, run the wbadmin get disks command.

Syntax

```
wbadmin enable backup [-addtarget:<BackupTarget>] [-removetarget:
<BackupTarget>] [-schedule:<TimeToRunBackup>] [-include:<VolumesToInclude>]
[-nonRecurseInclude:<ItemsToInclude>] [-exclude:<ItemsToExclude>] [-
nonRecurseExclude:<ItemsToExclude>][-systemState] [-hyperv:
<HyperVComponentsToExclude>] [-allCritical] [-systemState] [-vssFull | -
vssCopy] [-user:<UserName>] [-password:<Password>] [-allowDeleteOldBackups]
[-quiet]
```

Parameters

Parameter	Description

Parameter	Description
-addtarget	Specifies the storage location for backups. Requires you to specify the location as a disk, volume, or Universal Naming Convention (UNC) path to a remote shared folder (`\\<servername>\<sharename>`). By default, the backup will be saved at: `\\<servername>\<sharename> WindowsImageBackup <ComputerBackedUp>`. If you specify a disk, the disk will be formatted before use, and any existing data on it is permanently erased. If you specify a shared folder, you can't add more locations. You can only specify one shared folder as a storage location at a time. **Important:** If you save a backup to a remote shared folder, that backup is overwritten if you use the same folder to back up the same computer again. In addition, if the backup operation fails, you could end up with no backup because the older backup will be overwritten, but the newer backup won't be usable. You can avoid this by creating sub-folders in the remote shared folder to organize your backups. If you do this, the sub-folders need twice the space of the parent folder. Only one location can be specified in a single command. Multiple volume and disk backup storage locations can be added by running the command again.
-removetarget	Specifies the storage location that you want to remove from the existing backup schedule. Requires you to specify the location as a disk identifier.
-schedule	Specifies times of day to create a backup, formatted as HH:MM and comma delimited.
-include	Specifies the comma-delimited list of items to include in the backup. You can include multiple files, folders, or volumes. Volume paths can be specified using volume drive letters, volume mount points, or GUID-based volume names. If you use a GUID-based volume name, it should end with a backslash (`\`). You can use the wildcard character (`*`) in the file name when specifying a path to a file.
-nonRecurseInclude	Specifies the non-recursive, comma-delimited list of items to include in the backup. You can include multiple files, folders, or volumes. Volume paths can be specified using volume drive letters, volume mount points, or GUID-based volume names. If you use a GUID-based volume name, it should end with a backslash (`\`). You can use the wildcard character (`*`) in the file name when specifying a path to a file. Should be used only when the **-backupTarget** parameter is used.

Parameter	Description
-exclude	Specifies the comma-delimited list of items to exclude from the backup. You can exclude files, folders, or volumes. Volume paths can be specified using volume drive letters, volume mount points, or GUID-based volume names. If you use a GUID-based volume name, it should end with a backslash (`\`). You can use the wildcard character (`*`) in the file name when specifying a path to a file.
-nonRecurseExclude	Specifies the non-recursive, comma-delimited list of items to exclude from the backup. You can exclude files, folders, or volumes. Volume paths can be specified using volume drive letters, volume mount points, or GUID-based volume names. If you use a GUID-based volume name, it should end with a backslash (`\`). You can use the wildcard character (`*`) in the file name when specifying a path to a file.
-hyperv	Specifies the comma-delimited list of components to be included in backup. The identifier can be a component name or component GUID (with or without braces).
-systemState	Creates a backup that includes the system state in addition to any other items that you specified with the **-include** parameter. The system state contains boot files (Boot.ini, NDTLDR, NTDetect.com), the Windows Registry including COM settings, the SYSVOL (Group Policies and Logon Scripts), the Active Directory and NTDS.DIT on domain controllers and, if the certificates service is installed, the Certificate Store. If your server has the Web server role installed, the IIS Metadirectory will be included. If the server is part of a cluster, Cluster service information is also included.
-allCritical	Specifies that all critical volumes (volumes that contain operating system's state) be included in the backups. This parameter is useful if you are creating a backup for full system or system state recovery. It should be used only when **-backupTarget** is specified; otherwise, the command fails. Can be used with the **-include** option. **Tip:** The target volume for a critical-volume backup can be a local drive, but it can't be any of the volumes that are included in the backup.

Parameter	Description
-vssFull	Performs a full back up using the Volume Shadow Copy Service (VSS). All files are backed up, each file's history is updated to reflect that it was backed up, and the logs of previous backups may be truncated. If this parameter is not used, the wbadmin start backup command makes a copy backup, but the history of files being backed up is not updated. **Caution:** Don't use this parameter if you're using a product other than Windows Server Backup to back up apps that are on the volumes included in the current backup. Doing so can potentially break the incremental, differential, or other type of backups that the other backup product is creating because the history that they are relying on to determine how much data to backup might be missing and they might perform a full backup unnecessarily.
-vssCopy	Performs a copy backup using VSS. All files are backed up but the history of the files being backup up is not updated so you preserve the all the information on which files where changed, deleted, and so on, as well as any application log files. Using this type of backup does not affect the sequence of incremental and differential backups that might happen independent of this copy backup. This is the default value. **Warning:** A backup copy can't be used for incremental or differential backups or restores.
-user	Specifies the user with write permission to the backup storage destination (if it's a remote shared folder). The user needs to be a member of the **Administrators** or **Backup Operators** group on the computer getting backed up.
-password	Specifies the password for the user name provided by the parameter **-user**.
-allowDeleteOldBackups	Overwrites any backups made before the computer was upgraded.
-quiet	Runs the command without prompts to the user.

Examples

To schedule daily backups at 9:00 AM and 6:00 PM for hard disk drives E:, D:\mountpoint, and `\\?\Volume{cc566d14-44a0-11d9-9d93-806e6f6e6963}\`, and to save the files to the disk named, DiskID, type:

```
wbadmin enable backup -addtarget:DiskID -schedule:09:00,18:00 -
include:E:,D:\mountpoint,\\?\Volume{cc566d14-44a0-11d9-9d93-806e6f6e6963}\
```

To schedule daily backups of the D:\documents folder at 12:00 AM and 7:00 PM to the network location `\\backupshare\backup1`, using the network credentials for the **Backup Operator**, Aaren Ekelund (aekel), who's password is *$3hM9^5lp* and who is a member of the domain CONTOSOEAST, used to authenticate access to the network share, type:

```
wbadmin enable backup -addtarget:\\backupshare\backup1 -include:
D:\documents -user:CONTOSOEAST\aekel -password:$3hM9^5lp -
schedule:00:00,19:00
```

To schedule daily backups of volume T: and the D:\documents folder at 1:00 AM to drive H:, excluding the folder `d:\documents\~tmp`, and performing a full backup using the Volume Shadow Copy Service, type:

```
wbadmin enable backup -addtarget:H: -include T:,D:\documents -exclude
D:\documents\~tmp -vssfull -schedule:01:00
```

Related links

- Command-Line Syntax Key
- wbadmin command
- wbadmin enable backup command
- wbadmin start backup command
- wbadmin get disks command

wbadmin get disks

Article • 02/03/2023

Lists the internal and external disks that are currently online for the local computer.

To list the online disks using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

Syntax

```
wbadmin get disks
```

Related links

- Command-Line Syntax Key
- wbadmin command
- Get-WBDisk

wbadmin get items

Article • 02/03/2023

Lists the items included in a specific backup.

To list the items included in a specific backup using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

Syntax

```
wbadmin get items -version:<VersionIdentifier> [-backupTarget:
{<BackupDestinationVolume> | <NetworkSharePath>}] [-machine:
<BackupMachineName>]
```

Parameters

Parameter	Description
-version	Specifies the version of the backup in MM/DD/YYYY-HH:MM format. If you don't know the version information, run the wbadmin get versions command.
-backupTarget	Specifies the storage location that contains the backups for which you want the details. Use for listing backups stored at that target location. Backup target locations can be a locally attached disk drive or a remote shared folder. If this command is run on the same computer where the backup was created, this parameter isn't needed. However, this parameter is required to get information about a backup created from another computer.
-machine	Specifies the name of the computer that you want the backup details for. Useful when multiple computers have been backed up to the same location. Should be used when **-backupTarget** is specified.

Examples

To list items from the backup that was run on March 31, 2013 at 9:00 A.M., type:

```
wbadmin get items -version:03/31/2013-09:00
```

To list items from the backup of server01 that was run on April 30, 2013 at 9:00 A.M. and stored on `\\<servername>\<share>`, type:

```
wbadmin get items -version:04/30/2013-09:00 -backupTarget:\\servername\share
-machine:server01
```

Related links

- Command-Line Syntax Key
- wbadmin command
- wbadmin get versions command
- Get-WBBackupSet

wbadmin get status

Article • 02/03/2023

Reports the status of the backup or recovery operation that is currently running.

To get the status of the currently running backup or recovery operation using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

> **Important**
>
> This command doesn't stop until the backup or recovery operation is finished. The command continues to run even if you close the command window. To stop the current backup or recovery operation, run the **wbadmin stop job** command.

Syntax

```
wbadmin get status
```

Related links

- Command-Line Syntax Key
- wbadmin command
- wbadmin stop job command
- Get-WBJob

wbadmin get versions

Article • 02/03/2023

Lists details about the available backups that are stored on the local computer or another computer. The details provided for a backup include the backup time, the backup storage location, the version identifier, and the type of recoveries you can perform.

To get details about available backups using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

If this command is used without parameters, it lists all backups of the local computer, even if those backups are not available.

Syntax

```
wbadmin get versions [-backupTarget:{<BackupTargetLocation> |
<NetworkSharePath>}] [-machine:BackupMachineName]
```

Parameters

Parameter	Description
-backupTarget	Specifies the storage location that contains the backups that you want the details for. Use for listing backups stored at that target location. Backup target locations can be locally attached disk drives, volumes, remote shared folders, removable media such as DVD drives or other optical media. If this command is run on the same computer where the backup was created, this parameter isn't needed. However, this parameter is required to get information about a backup created from another computer.
-machine	Specifies the computer that you want backup details for. Use when backups of multiple computers are stored in the same location. Should be used when **-backupTarget** is specified.

Examples

To see a list of available backups that are stored on volume H:, type:

```
wbadmin get versions -backupTarget:H:
```

To see a list of available backups that are stored in the remote shared folder `\\<servername>\<share>` for the computer server01, type:

```
wbadmin get versions -backupTarget:\\servername\share -machine:server01
```

Related links

- Command-Line Syntax Key
- wbadmin command
- wbadmin get items command
- Get-WBBackupTarget

wbadmin restore catalog

Article • 02/03/2023

Recovers a backup catalog for the local computer from a storage location that you specify.

To recover a backup catalog included in a specific backup using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

> **Note**
>
> If the location (disk, DVD, or remote shared folder) where you store your backups is damaged or lost and can't be used to restore the backup catalog, run the **wbadmin delete catalog** command to delete the corrupted catalog. In this case, we recommend creating a new backup after your backup catalog is deleted.

Syntax

```
wbadmin restore catalog -backupTarget:{<BackupDestinationVolume> |
<NetworkShareHostingBackup>} [-machine:<BackupMachineName>] [-quiet]
```

Parameters

Parameter	Description
-backupTarget	Specifies the location of the backup catalog of the system as it was at the point after the backup was created.
-machine	Specifies the name of the computer that you want to recover the backup catalog for. Use when backups for multiple computers have been stored at the same location. Should be used when **-backupTarget** is specified.
-quiet	Runs the command without prompts to the user.

Examples

To restore a catalog from a backup stored on disk D:, type:

```
wbadmin restore catalog -backupTarget:D
```

To restore a catalog from a backup stored in the shared folder `\\<servername>\<share>` of server01, type:

```
wbadmin restore catalog -backupTarget:\\servername\share -machine:server01
```

Related links

- Command-Line Syntax Key
- wbadmin command
- wbadmin delete catalog command
- Restore-WBCatalog

wbadmin start backup

Article • 02/03/2023

Creates a backup using specified parameters. If no parameters are specified and you have created a scheduled daily backup, this command creates the backup by using the settings for the scheduled backup. If parameters are specified, it creates a Volume Shadow Copy Service (VSS) copy backup and won't update the history of the files that are being backed up.

To create a one-time backup using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

Syntax

com

```
wbadmin start backup [-backupTarget:{<BackupTargetLocation> |
<TargetNetworkShare>}] [-include:<ItemsToInclude>] [-nonRecurseInclude:
<ItemsToInclude>] [-exclude:<ItemsToExclude>] [-nonRecurseExclude:
<ItemsToExclude>] [-allCritical] [-systemState] [-noVerify] [-user:
<UserName>] [-password:<Password>] [-noInheritAcl] [-vssFull | -vssCopy] [-
quiet]
```

Parameters

Parameter	Description
-backupTarget	Specifies the storage location for this backup. Requires a hard disk drive letter (f:), a volume GUID-based path in the format of `\\?\Volume{GUID}`, or a Universal Naming Convention (UNC) path to a remote shared folder `(\\<servername>\<sharename>\)`. By default, the backup will be saved at: `\\<servername>\<sharename>\WindowsImageBackup\<ComputerBackedUp>\`.
-include	Specifies the comma-delimited list of items to include in the backup. You can include multiple files, folders, or volumes. Volume paths can be specified using volume drive letters, volume mount points, or GUID-based volume names. If you use a GUID-based volume name, it should be terminated with a backslash (`\`). You can use the wildcard character (`*`) in the file name when specifying a path to a file. The **-include** parameter should only be used in conjunction with the **-backupTarget** parameter.

Parameter	Description
-exclude	Specifies the comma-delimited list of items to exclude from the backup. You can exclude files, folders, or volumes. Volume paths can be specified using volume drive letters, volume mount points, or GUID-based volume names. If you use a GUID-based volume name, it should be terminated with a backslash (`\`). You can use the wildcard character (`*`) in the file name when specifying a path to a file. The **-exclude** parameter should only be used in conjunction with the **-backupTarget** parameter.
-nonRecurseInclude	Specifies the non-recursive, comma-delimited list of items to include in the backup. You can include multiple files, folders, or volumes. Volume paths can be specified using volume drive letters, volume mount points, or GUID-based volume names. If you use a GUID-based volume name, it should be terminated with a backslash (`\`). You can use the wildcard character (`*`) in the file name when specifying a path to a file. The **-nonRecurseInclude** parameter should only be used in conjunction with the **-backupTarget** parameter.
-nonRecurseExclude	Specifies the non-recursive, comma-delimited list of items to exclude from the backup. You can exclude files, folders, or volumes. Volume paths can be specified using volume drive letters, volume mount points, or GUID-based volume names. If you use a GUID-based volume name, it should be terminated with a backslash (`\`). You can use the wildcard character (`*`) in the file name when specifying a path to a file. The **-nonRecurseExclude** parameter should only be used in conjunction with the **-backupTarget** parameter.
-allCritical	Specifies that all critical volumes (volumes that contain operating system's state) be included in the backups. This parameter is useful if you're creating a backup for bare metal recovery. It should be used only when **-backupTarget** is specified, otherwise the command fails. Can be used with the **-include** option. **Tip:** The target volume for a critical-volume backup can be a local drive, but it Can't be any of the volumes that are included in the backup.
-systemState	Creates a backup that includes the system state in addition to any other items that you specified with the **-include** parameter. The system state contains boot files (Boot.ini, NDTLDR, NTDetect.com), the Windows Registry including COM settings, the SYSVOL (Group Policies and Logon Scripts), the Active Directory and NTDS.DIT on Domain Controllers and, if the certificates service is installed, the Certificate Store. If your server has the Web server role installed, the IIS Metadirectory will be included. If the server is part of a cluster, Cluster Service information will also be included.
-noVerify	Specifies that backups saved to removable media (such as a DVD) are not verified for errors. If you do not use this parameter, backups saved to removable media are verified for errors.

Parameter	Description
-user	If the backup is saved to a remote shared folder, specifies the user name with write permission to the folder.
-password	Specifies the password for the user name that is provided by the parameter **-user**.
-noInheritAcl	Applies the access control list (ACL) permissions that correspond to the credentials provided by the **-user** and **-password** parameters to `\\<servername>\<sharename>\WindowsImageBackup\<ComputerBackedUp>\` (the folder that contains the backup). To access the backup later, you must use these credentials or be a member of the Administrators group or the Backup Operators group on the computer with the shared folder. If **-noInheritAcl** is not used, the ACL permissions from the remote shared folder are applied to the `\<ComputerBackedUp>` folder by default so that anyone with access to the remote shared folder can access the backup.
-vssFull	Performs a full back up using the Volume Shadow Copy Service (VSS). All files are backed up, each file's history is updated to reflect that it was backed up, and the logs of previous backups may be truncated. If this parameter isn't used, **wbadmin start backup** makes a copy backup, but the history of files being backed up is not updated. **Caution:** Don't use this parameter if you are using a product other than Windows Server Backup to back up apps that are on the volumes included in the current backup. Doing so can potentially break the incremental, differential, or other type of backups that the other backup product is creating because the history that they are relying on to determine how much data to backup might be missing and they might perform a full backup unnecessarily.
-vssCopy	Performs a copy backup using VSS. All files are backed up but the history of the files being backup up is not updated so you preserve the all the information on which files where changed, deleted, and so on, as well as any application log files. Using this type of backup does not affect the sequence of incremental and differential backups that might happen independent of this copy backup. This is the default value. **Warning:** A copy backup can't be used for incremental or differential backups or restores.
-quiet	Runs the command without prompts to the user.

Remarks

- If you save your backup to a remote shared folder, and then perform another backup to the same computer and the same remote shared folder, you will overwrite your previous backup.

- If your backup operation fails, you can end up without a backup because the older backup is overwritten, but the newer backup isn't usable. To avoid this, we recommend creating subfolders in the remote shared folder to organize your backups. However, because of this organization, you must have twice the space available as the parent folder.

Examples

To create a backup of volumes *e:*, *d:\mountpoint*, and `\\?\Volume{cc566d14-4410-11d9-9d93-806e6f6e6963}\` to volume *f:*, type:

```
wbadmin start backup -backupTarget:f: -include:e:,d:\mountpoint,\\?
\Volume{cc566d14-44a0-11d9-9d93-806e6f6e6963}\
```

To perform a one-time backup of *f:\folder1* and *h:\folder2* to volume *d:*, to backup the system state, and to make a copy backup so the normally scheduled differential backup isn't impacted, type:

```
wbadmin start backup –backupTarget:d: -include:g\folder1,h:\folder2 –
systemstate -vsscopy
```

To perform a one-time, non-recursive backup of *d:\folder1* to the `\\backupshare\backup1*` network location, and to restrict access to members of the **Administrators** or **Backup Operators** group, type:

```
wbadmin start backup –backupTarget: \\backupshare\backup1 -noinheritacl -
nonrecurseinclude:d:\folder1
```

Related links

- Command-Line Syntax Key
- wbadmin command

wbadmin start recovery

Article • 02/03/2023

Runs a recovery operation based on the parameters that you specify.

To perform a recovery using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

Syntax

```
wbadmin start recovery -version:<VersionIdentifier> -items:
{<VolumesToRecover> | <AppsToRecover> | <FilesOrFoldersToRecover>} -
itemtype:{Volume | App | File} [-backupTarget:{<VolumeHostingBackup> |
<NetworkShareHostingBackup>}] [-machine:<BackupMachineName>] [-
recoveryTarget:{<TargetVolumeForRecovery> | <TargetPathForRecovery>}] [-
recursive] [-overwrite:{Overwrite | CreateCopy | Skip}] [-notRestoreAcl] [-
skipBadClusterCheck] [-noRollForward] [-quiet]
```

Parameters

Parameter	Description
-version	Specifies the version identifier of the backup to recover in MM/DD/YYYY-HH:MM format. If you don't know the version identifier, run the wbadmin get versions command.
-items	Specifies a comma-delimited list of volumes, apps, files, or folders to recover. You must use this parameter with the **-itemtype** parameter.
-itemtype	Specifies type of items to recover. Must be **Volume**, **App**, or **File**. If the **-itemtype** is *Volume*, you can specify only a single volume, by providing the volume drive letter, volume mount point, or GUID-based volume name. If the **-itemtype** is *App*, you can specify only a single application or you can use the value **ADIFM** to recover an installation of Active Directory. To be recovered, the app must have registered with Windows Server Backup. If the **-itemtype** is *File*, you can specify files or folders, but they should be part of the same volume and they should be under the same parent folder.

Parameter	Description
-backupTarget	Specifies the storage location that contains the backup that you want to recover. This parameter is useful when the location is different from where backups of this computer are usually stored.
-machine	Specifies the name of the computer that you want to recover the backup for. This parameter must be used when the **-backupTarget** parameter is specified. The **-machine** parameter is useful when multiple computers have been backed up to the same location.
-recoveryTarget	Specifies the location to restore to. This parameter is useful if this location is different than the location that was previously backed up. It can also be used for restorations of volumes, files, or apps. If you're restoring a volume, you can specify the volume drive letter of the alternate volume. If you're restoring a file or app, you can specify an alternate recovery location.
-recursive	Valid only when recovering files. Recovers the files in the folders and all files subordinate to the specified folders. By default, only files which reside directly in the specified folders are recovered.
-overwrite	Valid only when recovering files. Specifies the action to take when a file that is being recovered already exists in the same location. The valid options are: • **Skip** - Causes Windows Server Backup to skip the existing file and continue with recovery of the next file. • **CreateCopy** - Causes Windows Server Backup to create a copy of the existing file so that the existing file is not modified. • **Overwrite** - Causes Windows Server Backup to overwrite the existing file with the file from the backup.
-notRestoreAcl	Valid only when recovering files. Specifies to not restore the security access control lists (ACLs) of the files being recovered from the backup. By default, the security ACLs are restored (the default value is **true**). If this parameter is used, the ACLs for the restored files will be inherited from the location to which the files are being restored.
-skipBadClusterCheck	Valid only when recovering volumes. Skips checking the disks you are recovering to for bad cluster information. If you are recovering to an alternate server or hardware, we recommend that you don't use this parameter. You can manually run the command **chkdsk /b** on these disks at any time to check them for bad clusters, and then update the file system information accordingly. **Important:** Until you run **chkdsk /b**, the bad clusters reported on your recovered system might not be accurate.

Parameter	Description
-noRollForward	Valid only when recovering apps. Allows for previous point-in-time recovery of an app if you select the latest version from the backups. Previous point-in-time recovery is done as the default for all other non-latest versions of the app.
-quiet	Runs the command without prompts to the user.

Remarks

- To view a list of items available to recover from a specific backup version, run the wbadmin get items command. If a volume didn't have a mount point or drive letter at the time of backup, then this command returns a GUID-based volume name that should be used for recovering the volume.
- If you use a value of **ADIFM** to perform an install from media operation to recover the related data needed for Active Directory Domain Services, **ADIFM** creates a copy of the Active Directory database, registry, and SYSVOL state, and then saves this information in the location specified by **-recoveryTarget**. Use this parameter only when **-recoveryTarget** is specified.

Examples

To run a recovery of the backup from March 31, 2020, taken at 9:00 A.M., of volume d:, type:

```
wbadmin start recovery -version:03/31/2020-09:00 -itemType:Volume -items:d:
```

To run a recovery to drive d of the backup from March 31, 2020, taken at 9:00 A.M., of the registry, type:

```
wbadmin start recovery -version:03/31/2020-09:00 -itemType:App -
items:Registry -recoverytarget:d:\
```

To run a recovery of the backup from March 31, 2020, taken at 9:00 A.M., of the d:\folder and folders subordinate to d:\folder, type:

```
wbadmin start recovery -version:03/31/2020-09:00 -itemType:File -
items:d:\folder -recursive
```

To run a recovery of the backup from March 31, 2020, taken at 9:00 A.M., of the volume `\\?\Volume{cc566d14-44a0-11d9-9d93-806e6f6e6963}\`, type:

```
wbadmin start recovery -version:03/31/2020-09:00 -itemType:Volume -items:\\?
\Volume{cc566d14-44a0-11d9-9d93-806e6f6e6963}\
```

To run a recovery of the backup from April 30, 2020, taken at 9:00 A.M., of the shared folder `\\servername\share` from server01, type:

```
wbadmin start recovery -version:04/30/2020-09:00 -
backupTarget:\\servername\share -machine:server01
```

Related links

- Command-Line Syntax Key
- wbadmin command
- Start-WBFileRecovery
- Start-WBHyperVRecovery
- Start-WBSystemStateRecovery
- Start-WBVolumeRecovery

wbadmin start sysrecovery

Article • 02/03/2023

Performs a system recovery (bare metal recovery) using your specified parameters.

To perform a system recovery using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions.

> **Important**
>
> The **wbadmin start sysrecovery** command must be run from the Windows Recovery Console, and isn't listed in the default usage text for the **wbadmin** tool. For more information, see **Windows Recovery Environment (WinRE)**.

Syntax

```
wbadmin start sysrecovery -version:<VersionIdentifier> -backupTarget:
{<BackupDestinationVolume> | <NetworkShareHostingBackup>}  [-machine:
<BackupMachineName>] [-restoreAllVolumes] [-recreateDisks] [-excludeDisks]
[-skipBadClusterCheck] [-quiet]
```

Parameters

Parameter	Description
-version	Specifies the version identifier of the backup to recover in MM/DD/YYYY-HH:MM format. If you don't know the version identifier, run the wbadmin get versions command.
-backupTarget	Specifies the storage location that contains the backup(s) you want to recover. This parameter is useful when the storage location is different from where backups of this computer are usually stored.
-machine	Specifies the name of the computer that you want to recover the backup for. This parameter must be used when the **-backupTarget** parameter is specified. The **-machine** parameter is useful when multiple computers have been backed up to the same location.

Parameter	Description
-restoreAllVolumes	Recovers all volumes from the selected backup. If this parameter is not specified, only critical volumes (volumes that contain the system state and operating system components) are recovered. This parameter is useful when you need to recover non-critical volumes during system recovery.
-recreateDisks	Recovers a disk configuration to the state that existed when the backup was created. **Warning:** This parameter deletes all data on volumes that host operating system components. It might also delete data from data volumes.
-excludeDisks	Valid only when specified with the **-recreateDisks** parameter and must be input as a comma-delimited list of disk identifiers (as listed in the output of the wbadmin get disks command). Excluded disks aren't partitioned or formatted. This parameter helps preserve data on disks that you don't want modified during the recovery operation.
-skipBadClusterCheck	Valid only when recovering volumes. Skips checking the disks you are recovering to for bad cluster information. If you are recovering to an alternate server or hardware, we recommend that you don't use this parameter. You can manually run the command **chkdsk /b** on these disks at any time to check them for bad clusters, and then update the file system information accordingly. **Important:** Until you run **chkdsk /b**, the bad clusters reported on your recovered system might not be accurate.
-quiet	Runs the command without prompts to the user.

Examples

To start recovering the information from the backup that was run on March 31, 2020 at 9:00 A.M., located on drive d:, type:

```
wbadmin start sysrecovery -version:03/31/2020-09:00 -backupTarget:d:
```

To start recovering the information from the backup that was run on April 30, 2020 at 9:00 A.M., located in the shared folder `\\servername\share` for server01, type:

```
wbadmin start sysrecovery -version:04/30/2020-09:00 -
backupTarget:\\servername\share -machine:server01
```

Related links

- Command-Line Syntax Key
- wbadmin command
- Get-WBBareMetalRecovery

wbadmin start systemstatebackup

Article • 02/03/2023

Creates a system state backup of the local computer and stores it on the location specified.

To perform a system state backup using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

> **Note**
>
> Windows Server Backup doesn't back up or recover registry user hives (HKEY_CURRENT_USER) as part of system state backup or system state recovery.

Syntax

```
wbadmin start systemstatebackup -backupTarget:<VolumeName> [-quiet]
```

Parameters

Parameter	Description
-backupTarget	Specifies the location where you want to store the backup. The storage location requires a drive letter or a GUID-based volume of the format: `\\?\Volume{*GUID*}`. Use the command `-backuptarget:\\servername\sharedfolder\` to store system state backups.
-quiet	Runs the command without prompts to the user.

Examples

To create a system state backup and store it on volume f, type:

```
wbadmin start systemstatebackup -backupTarget:f:
```

Related links

- Command-Line Syntax Key
- wbadmin command
- Start-WBBackup

wbadmin start systemstaterecovery

Article • 02/03/2023

Performs a system state recovery to a location and from a backup that you specify.

To perform a system state recovery using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

> **Note**
>
> Windows Server Backup doesn't back up or recover registry user hives (HKEY_CURRENT_USER) as part of system state backup or system state recovery.

Syntax

```
wbadmin start systemstaterecovery -version:<VersionIdentifier> -showsummary
[-backupTarget:{<BackupDestinationVolume> | <NetworkSharePath>}]
[-machine:<BackupMachineName>] [-recoveryTarget:<TargetPathForRecovery>] [-
authsysvol] [-autoReboot] [-quiet]
```

Parameters

Parameter	Description
-version	Specifies the version identifier of the backup to recover in MM/DD/YYYY-HH:MM format. If you don't know the version identifier, run the wbadmin get versions command.
-showsummary	Reports the summary of the last system state recovery (after the restart required to finish the operation). This parameter can't be accompanied by any other parameters.
-backupTarget	Specifies the storage location with the backup(s) you want to recover. This parameter is useful when the storage location is different from where backups are usually stored.

Parameter	Description
-machine	Specifies the name of the computer to recover the backup for. This parameter must be used when the **-backupTarget** parameter is specified. The **-machine** parameter is useful when multiple computers have been backed up to the same location.
-recoveryTarget	Specifies what directory to restore to. This parameter is useful if the backup is restored to an alternate location.
-authsysvol	Performs an authoritative restore of the System Volume (sysvol) shared directory.
-autoReboot	Specifies to restart the system at the end of the system state recovery operation. This parameter is valid only for a recovery to the original location. We don't recommend you use this parameter if you need to perform steps after the recovery operation.
-quiet	Runs the command without prompts to the user.

Examples

To start a system state recovery of the backup from 03/31/2020 at 9:00 A.M., type:

```
wbadmin start systemstaterecovery -version:03/31/2020-09:00
```

To start a system state recovery of the backup from 04/30/2020 at 9:00 A.M. that is stored on the shared resource `\\servername\share` for server01, type:

```
wbadmin start systemstaterecovery -version:04/30/2013-09:00 -
backupTarget:\\servername\share -machine:server01
```

Related links

- Command-Line Syntax Key
- wbadmin command
- Start-WBSystemStateRecovery

wbadmin stop job

Article • 02/03/2023

Cancels the backup or recovery operation that is currently running.

> **ⓘ Important**
>
> Canceled operations can't be restarted. You must run a canceled backup or a recovery operation from the beginning again.

To stop a backup or recovery operation using this command, you must be a member of the **Backup Operators** group or the **Administrators** group, or you must have been delegated the appropriate permissions. In addition, you must run **wbadmin** from an elevated command prompt, by right-clicking **Command Prompt**, and then selecting **Run as administrator**.

Syntax

```
wbadmin stop job [-quiet]
```

Parameters

Parameter	Description
-quiet	Runs the command without prompts to the user.

Related links

- Command-Line Syntax Key
- wbadmin command

wdsutil

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Wdsutil is a command-line utility used for managing your Windows Deployment Services server. To run these commands, click **start**, right-click **Command prompt**, and click **Run as administrator**.

Commands

Command	Description
wdsutil add command	Adds objects or prestages computers.
wdsutil approve-autoadddevices command	Approves computers that are pending administrator approval.
wdsutil convert-riprepimage command	Converts an existing remote Installation Preparation (RIPrep) image to a Windows Image (.wim) file.
wdsutil copy command	Copies an image or a driver group.
wdsutil delete-autoadddevices command	Deletes computers that are in the Auto-add database (which stores information about the computers on the server).
wdsutil disable command	Disables all services for Windows Deployment Services.
wdsutil disconnect-client command	Disconnects a client from a multicast transmission or namespace.
wdsutil enable command	Enables all services for Windows Deployment Services.
wdsutil export-image command	Exports an image from the image store to a .wim file.
wdsutil get command	Retrieves properties and attributes about the specified object.

Command	Description
wdsutil initialize-server command	Configures a Windows Deployment Services server for initial use.
wdsutil new command	creates new capture and discover images as well as multicast transmissions and namespaces.
wdsutil progress command	Displays the progress status while a command is being executed.
wdsutil reject-autoadddevices command	Rejects computers that are pending administrator approval.
wdsutil remove command	removes objects.
wdsutil replace-image command	replaces a boot or installation image with a new version of that image.
wdsutil set command	Sets properties and attributes on the specified object.
wdsutil start server command	starts all services on the Windows Deployment Services server, including multicast transmissions, namespaces, and the Transport Server.
wdsutil stop server command	Stops all services on the Windows Deployment Services server.
wdsutil uninitialize-server command	reverts changes made during server initialization.
wdsutil update-serverfiles command	Updates server files on the remoteInstall share.
wdsutil verbose command	Displays verbose output for the specified command.

wdsutil add commands

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Parameters

Parameter	Description
wdsutil add-device command	Pre-stages a computer in active directory.
wdsutil add-image command	Adds boot or installation images.
wdsutil add-imagegroup command	Adds an image group.
wdsutil add-drivergrouppackage command	Adds a driver package to a driver group.
wdsutil add-drivergrouppackages command	Adds driver packages to a driver group.
wdsutil add-driverpackage command	Adds a driver package to the server.
wdsutil add-imagedriverpackage command	Adds a driver package that is in the driver store to an existing boot image on the server.
wdsutil add-imagedriverpackages command	Adds driver packages from the driver store to a boot image on the server.
wdsutil add-alldriverpackages subcommand	Adds driver packages from a folder to a server.
wdsutil add-drivergroup command	Adds a driver group to a server.
wdsutil add-drivergroupfilter command	Adds a filter to a driver group on a server.

Related links

- Command-Line Syntax Key

- Windows Deployment Services cmdlets

wdsutil add-alldriverpackages

Article • 02/03/2023

Adds all driver packages that are stored in a folder to a server.

Syntax

```
wdsutil /Add-AllDriverPackages /FolderPath:<folderpath> [/Server:
<servername>] [/Architecture:{x86 | ia64 | x64}] [/DriverGroup:<groupname>]
```

Parameters

Parameter	Description
/FolderPath:`<folderpath>`	Specifies the full path to the folder that contains the .inf files for the driver packages.
[/Server:`<servername>`]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.
[/Architecture:`{x86|ia64|x64}`]	Specifies the architecture type for the driver package.
[/DriverGroup:`<groupname>`]	Specifies the name of the driver group to which the packages should be added.

Examples

To add driver packages, type either:

```
wdsutil /verbose /Add-AllDriverPackages /FolderPath:C:\Temp\Drivers
/Architecture:x86
```

```
wdsutil /Add-AllDriverPackages /FolderPath:C:\Temp\Drivers\Printers
/DriverGroup:Printer Drivers
```

Related links

- Command-Line Syntax Key
- Windows Deployment Services cmdlets
- Add-WdsDriverPackage

wdsutil add-device

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Pre-stages a computer in Active Directory Domain Services (AD DS). Pre-staged computers are also called *known computers*. This allows you to configure properties to control the installation for the client. For example, you can configure the network boot program and the unattend file that the client should receive, as well as the server from which the client should download the network boot program.

Syntax

```
wdsutil /add-Device /Device:<Devicename> /ID:<UUID | MAC address>
[/ReferralServer:<Servername>] [/BootProgram:<Relativepath>]
[/WdsClientUnattend:<Relativepath>] [/User:<Domain\User | User@Domain>]
[/JoinRights:{JoinOnly | Full}] [/JoinDomain:{Yes | No}] [/BootImagepath:
<Relativepath>] [/OU:<DN of OU>] [/Domain:<Domain>]
```

Parameters

Parameter	Description
/Device:`<Devicename>`	Specifies the name of the device to be added.
/ID:`<UUID|MAC address>`	Specifies either the GUID/UUID or the MAC address of the computer. A GUID/UUID must be in one of two formats: Binary string (`/ID:ACEFA3E81F20694E953EB2DAA1E8B1B6`) or GUID string (`/ID:E8A3EFAC-201F-4E69-953E-B2DAA1E8B1B6`). A MAC address must be in the following format: **00B056882FDC** (no dashes) or **00-B0-56-88-2F-DC** (with dashes)
[/ReferralServer:`<Servername>`]	Specifies the name of the server to be contacted to download the network boot program and the boot image by using Trivial File Transfer Protocol (tftp).
[/BootProgram:`<Relativepath>`]	Specifies the relative path from the **remoteInstall** folder to the network boot program that this computer should receive. For example: `boot\x86\pxeboot.com`

Parameter	Description
[/WdsClientUnattend:`<Relativepath>`]	Specifies the relative path from the **remoteInstall** folder to the unattended installation file that automates the installation screens of the Windows Deployment Services client.
[/User:`<Domain\User|User@Domain>`]	Sets permissions on the computer account object to give the specified user the necessary rights to join the computer to the domain.
[/JoinRights:`{JoinOnly|Full}`]	Specifies the type of rights to be assigned to the user. • **JoinOnly** - Requires the administrator to reset the computer account before the user can join the computer to the domain. • **Full** - Gives full access to the user, which includes the right to join the computer to the domain.
[/JoinDomain:`{Yes|No}`]	Specifies whether the computer should be joined to the domain as this computer account during operating system installation. The default value is **Yes**.
[/BootImagepath:`<Relativepath>`]	Specifies the relative path from the **remoteInstall** folder to the boot image that this computer should use.
[/OU:`<DN of OU>`]	The distinguished name of the organizational unit where the computer account object should be created. For example: **OU=MyOU,CN=Test, DC=Domain,DC=com**. The default location is the default computer's container.
[/Domain:`<Domain>`]	The domain where the computer account object should be created. The default location is the local domain.

Examples

To add a computer by using a MAC address, type:

```
wdsutil /add-Device /Device:computer1 /ID:00-B0-56-88-2F-DC
```

To add a computer by using a GUID string, type:

```
wdsutil /add-Device /Device:computer1 /ID:{E8A3EFAC-201F-4E69-953F-
B2DAA1E8B1B6} /ReferralServer:WDSServer1
```

```
/BootProgram:boot\x86\pxeboot.com/WDSClientUnattend:WDSClientUnattend\unatte
nd.xml /User:Domain\MyUser/JoinRights:Full
/BootImagepath:boot\x86\images\boot.wim /OU:OU=MyOU,CN=Test,DC=Domain,DC=com
```

Related links

- Command-Line Syntax Key
- wdsutil get-alldevices command
- wdsutil get-device command
- wdsutil set-device command
- Windows Deployment Services cmdlets
- New-WdsClient

wdsutil add-drivergroup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds a driver group to the server.

Syntax

```
wdsutil /add-DriverGroup /DriverGroup:<Groupname>\n\ [/Server:<Servername>]
[/Enabled:{Yes | No}] [/Applicability:{Matched | All}] [/Filtertype:
<Filtertype> /Policy:{Include | Exclude} /Value:<Value> [/Value:<Value>
...]]
```

Parameters

Parameter	Description
/DriverGroup:`<Groupname>`	Specifies the name of the new driver group.
/Server:`<Servername>`	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.
/Enabled:`{Yes|No}`	Enables or disables the package.
/Applicability:`{Matched|All}`	Specifies which packages to install if the filter criteria are met. **Matched** means install only the driver packages that match a client s hardware. **All** means install all the packages to clients regardless of their hardware.

Parameter	Description
/Filtertype:`<Filtertype>`	Specifies the type of the filter to add to the group. You can specify multiple filter types in a single command. Each filter type must be followed by **/Policy** and at least one **/Value**. Valid values include: • BiosVendor • Biosversion • Chassistype • Manufacturer • Uuid • Osversion • Osedition • OsLanguage For information about getting values for all other filter types, see Driver Group Filters.
[/Policy:`{Include|Exclude}`]	Specifies the policy to be set on the filter. If **/Policy** is set to **Include**, client computers that match the filter are allowed to install the drivers in this group. If **/Policy** is set to **Exclude**, then client computers that match the filter are not allowed to install the drivers in this group.
[/Value:`<Value>`]	Specifies the client value that corresponds to **/Filtertype**. You can specify multiple values for a single type. For information about acceptable filter type values, see Driver Group Filters.

Examples

To add a driver group, type either:

```
wdsutil /add-DriverGroup /DriverGroup:printerdrivers /Enabled:Yes
```

```
wdsutil /add-DriverGroup /DriverGroup:printerdrivers /Applicability:All
/Filtertype:Manufacturer /Policy:Include /Value:Name1
/Filtertype:Chassistype /Policy:Exclude /Value:Tower /Value:MiniTower
```

Related links

- Command-Line Syntax Key

- wdsutil add-drivergrouppackage command
- wdsutil add-drivergrouppackages command
- wdsutil add-drivergroupfilter command
- Windows Deployment Services cmdlets

add-DriverGroupFilter

Article • 02/03/2023

Adds a filter to a driver group on a server.

Syntax

```
wdsutil /Add-DriverGroupFilter /DriverGroup:<Group Name> [/Server:<Server name>] /FilterType:<Filter Type> /Policy:{Include | Exclude} /Value:<Value> [/Value:<Value> ...]
```

Parameters

Parameter	Description
/DriverGroup:`<Groupname>`	Specifies the name of the new driver group.
/Server:`<Servername>`	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.
/Filtertype:`<Filtertype>`	Specifies the type of the filter to add to the group. You can specify multiple filter types in a single command. Each filter type must be followed by **/Policy** and at least one **/Value**. Valid values include: • BiosVendor • Biosversion • Chassistype • Manufacturer • Uuid • Osversion • Osedition • OsLanguage For information about getting values for all other filter types, see Driver Group Filters.
[/Policy:`{Include|Exclude}`]	Specifies the policy to be set on the filter. If **/Policy** is set to **Include**, client computers that match the filter are allowed to install the drivers in this group. If **/Policy** is set to **Exclude**, then client computers that match the filter are not allowed to install the drivers in this group.

Parameter	Description
[/Value:`<Value>`]	Specifies the client value that corresponds to **/Filtertype**. You can specify multiple values for a single type. For information about acceptable filter type values, see Driver Group Filters.

Examples

To add a filter to a driver group, type either:

```
wdsutil /Add-DriverGroupFilter /DriverGroup:PrinterDrivers
/FilterType:Manufacturer /Policy:Include /Value:Name1 /Value:Name2
```

```
wdsutil /Add-DriverGroupFilter /DriverGroup:PrinterDrivers
/FilterType:Manufacturer /Policy:Include /Value:Name1
/FilterType:ChassisType /Policy:Exclude /Value:Tower /Value:MiniTower
```

Related links

- Command-Line Syntax Key
- wdsutil add-drivergrouppackage command
- wdsutil add-drivergrouppackages command
- wdsutil add-drivergroup command
- Windows Deployment Services cmdlets

wdsutil add-drivergrouppackage

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds a driver package to a driver group.

Syntax

```
wdsutil /add-DriverGroupPackage /DriverGroup:<Group Name> [/Server:<Server Name>] {/DriverPackage:<Name> | /PackageId:<ID>}
```

Parameters

Parameter	Description
/DriverGroup:`<Groupname>`	Specifies the name of the new driver group.
/Server:`<Servername>`	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.
/DriverPackage:`<Name>`	Specifies the name of the driver package to be added to the group. You must specify this option if the driver package cannot be uniquely identified by name.
/PackageId:`<ID>`	Specifies the ID for a package. To find the Package ID, select the driver group that the package is in (or the **All Packages** node), right-click the package, and then select **Properties**. The Package ID is listed on the **General** tab, for example: **{DD098D20-1850-4fc8-8E35-EA24A1BEFF5E}**.

Examples

To add a driver group package, type either:

```
wdsutil /add-DriverGroupPackage /DriverGroup:printerdrivers /PackageId:{4D36E972-E325-11CE-Bfc1-08002BE10318}
```

```
wdsutil /add-DriverGroupPackage /DriverGroup:printerdrivers
/DriverPackage:XYZ
```

Related links

- Command-Line Syntax Key
- wdsutil add-drivergroupfilter command
- wdsutil add-drivergrouppackages command
- wdsutil add-drivergroup command
- Windows Deployment Services cmdlets

wdsutil add-drivergrouppackages

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds driver group packages.

Syntax

```
wdsutil /add-DriverGroupPackages /DriverGroup:<Group Name> [/Server:<Server Name>] /Filtertype:<Filter type> /Operator:{Equal | NotEqual | GreaterOrEqual | LessOrEqual | Contains} /Value:<Value> [/Value:<Value>]
```

Parameters

Parameter	Description
/DriverGroup:`<Groupname>`	Specifies the name of the new driver group.
/Server:`<Servername>`	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.

Parameter	Description
/Filtertype:`<Filtertype>`	Specifies the type of the driver package to search for. You can specify multiple attributes in a single command. You must also specify **/Operator** and **/Value** with this option. Valid values include: • PackageId • PackageName • PackageEnabled • Packagedateadded • PackageInfFilename • PackageClass PackageProvider • PackageArchitecture • PackageLocale • PackageSigned • PackagedatePublished • Packageversion • Driverdescription • DriverManufacturer • DriverHardwareId • DrivercompatibleId • DriverExcludeId • DriverGroupId • DriverGroupName** .
/Operator:`{Equal|NotEqual|GreaterOrEqual|LessOrEqual|Contains}`	Specifies the relationship between the attribute and the values. You can only specify **Contains** with string attributes. You can only specify **Equal**, **NotEqual**, **GreaterOrEqual** and **LessOrEqual** with date and version attributes.
/Value:`<Value>`	Specifies the client value corresponding to **/Filtertype**. You can specify multiple values for a single **/Filtertype**. The available values for each filter are:

Parameter	Description
	• **PackageId** - Specify a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318} • **PackageName** - Specify any string value • **PackageEnabled** - Specify **Yes** or **No** • **Packagedateadded** - Specify the date in the following format: YYYY/MM/DD • **PackageInfFilename** - Specify any string value • **PackageClass** - Specify a valid class name or class GUID. For example: **DiskDrive**, **Net**, or {4d36e972-e325-11ce-bfc1-08002be10318} • **PackageProvider** - Specify any string value • **PackageArchitecture** - Specify **x86**, **x64**, or **ia64** • **PackageLocale** - Specify a valid language identifier. For example: **en-US** or **es-ES** • **PackageSigned** - Specify **Yes** or **No** • **PackagedatePublished** - Specify the date in the following format: YYYY/MM/DD • **Packageversion** - Specify the version in the following format: a.b.x.y. For example: 6.1.0.0 • **Driverdescription** - Specify any string

Parameter	Description
	value • **DriverManufacturer** - Specify any string value • **DriverHardwareId** - Specify any string value • **DrivercompatibleId** - Specify any string value • **DriverExcludeId** - Specify any string value • **DriverGroupId** - Specify a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318} • **DriverGroupName** - Specify any string value For more information about these values, see Driver and Package attributes.

Examples

To add a driver group package, type either:

```
wdsutil /verbose /add-DriverGroupPackages /DriverGroup:printerdrivers
/Filtertype:PackageClass /Operator:Equal /Value:printer
/Filtertype:DriverManufacturer /Operator:NotEqual /Value:Name1 /Value:Name2
```

```
wdsutil /verbose /add-DriverGroupPackages /DriverGroup:DisplayDriversX86
/Filtertype:PackageClass /Operator:Equal /Value:Display
/Filtertype:PackageArchitecture /Operator:Equal /Value:x86
/Filtertype:Packagedateadded /Operator:LessOrEqual /Value:2008/01/01
```

Related links

- Command-Line Syntax Key
- wdsutil add-driverpackage command
- wdsutil add-drivergrouppackage command
- wdsutil add-alldriverpackages command
- Windows Deployment Services cmdlets

add-DriverPackage

Article • 02/03/2023

Adds a driver package to the server.

Syntax

```
wdsutil /Add-DriverPackage /InfFile:<Inf File path> [/Server:<Server name>]
[/Architecture:{x86 | ia64 | x64}] [/DriverGroup:<Group Name>] [/Name:
<Friendly Name>]
```

Parameters

Parameter	Description
/InfFile:`<InfFilepath>`	Specifies the full path of the .inf file to add.
[/Server:`<Servername>`]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.
[/Architecture:`{x86 | ia64 | x64}`]	Specifies the architecture type for the driver package.
[/DriverGroup:`<groupname>`]	Specifies the name of the driver group to which the packages should be added.
[/Name:`<friendlyname>`]	Specifies the friendly name for the driver package.

Examples

To add a driver package, type either:

```
wdsutil /verbose /Add-DriverPackage /InfFile:C:\Temp\Display.inf
```

```
wdsutil /Add-DriverPackage /Server:MyWDSServer /InfFile:C:\Temp\Display.inf
/Architecture:x86 /DriverGroup:x86Drivers /Name:Display Driver
```

Related links

- Command-Line Syntax Key
- wdsutil add-drivergrouppackage command
- wdsutil add-alldriverpackages command
- Windows Deployment Services cmdlets

wdsutil add-image

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds images to a Windows Deployment Services server.

Syntax

For boot images, use the following syntax:

```
wdsutil /Add-Image /ImageFile:<wim file path> [/Server:<Server name>
/ImageType:Boot [/SkipVerify] [/Name:<Image name>] [/Description:<Image
description>] [/Filename:<New wim file name>]
```

For install images, use the following syntax:

```
wdsutil /Add-Image /ImageFile:<wim filepath> [/Server:<Servername>]
/ImageType:Install [/SkipVerify] /ImageGroup:<Image group name>]
[/SingleImage:<Single image name>] [/Name:<Name>] [/Description:
<Description>] [/Filename:<File name>] [/UnattendFile:<Unattend file path>]
```

Parameters

Parameter	Description
/ImageFile:`<.wim filepath>`	Specifies the full path and file name of the Windows Image (.wim) file that contains the images to be added.
[/Server:`<Servername>`]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If a server name is not specified, the local server is used.
[/ImageType:`{Boot | Install}`]	Specifies the type of images to be added.
[/SkipVerify]	Specifies that integrity verification will not be performed on the source image file before the image is added.

Parameter	Description
[/Name:`<Name>`]	Sets the display name of the image.
[/Description:`<Description>`]	Sets the description of the image.
[/Filename:`<Filename>`]	Specifies the new file name for the .wim file. This enables you to change the filename of the .wim file when adding the image. If you don't specify a filename, the source image filename is used. In all cases, Windows Deployment Services checks to determine whether the file name is unique in the boot image store of the destination computer.
/ImageGroup:`<Imagegroupname>`]	Specifies the name of the image group in which the images are to be added. If more than one image group exists on the server, the image group must be specified. If you don't specify the image group, and an image group doesn't already exist, a new image group is created. Otherwise, the existing image group is used.
[/SingleImage:`<Singleimagename>`] [/Name:`<Name>`] [/Description: `<Description>`]	Copies the specified single image out of a .wim file, and sets the image's display name and description.
[/UnattendFile:`<Unattendfilepath>`]	Specifies the full path to the unattended installation file to be associated with the images that are being added. If **/SingleImage** isn't specified, the same unattend file is associated with all of the images in the .wim file.

Examples

To add a boot image, type:

```
wdsutil /Add-Image /ImageFile:"C:\MyFolder\Boot.wim" /ImageType:Boot
wdsutil /Verbose /Progress /Add-Image /ImageFile:\\MyServer\Share\Boot.wim
/Server:MyWDSServer /ImageType:Boot /Name:"My WinPE Image"
/Description:"WinPE Image containing the WDS Client" /Filename:WDSBoot.wim
```

To add an install image, type one of the following:

```
wdsutil /Add-Image /ImageFile:"C:\MyFolder\Install.wim" /ImageType:Install
wdsutil /Verbose /Progress /Add-Image
/ImageFile:\\MyServer\Share\Install.wim /Server:MyWDSServer
/ImageType:Install /ImageGroup:ImageGroup1
```

```
/SingleImage:"Windows Pro" /Name:"My WDS Image" /Description:"Windows Pro
image with Microsoft Office" /Filename:"Win Pro.wim"
/UnattendFile:"\\server\share\unattend.xml"
```

Related links

- Command-Line Syntax Key
- wdsutil copy-image command
- wdsutil export-image command
- wdsutil get-image command
- wdsutil remove-image command
- wdsutil replace-image command
- wdsutil set-image command
- Windows Deployment Services cmdlets

wdsutil add-imagedriverpackage

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds a driver package that is in the driver store to an existing boot image on the server.

Syntax

```
wdsutil /add-ImageDriverPackage [/Server:<Servername>] [media:<Imagename>]
[mediatype:Boot] [/Architecture:{x86 | ia64 | x64}] [/Filename:<Filename>]
{/DriverPackage:<Package Name> | /PackageId:<ID>}
```

Parameters

Parameter	Description
[/Server:`<Servername>`]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If a server name is not specified, the local server is used.
[media:`<Imagename>`]	Specifies the name of the image to add the driver to.
[mediatype:Boot]	Specifies the type of image to add the driver to. Driver packages can only be added to boot images.
[/Architecture:`{x86 | ia64 | x64}`]	Specifies the architecture of the boot image. Because it's possible to have the same image name for boot images in different architectures, you should specify the architecture to ensure the correct image is used.
[/Filename:`<Filename>`]	Specifies the name of the file. If the image cannot be uniquely identified by name, the file name must be specified.
[/DriverPackage:`<Name>`	Specifies the name of the driver package to add to the image.
[/PackageId:`<ID>`]	Specifies the Windows Deployment Services ID of the driver package. You must specify this option if the driver package can't be uniquely identified by name. To find the Package ID, select the driver group that the package is in (or the **All Packages** node), right-click the package, and then select **Properties**. The Package ID is listed on the **General** tab. For example: {DD098D20-1850-4fc8-8E35-EA24A1BEFF5E}.

Examples

To add a driver package to a boot image, type either:

```
wdsutil /add-ImageDriverPackagmedia:WinPE Boot Imagemediatype:Boot
/Architecture:x86 /DriverPackage:XYZ
```

```
wdsutil /verbose /add-ImageDriverPackagmedia:WinPE Boot Image
/Server:MyWDSServemediatype:Boot /Architecture:x64 /PackageId:{4D36E972-
E325-11CE-Bfc1-08002BE10318}
```

Related links

- Command-Line Syntax Key
- wdsutil add-imagedriverpackages command
- Windows Deployment Services cmdlets

wdsutil add-imagedriverpackages

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds driver packages from the driver store to a boot image.

Syntax

```
wdsutil /add-ImageDriverPackages [/Server:<Server name>media:<Image
namemediatype:Boot /Architecture:{x86 | ia64 | x64} [/Filename:<File name>]
/Filtertype:<Filter type> /Operator:{Equal | NotEqual | GreaterOrEqual |
LessOrEqual | Contains} /Value:<Value> [/Value:<Value> ...]
```

Parameters

Parameter	Description
[/Server:`<Servername>`]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If a server name is not specified, the local server is used.
[media:`<Imagename>`]	Specifies the name of the image to add the driver to.
[mediatype:Boot]	Specifies the type of image to add the driver to. Driver packages can only be added to boot images.

Parameter	Description
[/Architecture:`{x86 | ia64 | x64}`]	Specifies the architecture of the boot image. Because it's possible to have the same image name for boot images in different architectures, you should specify the architecture to ensure the correct image is used.
[/Filename:`<Filename>`]	Specifies the name of the file. If the image cannot be uniquely identified by name, the file name must be specified.
/Filtertype:`<Filtertype>`	Specifies the attribute of the driver package to search for. You can specify multiple attributes in a single command. You must also specify **/Operator** and **/Value** with this option. Valid values include: • PackageId • PackageName • PackageEnabled • Packagedateadded • PackageInfFilename • PackageClass PackageProvider • PackageArchitecture • PackageLocale • PackageSigned • PackagedatePublished • Packageversion • Driverdescription • DriverManufacturer • DriverHardwareId • DrivercompatibleId • DriverExcludeId • DriverGroupId • DriverGroupName** .

Parameter	Description
/Operator:`{Equal|NotEqual|GreaterOrEqual|LessOrEqual|Contains}`	Specifies the relationship between the attribute and the values. You can only specify **Contains** with string attributes. You can only specify **GreaterOrEqual** and **LessOrEqual** with date and version attributes.
/Value:`<Value>`	Specifies the value to search for relative to the specified `<attribute>`. You can specify multiple values for a single **/Filtertype**. The available values for each filter are: • **PackageId** - Specify a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318} • **PackageName** - Specify any string value • **PackageEnabled** - Specify **Yes** or **No** • **Packagedateadded** - Specify the date in the following format: YYYY/MM/DD • **PackageInfFilename** - Specify any string value • **PackageClass** - Specify a valid class name or class GUID. For example: **DiskDrive**, **Net**, or {4d36e972-e325-11ce-bfc1-08002be10318} • **PackageProvider** - Specify any string value • **PackageArchitecture** - Specify **x86**, **x64**, or **ia64** • **PackageLocale** - Specify a valid

Parameter	Description
	language identifier. For example: **en-US** or **es-ES** • **PackageSigned** - Specify **Yes** or **No** • **PackagedatePublished** - Specify the date in the following format: YYYY/MM/DD • **Packageversion** - Specify the version in the following format: a.b.x.y. For example: 6.1.0.0 • **Driverdescription** - Specify any string value • **DriverManufacturer** - Specify any string value • **DriverHardwareId** - Specify any string value • **DrivercompatibleId** - Specify any string value • **DriverExcludeId** - Specify any string value • **DriverGroupId** - Specify a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318} • **DriverGroupName** - Specify any string value For more information about these values, see Driver and Package attributes.

Examples

To add driver packages to a boot image, type one of the following:

```
```

```
wdsutil /add-ImageDriverPackagemedia:WinPE Boot Imagemediatype:Boot
/Architecture:x86 /Filtertype:DriverGroupName /Operator:Equal /Value:x86Bus
/Filtertype:PackageProvider /Operator:Contains /Value:Provider1
/Filtertype:Packageversion /Operator:GreaterOrEqual /Value:6.1.0.0
```

```
wdsutil /verbose /add-ImageDriverPackagemedia: WinPE Boot Image
/Server:MyWDSServemediatype:Boot /Architecture:x64 /Filtertype:PackageClass
/Operator:Equal /Value:Net /Filtertype:DriverManufacturer /Operator:NotEqual
/Value:Name1 /Value:Name2 /Filtertype:Packagedateadded /Operator:LessOrEqual
/Value:2008/01/01
```

```
wdsutil /verbose /add-ImageDriverPackagemedia:WinPE Boot Image
/Server:MyWDSServemediatype:Boot /Architecture:x64 /Filtertype:PackageClass
/Operator:Equal /Value:Net /Value:System /Value:DiskDrive /Value:HDC
/Value:SCSIAdapter
```

Related links

- Command-Line Syntax Key
-
- wdsutil add-imagedriverpackage command
-
- wdsutil add-alldriverpackages command
- Windows Deployment Services cmdlets

wdsutil add-imagegroup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Adds an image group to a Windows Deployment Services server.

Syntax

```
wdsutil [Options] /add-ImageGroup imageGroup:<Imagegroupname> [/Server:
<Server name>]
```

Parameters

Parameter	Description
imageGroup:`<Imagegroupname>`	Specifies the name of the image to be added.
[/Server:`<Servername>`]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If a server name is not specified, the local server is used.

Examples

To add an image group, type either:

```
wdsutil /add-ImageGroup imageGroup:ImageGroup2
```

```
wdsutil /verbose /add-Imagegroup imageGroup:My Image Group
/Server:MyWDSServer
```

Related links

- Command-Line Syntax Key
- wdsutil get-allimagegroups command
- wdsutil get-imagegroup command
- wdsutil remove-imagegroup command
- wdsutil set-imagegroup command
- Windows Deployment Services cmdlets

wdsutil approve-autoadddevices

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Approves computers that are pending administrative approval. When the Auto-add policy is enabled, administrative approval is required before unknown computers (those that are not pre-staged) can install an image. You can enable this policy using the **PXE Response** tab of the server s properties page.

Syntax

```
wdsutil [Options] /Approve-AutoaddDevices [/Server:<Server name>]
/RequestId:{<Request ID>| ALL} [/MachineName:<Device name>] [/OU:<DN of OU>]
[/User:<Domain\User | User@Domain>] [/JoinRights:{JoinOnly | Full}]
[/JoinDomain:{Yes | No}] [/ReferralServer:<Server name>] [/BootProgram:
<Relative path>] [/WdsClientUnattend:<Relative path>] [/BootImagepath:
<Relative path>]
```

Parameters

Parameter	Description
/Server:`<Servername>`	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.
/RequestId:`{Request ID|ALL}`	Specifies the request ID assigned to the pending computer. Specify **ALL** to approve all pending computers.
/Machinename:`<Devicename>`	Specifies the name of the device to be added. You can't use this option when approving all computers.
[/OU:`<DN of OU>`]	The distinguished name of the organizational unit where the computer account object should be created. For example: **OU=MyOU,CN=Test, DC=Domain,DC=com**. The default location is the default computer's container.

Parameter	Description
[/User:`<Domain\User|User@Domain>`]	Sets permissions on the computer account object to give the specified user the necessary rights to join the computer to the domain.
[/JoinRights:`{JoinOnly|Full}`]	Specifies the type of rights to be assigned to the user. • **JoinOnly** - Requires the administrator to reset the computer account before the user can join the computer to the domain. • **Full** - Gives full access to the user, which includes the right to join the computer to the domain.
[/JoinDomain:`{Yes|No}`]	Specifies whether the computer should be joined to the domain as this computer account during operating system installation. The default value is **Yes**.
[/ReferralServer:`<Servername>`]	Specifies the name of the server to contact to download the network boot program and boot image by using Trivial File Transfer Protocol (tftp).
[/BootProgram:`<Relativepath>`]	Specifies the relative path from the **remoteInstall** folder to the network boot program that this computer should receive. For example: **boot\x86\pxeboot.com**.
[/WdsClientUnattend:`<Relativepath>`]	Specifies the relative path from the **remoteInstall** folder to the unattend file that automates the Windows Deployment Services client.
[/BootImagepath:`<Relativepath>`]	Specifies the relative path from the remoteInstall folder to the boot image that this computer should receive.

Examples

To approve the computer with a RequestId of 12, type:

```
wdsutil /Approve-AutoaddDevices /RequestId:12
```

To approve the computer with a RequestID of 20 and to deploy the image with the specified settings, type:

```
wdsutil /Approve-AutoaddDevices /RequestId:20 /MachineName:computer1
/OU:OU=Test,CN=company,DC=Domain,DC=Com /User:Domain\User1
```

```
/JoinRights:Full /ReferralServer:MyWDSServer
/BootProgram:boot\x86\pxeboot.n12
/WdsClientUnattend:WDSClientUnattend\Unattend.xml
/BootImagepath:boot\x86\images\boot.wim
```

To approve all pending computers, type:

```
wdsutil /verbose /Approve-AutoaddDevices /RequestId:ALL
```

Related links

- Command-Line Syntax Key
- wdsutil delete-autoadddevices command
- wdsutil get-autoadddevices command
- wdsutil reject-autoadddevices command
- Windows Deployment Services cmdlets

convert-riprepimage

Article • 02/03/2023

Converts an existing Remote Installation Preparation (RIPrep) image to Windows Image (.wim) format.

Syntax

```
wdsutil [Options] /Convert-RIPrepImage /FilePath:<Filepath and name>
/DestinationImage /FilePath:<Filepath and name> [/Name:<Name>]
[/Description:<Description>] [/InPlace] [/Overwrite:{Yes | No | Append}]
```

Parameters

Parameter	Description
/FilePath:`<Filepath and name>`	Specifies the full filepath and name of the .sif file that corresponds to the RIPrep image. This file is typically called Riprep.sif and is found in the **\Templates** subfolder of the folder that contains the RIPrep image.
/DestinationImage	Specifies the settings for the destination image. Uses the following options; • `/FilePath:<Filepath and name>` - Sets the full file path for the new file. For example: **C:\Temp\convert.wim** • [`/Name:<Name>`] - Sets the display name of the image. If no display name is specified, the display name of the source image is used. • [`/Description:<Description>`] - Sets the description of the image. • [/InPlace] - Specifies that the conversion should take place on the original RIPrep image and not on a copy of the original image, which is the default behavior. • [`/Overwrite:{Yes | No | Append}` - Sets whether this image should overwrite or append any existing files.

Examples

To convert the specified RIPrep.sif image to RIPREP.wim, type:

```
wdsutil /Convert-RiPrepImage /FilePath:R:\RemoteInstall\Setup\English
\Images\Win2k3.SP1\i386\Templates\riprep.sif /DestinationImage
```

```
/FilePath:C:\Temp\RIPREP.wim
```

To convert the specified RIPrep.sif image to RIPREP.wim with the specified name and description, and overwrite it with the new file if a file already exists, type:

```
wdsutil /Verbose /Progress /Convert-RiPrepImage /FilePath:\\Server
\RemInst\Setup\English\Images\WinXP.SP2\i386\Templates\riprep.sif
/DestinationImage /FilePath:\\Server\Share\RIPREP.wim /Name:WindowsXP image
/Description:Converted RIPREP image of WindowsXP /Overwrite:Append
```

Related links

- Command-Line Syntax Key
- Windows Deployment Services cmdlets

wdsutil copy commands

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies an image or a driver group.

Parameters

Parameter	Description
wdsutil copy-image command	Copies images that are within the same image group.
wdsutil copy-drivergroup command	Copies an existing driver group on the server.

Related links

- Command-Line Syntax Key
- Windows Deployment Services cmdlets

copy-drivergroup

Article • 02/03/2023

Duplicates an existing driver group on the server including the filters, driver packages, and enabled/disabled status.

Syntax

```
wdsutil /Copy-DriverGroup [/Server:<Server name>] /DriverGroup:<Source Groupname> /GroupName:<New Groupname>
```

Parameters

Parameter	Description
/Server:`<Servername>`	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.
/DriverGroup:`<Source Groupname>`	Specifies the name of the source driver group.
/GroupName:`<New Groupname>`	Specifies the name of the new driver group.

Examples

To copy a driver group, type either:

```
wdsutil /Copy-DriverGroup /Server:MyWdsServer /DriverGroup:PrinterDrivers /GroupName:X86PrinterDrivers
```

```
wdsutil /Copy-DriverGroup /DriverGroup:PrinterDrivers /GroupName:ColorPrinterDrivers
```

Related links

- Command-Line Syntax Key
- Windows Deployment Services cmdlets

wdsutil copy-image

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Copies images that are within the same image group. To copy images between image groups, use the wdsutil Export-Image command command and then the wdsutil add-Image command command.

Syntax

```
wdsutil [Options] /copy-Image image:<Image name> [/Server:<Server name>]
imagetype:Install imageGroup:<Image group name>] [/Filename:<File name>]
/DestinationImage /Name:<Name> /Filename:<File name> [/Description:
<Description>]
```

Parameters

Parameter	Description
image:`<Imagename>`	Specifies the name of the image to be copied.
[/Server:`<Servername>`]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
imagetype:Install	Specifies the type of image to be copied. This option must be set to **install**.
\imageGroup:`<Image groupname>`]	Specifies the image group that contains the image to be copied. If no image group is specified and only one group exists on the server, that image group is used by default. If more than one image group exists on the server, you must specify the image group.
[/Filename:`<Filename>`]	Specifies the file name of the image to be copied. If the source image cannot be uniquely identified by name, you must specify the file name.

Parameter	Description
/DestinationImage	Specifies the settings for the destination image. The valid values are: • /Name:`<Name>` - Sets the display name of the image to be copied. • /Filename:`<Filename>` - Sets the name of the destination image file that will contain the image copy. • [/Description:`<Description>`] - Sets the description of the image copy.

Examples

To create a copy of the specified image and name it WindowsVista.wim, type:

```
wdsutil /copy-Image image:Windows Vista with Office imagetype:Install
/DestinationImage /Name:copy of Windows Vista with Office /
Filename:WindowsVista.wim
```

To create a copy of the specified image, apply the specified settings, and name the copy WindowsVista.wim, type:

```
wdsutil /verbose /Progress /copy-Image image:Windows Vista with Office
/Server:MyWDSServe imagetype:Install imageGroup:ImageGroup1
/Filename:install.wim /DestinationImage /Name:copy of Windows Vista with
Office /Filename:WindowsVista.wim /Description:This is a copy of the
original Windows image with Office installed
```

Related links

- Command-Line Syntax Key
- wdsutil add-image command
- wdsutil export-image command
- wdsutil get-image command
- wdsutil remove-image command
- wdsutil replace-image command

- wdsutil set-image command
- Windows Deployment Services cmdlets

wdsutil delete-autoadddevices

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Deletes computers that are pending, rejected, or approved from the auto-add database. This database stores information about these computers on the server.

Syntax

```
wdsutil /delete-AutoaddDevices [/Server:<Servername>] /Devicetype:
{PendingDevices | RejectedDevices |ApprovedDevices}
```

Parameters

Parameter	Description
[/Server:`<Servername>`]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
/Devicetype:`{PendingDevices|RejectedDevices|ApprovedDevices}`	Specifies the type of computer to delete from the database. This type can be **PendingDevices**, which returns all computers in the database that have a status of pending, **RejectedDevices**, which returns all computers in the database that have a status of rejected, or **ApprovedDevices**, which returns all computers that have a status of approved.

Examples

To delete all rejected computers, type:

```
wdsutil /delete-AutoaddDevices /Devicetype:RejectedDevices
```

To delete all approved computers, type:

```
wdsutil /verbose /delete-AutoaddDevices /Server:MyWDSServer
/Devicetype:ApprovedDevices
```

Related links

- Command-Line Syntax Key
- wdsutil approve-autoadddevices command
- wdsutil get-autoadddevices command
- wdsutil reject-autoadddevices command
- Windows Deployment Services cmdlets

wdsutil disable commands

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Disables all services for Windows Deployment Services.

Parameters

Parameter	Description
wdsutil disable-server command	Disables all Windows Deployment Services services on a specified server (Deployment Server).
wdsutil disable-transportserver command	Disables all Windows Deployment Services services on a specified Transport Server.

Related links

- Command-Line Syntax Key
- Windows Deployment Services cmdlets

wdsutil disable-server

Article • 02/03/2023

Disables all services for a Windows Deployment Services server.

Syntax

```
wdsutil [Options] /Disable-Server [/Server:<Server name>]
```

Parameters

Parameter	Description
[/Server:`<Servername>`]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Examples

To disable the server, type either:

```
wdsutil /Disable-Server
```

```
wdsutil /Verbose /Disable-Server /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key
- Windows Deployment Services cmdlets

wdsutil disable-transportserver

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Disables all services for a Transport Server.

Syntax

```
wdsutil [Options] /Disable-TransportServer [/Server:<Servername>]
```

Parameters

Parameter	Description
[/Server:`<Servername>`]	Specifies the name of the Transport Server to be disabled. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no Transport Server name is specified, the local server will be used.

Examples

To disable the server, type either:

```
wdsutil /Disable-TransportServer
```

```
wdsutil /verbose /Disable-TransportServer /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key

- wdsutil enable-transportserver command
- wdsutil get-transportserver command
- wdsutil set-transportserver command
- wdsutil start-transportserver command
- wdsutil stop-transportserver command
- Windows Deployment Services cmdlets

wdsutil disconnect-client

Article • 02/03/2023

Disconnects a client from a multicast transmission or namespace. Unless you specify **/Force**, the client will fall back to another transfer method (if it's supported by the client).

Syntax

```
wdsutil /Disconnect-Client /ClientId:<Client ID> [/Server:<Server name>]
[/Force]
```

Parameters

Parameter	Description
/ClientId:`<ClientID>`	Specifies the ID of the client to be disconnected. To view the ID of a client, run the `wdsutil /get-multicasttransmission /show:clients` command.
[/Server:`<Servername>`]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
[/Force]	Stops the installation completely and does not use a fallback method. Because Wdsmcast.exe doesn't support any fallback mechanism, the default behavior is as follows: • **If you're using the Windows Deployment Services client:** The client continues the installation by using unicasting. • **If you aren't using the Windows Deployment Services client:** The installation fails. **Important:** We strongly recommend using this parameter cautiously because if the installation fails, the computer can be left in an unusable state.

Examples

To disconnect a client, type:

```
wdsutil /Disconnect-Client /ClientId:1
```

To disconnect a client and force the installation to fail, type:

```
wdsutil /Disconnect-Client /Server:MyWDSServer /ClientId:1 /Force
```

Related links

- Command-Line Syntax Key
- wdsutil get-multicasttransmission command
- Windows Deployment Services cmdlets

wdsutil enable commands

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables all services for Windows Deployment Services.

Parameters

Parameter	Description
wdsutil enable-server command	Enables all services on a specified Windows Deployment Services server (Deployment Server).
wdsutil enable-transportserver command	Enables all services on a specified Transport Server.

Related links

- Command-Line Syntax Key
- Windows Deployment Services cmdlets

wdsutil enable-server

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables all services for Windows Deployment Services.

Syntax

```
wdsutil [options] /Enable-Server [/Server:<Servername>]
```

Parameters

Parameter	Description
[/Server:`<Servername>`]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.

Examples

To enable the services on the server, type either:

```
wdsutil /Enable-Server
```

```
wdsutil /verbose /Enable-Server /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key

- wdsutil disable-server command
- wdsutil get-Server command
- wdsutil initialize-server command
- wdsutil set-server command
- wdsutil start-server command
- wdsutil stop-server command
- wdsutil uninitialize-server command
- Windows Deployment Services cmdlets

wdsutil enable-transportserver

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Enables all services for the Transport Server.

Syntax

```
wdsutil [options] /Enable-TransportServer [/Server:<Servername>]
```

Parameters

Parameter	Description
[/Server:`<Servername>`]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.

Examples

To enable the services on the server, type either:

```
wdsutil /Enable-TransportServer
```

```
wdsutil /verbose /Enable-TransportServer /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key

- wdsutil disable-transportserver command
- wdsutil get-transportserver command
- wdsutil set-transportserver command
- wdsutil start-transportserver command
- wdsutil stop-transportserver command
- Windows Deployment Services cmdlets

wdsutil export-image

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Exports an existing image from the image store to another Windows Image (.wim) file.

Syntax

For boot images:

```
wdsutil [options] /Export-Image image:<Image name> [/Server:<Servername>]
    imagetype:Boot /Architecture:{x86 | ia64 | x64} [/Filename:<Filename>]
     /DestinationImage
         /Filepath:<Filepath and name>
         [/Name:<Name>]
         [/Description:<Description>]
     [/Overwrite:{Yes | No}]
```

For install images:

```
wdsutil [options] /Export-Image image:<Image name> [/Server:<Servername>]
    imagetype:Install imageGroup:<Image group name>]
     [/Filename:<Filename>]
     /DestinationImage
         /Filepath:<Filepath and name>
         [/Name:<Name>]
         [/Description:<Description>]
     [/Overwrite:{Yes | No | append}]
```

Parameters

Parameter	Description
image:`<Imagename>`	Specifies the name of the image to be exported.

Parameter	Description
[/Server:`<Servername>`]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
imagetype:`{Boot|Install}`	Specifies the type of image to be exported.
\imageGroup:`<Image group name>`]	Specifies the image group containing the image to be exported. If no image group name is specified and only one image group exists on the server, that image group will be used by default. If more than one image group exists on the server, the image group must be specified.
/Architecture:`{x86|ia64|x64}`	Specifies the architecture of the image to be exported. Because it is possible to have the same image name for boot images in different architectures, specifying the architecture value ensures that the correct image will be returned.
[/Filename:`<Filename>`]	if the image cannot be uniquely identified by name, the file name must be specified.
/DestinationImage	Specifies the settings for the destination image. You can specify these settings using the following options: • `/Filepath:<Filepath and name>` - Specifies the full file path for the new image. • `[/Name:<Name>]` - Sets the display name of the image. If no name is specified, the display name of the source image will be used. • `[/Description: <Description>]` - Sets the description of the image.
[/Overwrite:`{Yes|No|append}`]	Determines whether the file specified in the **/DestinationImage** option will be overwritten if an existing file with that name already exists at the /Filepath. The **Yes** option causes the existing file to be overwritten, the **No** option (default) causes an error to occur if a file with the same name already exists, and the **append** option causes the generated image to be appended as a new image within the existing .wim file.

Examples

To export a boot image, type either:

```
wdsutil /Export-Image image:WinPE boot image imagetype:Boot
/Architecture:x86 /DestinationImage /Filepath:C:\temp\boot.wim
```

```
wdsutil /verbose /Progress /Export-Image image:WinPE boot image
/Server:MyWDSServer imagetype:Boot /Architecture:x64 /Filename:boot.wim
/DestinationImage /Filepath:\\Server\Share\ExportImage.wim /Name:Exported
WinPE image /Description:WinPE Image from WDS server /Overwrite:Yes
```

To export an install image, type either:

```
wdsutil /Export-Image image:Windows Vista with Office imagetype:Install
/DestinationImage /Filepath:C:\Temp\Install.wim
```

```
wdsutil /verbose /Progress /Export-Image image:Windows Vista with Office
/Server:MyWDSServer imagetype:Instal imageGroup:ImageGroup1
/Filename:install.wim /DestinationImage /Filepath:\\server\share\export.wim
/Name:Exported Windows image /Description:Windows Vista image from WDS
server /Overwrite:append
```

Related links

- Command-Line Syntax Key
- wdsutil add-image command
- wdsutil copy-image command
- wdsutil get-image command
- wdsutil remove-image command
- wdsutil replace-image command
- wdsutil set-image command
- Windows Deployment Services cmdlets

wdsutil get

Article • 08/20/2024

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves properties or attributes about the specified object.

Subcommands

Expand table

Subcommand	Description
wdsutil get-alldevices command	Displays information about all prestaged computers.
wdsutil get-allImagegroups command	Displays information about all image groups.
wdsutil get-allimages command	Displays information about all images.
wdsutil get-allmulticasttransmissions command	Displays the attributes of all multicast transmissions.
wdsutil get-allnamespaces command	Displays the attributes of all namespaces.
wdsutil get-allservers command	Displays information about all Windows Deployment Services servers.
wdsutil get-autoadddevices command	Displays computers that are pending administrative approval on a specified server.
wdsutil get-device command	Displays the attributes of a pending computer.
wdsutil get-image command	Displays the attributes of an existing image.
wdsutil get-imagefile command	Displays information about images in a specified `.wim` file.
wdsutil get-imagegroup command	Displays information about a specified image group.
wdsutil get-multicasttransmission command	Displays the attributes of a specified multicast transmission.
wdsutil get-namespace command	Displays the attributes of a specified namespace.

Subcommand	Description
wdsutil get-server command	Displays information about a specified Windows Deployment Services server.
wdsutil get-transportserver command	Displays information about a specified Transport Server.
wdsutil get-driverpackage command	Displays information about driver packages on a server.
wdsutil get-driverpackagefile command	Displays information about driver package, including the drivers and files it contains.
wdsutil get-alldrivergroups command	Displays information about all the driver groups on server.
wdsutil get-drivergroup command	Displays information about driver groups on a server.
wdsutil get-alldriverpackages command	Displays information about all the driver packages on a server that match the specified search criteria.
wdsutil get-driverpackagefile command	Displays information about a driver package, including the drivers and files it contains.

Feedback

Was this page helpful? Yes No

wdsutil get-alldevices

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays the Windows Deployment Services properties of all pre-staged computers. A pre-staged computer is a physical computer that has been linked to a computer account in active directory Domain Services.

Syntax

```
wdsutil [options] /get-alldevices [/forest:{Yes | No}] [/referralserver:<servername>]
```

Parameters

Parameter	Description
`[/forest:{Yes | No}]`	Specifies whether Windows Deployment Services should return computers in the entire forest or the local domain. The default setting is **No**, meaning that only the computers in the local domain are returned.
`[/referralserver:<servername>]`	Returns only those computers that are pre-staged for the specified server.

Examples

To view all computers, type either:

```
wdsutil /get-alldevices
```

```
wdsutil /verbose /get-alldevices /forest:Yes /referralserver:MyWDSServer
```

Related links

- Command-Line Syntax Key
- wdsutil set-device command
- wdsutil add-device command
- wdsutil get-device command

wdsutil get-alldrivergroups

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about all the driver groups on a server.

Syntax

```
wdsutil /get-alldrivergroups [/server:<servername>] [/show:{packagemetadata | filters | all}]
```

Parameters

Parameter	Description
`[/server:<servername>]`	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.
`/show:{packagemetadata | filters | all}]`	Displays the metadata for all the driver packages in the specified group. **PackageMetaData** displays information about all the filters for the driver group. **Filters** displays the metadata for all driver packages and filters for the group.

Examples

To view information about a driver file, type either:

```
wdsutil /get-alldrivergroups /server:MyWdsServer /show:All
```

```
wdsutil /get-alldrivergroups [/show:packagemetadata]
```

Related links

- Command-Line Syntax Key
-
- wdsutil get-drivergroup command

wdsutil get-alldriverpackages

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about all the driver packages on a server that match the specified search criteria.

Syntax

```
wdsutil /get-alldriverpackages [/server:<servername>] [/show:{drivers | files | all}] [/filtertype:<filtertype> /operator:{equal | notequal | greaterorequal | lessorequal | contains} /value:<value> [/value:<value> ...]]
```

Parameters

Parameter	Description
`[/server:<servername>]`	The name of the server. This can be the NetBIOS name or the FQDN. If a server name isn't specified, the local server is used.
`[/show:{drivers | files | all}]`	Indicates the package information to display. If **/show** isn't specified, the default is to return only the driver package metadata. **Drivers** displays the list of drivers in the package, **files** displays the list of files in the package, and **all** displays drivers and files.

Parameter	Description
`/filtertype:<filtertype>`	Specifies the attribute of the driver package to search for. You can specify multiple attributes in a single command. You must also specify **/operator** and **/value** with this option. The `<filtertype>` can be one of the following: • PackageId • PackageName • PackageEnabled • Packagedateadded • PackageInfFilename • PackageClass • PackageProvider • PackageArchitecture • PackageLocale • PackageSigned • PackagedatePublished • Packageversion • Driverdescription • DriverManufacturer • DriverHardwareId • DrivercompatibleId • DriverGroupId • DriverGroupName
`/operator:{equal | notequal | greaterorequal | lessorequal | contains}`	Specifies the relationship between the attribute and the values. You can specify **contains** only with string attributes. You can specify **greaterorequal** and **lessorequal** only with date and version attributes.

Parameter	Description
`/value:<value>`	Specifies the value to search on for the specified `<attribute>`. You can specify multiple values for a single **/filtertype**. The list below outlines the attributes you can specify for each filter. For more information about these attributes, see Driver and Package attributes. The attributes can include: • **PackageId.** Specifies a valid GUID. For example:{4d36e972-e325-11ce-bfc1-08002be10318}. • **PackageName.** Specifies any string value. • **PackageEnabled.** Specifies *Yes* or *No*. • **Packagedateadded.** Specifies the date in the following format: YYYY/MM/DD • **PackageInfFilename.** Specifies any string value. • **PackageClass.** Specifies a valid class name or class GUID. For example: *DiskDrive*, *Net*, or *{4d36e972-e325-11ce-bfc1-08002be10318}*. • **PackageProvider.** Specifies any string value. • **PackageArchitecture.** Specifies *x86*, *x64*, or *ia64*. • **PackagLocale.** Specifies a valid language identifier. For example: *en-US* or *es-ES*. • **PackageSigned.** Specifies **Yes** or **No**. • **PackagedatePublished.** Specifies the date in the following format: YYYY/MM/DD. • **Packageversion.** Specifies the version in the following format: a.b.x.y. For example: 6.1.0.0. • **Driverdescription.** Specifies any string value. • **DriverManufacturer.** Specifies any string value. • **DriverHardwareId.** Specifies any string value. • **DrivercompatibleId.** Specifies any string value. • **DriverExcludeId.** Specifies any string value. • **DriverGroupId.** Specifies a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318}. • **DriverGroupName.** Specifies any string value.

Examples

To display information, type either:

```
wdsutil /get-alldriverpackages /server:MyWdsServer /show:all
/filtertype:drivergroupname /operator:contains /value:printer
/filtertype:packagearchitecture /operator:equal /value:x64 /value:x86
```

```
wdsutil /get-alldriverpackages /show:drivers /filtertype:packagedateadded
/operator:greaterorequal /value:2008/01/01
```

Related links

- Command-Line Syntax Key
- wdsutil get-driverpackage command
- wdsutil get-driverpackagefile command

wdsutil get-allimagegroups

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves information about all image groups on a server and all images in those image groups.

Syntax

```
wdsutil [options] /get-allimagegroups [/server:<servername>] [/detailed]
```

Parameters

Parameter	Description
`[/server:<servername>]`	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
[/detailed]	Returns the image metadata from each image. If this parameter isn't used, the default behavior is to return only the image name, description, and file name for each image.

Examples

To view information about the image groups, type either:

```
wdsutil /get-allimagegroups
```

```
wdsutil /verbose /get-allimagegroups /server:MyWDSServer /detailed
```

Related links

- Command-Line Syntax Key
- wdsutil add-imagegroup command
- wdsutil remove-imagegroup command
- wdsutil set-imagegroup command

wdsutil get-allimages

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves information about all images on a server.

Syntax

```
wdsutil /get-allimages [/server:<servername>] /show:{boot | install |
legacyris | all} [/detailed]
```

Parameters

Parameter	Description
`[/server:<servername>]`	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
`/show:{boot | install | legacyris | all}`	Where **boot** returns only boot images, **install** returns install images as well as information about the image groups that contain them, **LegacyRis** returns only remote Installation Services (RIS) images, and **All** returns boot image information, install image information (including information about the image groups), and RIS image information.
[/detailed]	Indicates that all image metadata from each image should be returned. If this option is not used, the default behavior is to return only the image name, description, and file name.

Examples

To view information about the images, type either:

```
wdsutil /get-allimages /show:install
```

```
wdsutil /verbose /get-allimages /server:MyWDSServer /show:all /detailed
```

Related links

- Command-Line Syntax Key
- wdsutil add-image command
- wdsutil copy-image command
- wdsutil export-image command
- wdsutil remove-image command
- wdsutil replace-image command
- wdsutil set-image command

wdsutil get-allmulticasttransmissions

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about all multicast transmissions on a server.

Syntax

For Windows Server 2008:

```
wdsutil /Get-AllMulticastTransmissions [/Server:<Server name>]
[/Show:Clients] [/ExcludedeletePending]
```

For Windows Server 2008 R2:

```
wdsutil /Get-AllMulticastTransmissions [/Server:<Server name>] [/Show:{Boot
| Install | All}] [/details:Clients]  [/ExcludedeletePending]
```

Parameters

Parameter	Explanation
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
[/Show]	**Windows Server 2008** /Show:Clients - Displays information about client computers that are connected to the multicast transmissions. **Windows Server 2008 R2** Show: {Boot | Install | All} - The type of image to return. **Boot** returns only boot image transmissions. **Install** returns only install image transmissions. **All** returns both image types.

Parameter	Explanation
/details:clients	Only supported for Windows Server 2008 R2. If present, clients that are connected to the transmission will be displayed.
[/ExcludedeletePending]	Excludes any deactivated transmissions from the list.

Examples

To view information about all transmissions, type:

- Windows Server 2008: `wdsutil /Get-AllMulticastTransmissions`
- Windows Server 2008 R2: `wdsutil /Get-AllMulticastTransmissions /Show:All` To view information about all transmissions except deactivated transmissions, type:
- Windows Server 2008: `wdsutil /Get-AllMulticastTransmissions /Server:MyWDSServer /Show:Clients /ExcludedeletePending`
- Windows Server 2008 R2: `wdsutil /Get-AllMulticastTransmissions /Server:MyWDSServer /Show:All /details:Clients /ExcludedeletePending`

Related links

- Command-Line Syntax Key
- wdsutil get-multicasttransmission command
- wdsutil new-multicasttransmission command
- wdsutil remove-multicasttransmission command
- wdsutil start-multicasttransmission command

wdsutil get-allnamespaces

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about all namespaces on a server.

Syntax

Windows Server 2008:

```
wdsutil /Get-AllNamespaces [/Server:<Server name>] [/ContentProvider:<name>]
[/Show:Clients] [/ExcludedeletePending]
```

Windows Server 2008 R2:

```
wdsutil /Get-AllNamespaces [/Server:<Server name>] [/ContentProvider:<name>]
[/details:Clients] [/ExcludedeletePending]
```

Parameters

Parameter	Windows Server 2008	Windows Server 2008 R2
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.	
[/ContentProvider:<name>]	Displays the namespaces for the specified content provider only.	
[/Show:Clients]	Only supported for Windows Server 2008. Displays information about client computers that are connected to the namespace.	

Parameter	Windows Server 2008	Windows Server 2008 R2
[/details:Clients]	Only supported for Windows Server 2008 R2. Displays information about client computers that are connected to the namespace.	
[/ExcludedeletePending]	Excludes any deactivated transmissions from the list.	

Examples

To view all namespaces, type:

```
wdsutil /Get-AllNamespaces
```

To view all namespaces except those that are deactivated, type:

- Windows Server 2008

  ```
  wdsutil /Get-AllNamespaces /Server:MyWDSServer
  /ContentProvider:MyContentProv /Show:Clients /ExcludedeletePending
  ```

- Windows Server 2008 R2

  ```
  wdsutil /Get-AllNamespaces /Server:MyWDSServer
  /ContentProvider:MyContentProv /details:Clients /ExcludedeletePending
  ```

Related links

- Command-Line Syntax Key
- wdsutil new-namespace command
- wdsutil remove-namespace command
- wdsutil start-nmespace command

get-AllServers

Article • 02/03/2023

Retrieves information about all Windows Deployment Services servers.

> **Note**
>
> This command may take an extended amount of time to complete if there are many Windows Deployment Services servers in your environment or if the network connection linking the servers is slow.

Syntax

```
wdsutil [Options] /Get-AllServers /Show:{Config | Images | All} [/Detailed]
[/Forest:{Yes | No}]
```

Parameters

Parameter	Description
/Show: {Config	Images
[/Detailed]	When used in conjunction with the **/Show:Images** or **/Show:All**, returns all image metadata from each image. If the **/Detailed** option is not specified, the default behavior is to return the image name, description, and file name.
[/Forest: {Yes	No}]

Examples

To view information about all servers, type:

```
wdsutil /Get-AllServers /Show:Config
```

To view detailed information about all servers, type:

```
wdsutil /Verbose /Get-AllServers /Show:All /Detailed /Forest:Yes
```

Related links

- Command-Line Syntax Key

wdsutil get-autoadddevices

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays all computers that are in the Auto-add database on a Windows Deployment Services server.

Syntax

```
wdsutil [Options] /Get-AutoaddDevices [/Server:<Server name>] /Devicetype:
{PendingDevices | RejectedDevices | ApprovedDevices}
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
/Devicetype: {PendingDevices | RejectedDevices | ApprovedDevices}	Specifies the type of computer to return. - **PendingDevices** returns all computers in the database that have a status of pending. - **RejectedDevices** returns all computers in the database that have a status of rejected. - **ApprovedDevices** returns all computers in the database that have a status of approved.

Examples

To see all of the approved computers, type:

```
wdsutil /Get-AutoaddDevices /Devicetype:ApprovedDevices
```

To see all of the rejected computers, type:

```
wdsutil /verbose /Get-AutoaddDevices /Devicetype:RejectedDevices
/Server:MyWDSServer
```

Related links

- Command-Line Syntax Key
- wdsutil delete-autoadddevices command
- wdsutil approve-autoadddevices command
- wdsutil reject-autoadddevices command

wdsutil get-device

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves Windows Deployment Services information about a prestaged computer (that is, a physical computer that has been lined to a computer account in active directory Domain Services.

Syntax

```
wdsutil /Get-Device {/Device:<Device name> | /ID:<MAC or UUID>} [/Domain:
<Domain>] [/forest:{Yes | No}]
```

Parameters

Parameter	Description
/Device:<Device name>	Specifies the name of the computer (SAMAccountName).
/ID:<MAC or UUID>	Specifies either the MAC address or the UUID (GUID) of the computer, as shown in the following examples. Note that a valid GUID must be in one of two formats binary string or GUID string - **Binary string**: /ID:ACEFA3E81F20694E953EB2DAA1E8B1B6 - **MAC address**: 00B056882FDC (no dashes) or 00-B0-56-88-2F-DC (with dashes) - **GUID string**: /ID:E8A3EFAC-201F-4E69-953-B2DAA1E8B1B6
[/Domain:<Domain>]	Specifies the domain to be searched for the prestaged computer. The default value for this parameter is the local domain.
[/forest:{Yes | No}]	Specifies whether Windows Deployment Services should search the entire forest or the local domain. The default value is **No**, meaning that only the local domain will be searched.

Examples

To get information by using the computer name, type:

```
wdsutil /Get-Device /Device:computer1
```

To get information by using the MAC address, type:

```
wdsutil /verbose /Get-Device /ID:00-B0-56-88-2F-DC /Domain:MyDomain
```

To get information by using the GUID string, type:

```
wdsutil /verbose /Get-Device /ID:E8A3EFAC-201F-4E69-953-B2DAA1E8B1B6
/forest:Yes
```

Related links

- Command-Line Syntax Key
- wdsutil set-device command
- wdsutil add-device command
- wdsutil get-alldevices command

wdsutil get-drivergroup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about the driver groups on a server.

Syntax

```
wdsutil /Get-DriverGroup /DriverGroup:<Group Name> [/Server:<Server name>]
```

Parameters

Parameter	Description
/DriverGroup:<Group Name>	Specifies the name of the driver group.
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. if a server name is not specified, the local server is used.
[/Show:{PackageMetaData | Filters | All}]	Displays the metadata for all the driver packages in the specified group. **PackageMetaData** displays information about all the filters for the driver group. **Filters** displays the metadata for all driver packages and filters for the group.

Examples

To view information about a driver file, type:

```
wdsutil /Get-DriverGroup /DriverGroup:printerdrivers /Show:PackageMetaData
```

```
wdsutil /Get-DriverGroup /DriverGroup:printerdrivers /Server:MyWdsServer
/Show:Filters
```

Related links

- Command-Line Syntax Key
- wdsutil get-alldrivergroups command

get-DriverPackage

Article • 02/03/2023

Displays information about a driver package on the server.

Syntax

```
wdsutil /Get-DriverPackage [/Server:<Server name>] {/DriverPackage:<Package Name> | /PackageId:<ID>} [/Show:{Drivers | Files | All}]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If no server name is specified, the local server is used.
[/DriverPackage:<Name>]	Specifies the name of the driver package to show.
[/PackageId:<ID>]	Specifies the Windows Deployment Services ID of the driver package to show. You must specify the ID if the driver package cannot be uniquely identified by name.
[/Show: {Drivers	Files

Examples

To view information about a driver package, type one of the following:

```
wdsutil /Get-DriverPackage /PackageId:{4D36E972-E325-11CE-BFC1-08002BE10318}
```

```
wdsutil /Get-DriverPackage /DriverPackage:MyDriverPackage /Show:All
```

Related links

- Command-Line Syntax Key

wdsutil get-driverpackagefile

Article • 08/20/2024

Displays information about a driver package, including the drivers and files it contains.

Syntax

```
wdsutil /Get-DriverPackageFile /InfFile:<InfFilePath> [/Architecture:{x86 | x64 | arm | arm64}] [/Show:{Drivers | Files | All}]
```

Parameters

Expand table

Parameter	Description
/InfFile:`<InfFilePath>`	Specifies the full path and file name of the driver package `.inf` file.
/Architecture:`x86 | x64 | arm | arm64`	The architecture of the driver package.
/Show:`Drivers | Files | All`	Indicates the package information to display. The default, if `/show` isn't specified, is to return only the driver package metadata. • **Drivers** displays the list of drivers in the package. • **Files** displays the list of files in the package. • **All** displays drivers and files.

Examples

To view information about a driver file, type:

```
wdsutil /Get-DriverPackageFile /InfFile:C:\temp\1394.inf /Architecture:x86
```

Related links

- Command-Line Syntax Key

Feedback

Was this page helpful? Yes No

wdsutil get-image

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves information about an image.

Syntax

For boot images:

```
wdsutil [Options] /Get-Image image:<Image name> [/Server:<Server name>
imagetype:Boot /Architecture:{x86 | ia64 | x64} [/Filename:<File name>]
```

For install images:

```
wdsutil [Options] /Get-image image:<Image name> [/Server:<Server name>
imagetype:Install imagegroup:<Image group name>] [/Filename:<File name>]
```

Parameters

Parameter	Description
\image: <Image name>	Specifies the name of the image.
[/Server: <Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
imagetype: {Boot | Install}	Specifies the type of image.
/Architecture: {x86 | ia64 | x64}	Specifies the architecture of the image. Because it is possible to have the same image name for boot images in different architectures, specifying the architecture value ensures that the correct image is returned.

Parameter	Description
[/Filename: <File name>]	if the image cannot be uniquely identified by name, you must use this option to specify the file name.
\imagegroup: <Image group name>]	Specifies the image group that contains the image. If no image group is specified and only one image group exists on the server, that group will be used. If more than one image group exists on the server, you must use this parameter to specify the image group.

Examples

To retrieve information about a boot image, type one of the following:

```
wdsutil /Get-Image image:WinPE boot imagetype:Boot /Architecture:x86
wdsutil /verbose /Get-Image image:WinPE boot image /Server:MyWDSServer
imagetype:Boot /Architecture:x86 /Filename:boot.wim
```

To retrieve information about an install image, type one of the following:

```
wdsutil /Get-Image:Windows Vista with Office imagetype:Install
wdsutil /verbose /Get-Image:Windows Vista with Office /Server:MyWDSServer
imagetype:Install imagegroup:ImageGroup1 /Filename:install.wim
```

Related links

- Command-Line Syntax Key
- wdsutil add-image command
- wdsutil copy-image command
- wdsutil export-image command
- wdsutil remove-image command
- wdsutil replace-image command
- wdsutil set-image command

get-ImageFile

Article • 02/03/2023

Retrieves information about the images contained in a Windows Image (.wim) file.

Syntax

```
wdsutil [Options] /Get-ImageFile /ImageFile:<wim file path> [/Detailed]
```

Parameters

Parameter	Description
/ImageFile:<WIM file path>	Specifies the full path and file name of the .wim file.
[/Detailed]	Returns all image metadata from each image. If this option is not used, the default behavior is to return only the image name, description, and file name.

Examples

To view information about an image, type:

```
wdsutil /Get-ImageFile /ImageFile:C:\temp\install.wim
```

To view detailed information, type:

```
wdsutil /Verbose /Get-ImageFile /ImageFile:\\Server\Share\My Folder
\install.wim /Detailed
```

Related links

- Command-Line Syntax Key

wdsutil get-imagegroup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves information about an image group and the images within it.

Syntax

```
wdsutil [Options] /Get-ImageGroup ImageGroup:<Image group name> [/Server:
<Server name>] [/detailed]
```

Parameters

Parameter	Description
/ImageGroup:<Image group name>	Specifies the name of the image group.
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
[/detailed]	Returns the image metadata for each image. If this parameter is not use, the default behavior is to return only the image name, description, and file name.

Examples

To view information about an image group, type:

```
wdsutil /Get-ImageGroup ImageGroup:ImageGroup1
```

To view information including metadata, type:

```
```

```
wdsutil /verbose /Get-ImageGroup ImageGroup:ImageGroup1 /Server:MyWDSServer
/detailed
```

Related links

- Command-Line Syntax Key
- wdsutil add-imagegroup command
- wdsutil get-allimagegroups command
- wdsutil remove-imagegroup command
- wdsutil set-imagegroup command

wdsutil get-multicasttransmission

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about the multicast transmission for a specified image.

Syntax

Windows Server 2008

```
wdsutil [Options] /Get-MulticastTransmissiomedia:<Image name> [/Server:
<Server name>mediatype:InstallmediaGroup:<Image group name>]
[/Filename:<File name>] [/Show:Clients]
```

Windows Server 2008 R2

for boot image transmissions:

```
wdsutil [Options] /Get-MulticastTransmissiomedia:<Image name>
    [/Server:<Server name>]
    [/details:Clients]
  mediatype:Boot
    /Architecture:{x86 | ia64 | x64}
        [/Filename:<File name>]
```

for install image transmissions:

```
wdsutil [Options] /Get-MulticastTransmissiomedia:<Image name>
         [/Server:<Server name>]
         [/details:Clients]
       mediatype:Install
    mediaGroup:<Image Group>]
     [/Filename:<File name>]
```

Parameters

Parameter	Description
media:<Image name>	Displays the multicast transmission that is associated with this image.
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
/imagetype:Install	Specifies the image type. Note that this option must be set to **Install**.
/imagegroup:<Image group name>]	Specifies the image group that contains the image. If no image group name is specified and only one image group exists on the server, that image group is used. If more than one image group exists on the server, you must use this option to specify an image group.
/Architecture:{x86 | ia64 | x64}	Specifies the architecture of the boot image that is associated with the transmission. Because it is possible to have the same image name for boot images in different architectures, you should specify the architecture to ensure that the correct image is used.
[/Filename:<File name>]	Specifies the file that contains the image. If the image cannot be uniquely identified by name, you must use this option to specify the file name.
[/Show:Clients] or [/details:Clients]	Displays information about client computers that are connected to the multicast transmission.

Examples

Windows Server 2008

To view information about the transmission for an image named Vista with Office, type one of the following:

```
wdsutil /Get-MulticastTransmission:Vista with Office imagetype:Install
wdsutil /Get-MulticastTransmission /Server:MyWDSServer image:Vista with
Office imagetype:Install imageGroup:ImageGroup1 /Filename:install.wim
/Show:Clients
```

Windows Server 2008 R2

To view information about the transmission for an image named Vista with Office, type one of the following:

```
wdsutil /Get-MulticastTransmission:Vista with Office
 /Imagetype:Install
```

```
wdsutil /Get-MulticastTransmission /Server:MyWDSServer image:Vista with
Office imagetype:Install ImageGroup:ImageGroup1 /Filename:install.wim
/details:Clients
```

```
wdsutil /Get-MulticastTransmission /Server:MyWDSServer:X64 Boot
Imagetype:Boot /Architecture:x64 /Filename:boot.wim /details:Clients
```

Related links

- Command-Line Syntax Key
- wdsutil get-allmulticasttransmissions command
- wdsutil new-multicasttransmission command
- wdsutil remove-multicasttransmission command
- wdsutil start-multicasttransmission command

wdsutil get-namespace

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about a custom namespace.

Syntax

Windows Server 2008 R2

```
wdsutil /Get-Namespace /Namespace:<Namespace name> [/Server:<Server name>]
[/Show:Clients]
```

Windows Server 2008 R2

```
wdsutil /Get-Namespace /Namespace:<Namespace name> [/Server:<Server name>]
[/details:Clients]
```

Parameters

Parameter	Description
/Namespace:<Namespace name>	Specifies the name of the namespace. Note that this is not the friendly name, and it must be unique. - Deployment Server: The syntax for namespace name is /Namspace:WDS:<ImageGroup>/<ImageName>/<Index>. For example: **WDS:ImageGroup1/install.wim/1** - Transport Server: This value should match the name given to the namespace when it was created on the server.
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.

Parameter	Description
[/Show:Clients] or [/details:Clients]	Displays information about client computers that are connected to the specified namespace.

Examples

To view information about a namespace, type:

```
wdsutil /Get-Namespace /Namespace:Custom Auto 1
```

To view information about a namespace and the clients that are connected, type one of the following:

- Windows Server 2008: `wdsutil /Get-Namespace /Server:MyWDSServer /Namespace:Custom Auto 1 /Show:Clients`
- Windows Server 2008 R2: `wdsutil /Get-Namespace /Server:MyWDSServer /Namespace:Custom Auto 1 /details:Clients`

Related links

- Command-Line Syntax Key
- wdsutil get-allnamespaces command
- wdsutil new-namespace command
- wdsutil remove-namespace command
- wdsutil start-namespace command

wdsutil get-server

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Retrieves information from the specified Windows Deployment Services server.

Syntax

```
wdsutil [Options] /Get-Server [/Server:<Server name>] /Show:{Config | Images | All} [/detailed]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
/Show:{Config | Images | All}	Specifies the type of information to return. - **Config** returns configuration information. - **Images** returns information about image groups, boot images, and install images. - **All** returns configuration information and image information.
[/detailed]	You can use this option with **/Show:Images** or **/Show:All** to indicate that all image metadata from each image should be returned. If the **/detailed** option is not used, the default behavior is to return the image name, description, and file name.

Examples

To view information about the server, type:

```
wdsutil /Get-Server /Show:Config
```

To view detailed information about the server, type:

```
wdsutil /verbose /Get-Server /Server:MyWDSServer /Show:All /detailed
```

Related links

- Command-Line Syntax Key
- wdsutil disable-server command
- wdsutil enable-server command
- wdsutil initialize-server command
- wdsutil set-server command
- wdsutil start-server command
- wdsutil stop-server command
- wdsutil uninitialize-server command

wdsutil get-transportserver

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Displays information about a specified Transport Server.

Syntax

```
wdsutil [Options] /Get-TransportServer [/Server:<Server name>] /Show:
{Config}
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
/Show:{Config}	Returns configuration information about the specified Transport Server.

Examples

To view information about the server, type:

```
wdsutil /Get-TransportServer /Show:Config
```

To view configuration information, type:

```
wdsutil /Get-TransportServer /Server:MyWDSServer /Show:Config
```

Related links

- Command-Line Syntax Key
- wdsutil disable-transportserver command
- wdsutil enable-transportserver command
- wdsutil set-transportserver command
- wdsutil start-transportserver command
- wdsutil stop-transportserver command

wdsutil initialize-server

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configures a Windows Deployment Services server for initial use after the server role has been installed. After you run this command, you should use the wdsutil add-Image command command to add images to the server.

Syntax

```
wdsutil /Initialize-Server [/Server:<Server name>] /remInst:<Full path>
[/Authorize]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
/remInst:<Full path>	Specifies the full path and name of the remoteInstall folder. If the specified folder does not already exist, this option will create it when the command is run. You should always enter a local path, even in the case of a remote computer. For example: **D:\remoteInstall**.
[/Authorize]	Authorizes the server in Dynamic Host Control Protocol (DHCP). This option is necessary only if DHCP rogue detection is enabled, meaning that the Windows Deployment Services PXE server must be authorized in DHCP before client computers can be serviced. Note that DHCP rogue detection is disabled by default.

Examples

To initialize the server and set the remoteInstall shared folder to the F: drive, type.

```
wdsutil /Initialize-Server /remInst:F:\remoteInstall
```

To initialize the server and set the remoteInstall shared folder to the C: drive, type.

```
wdsutil /verbose /Progress /Initialize-Server /Server:MyWDSServer
/remInst:C:\remoteInstall
```

Related links

- Command-Line Syntax Key
- wdsutil disable-server command
- wdsutil enable-server command
- wdsutil get-server command
- wdsutil set-server command
- wdsutil start-server command
- wdsutil stop-server command
- wdsutil uninitialize-server command

wdsutil new

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates capture and discover images, multicast transmissions, and namespaces.

Subcommands

Subcommand	Description
wdsutil new-captureimage command	creates a new capture image from an existing boot image.
wdsutil new-discoverimage command	creates a new discover image from an existing boot image.
wdsutil new-multicasttransmission command	creates a new multicast transmission.
wdsutil new-namespace command	creates a new namespace.

new-CaptureImage

Article • 02/03/2023

Creates a new capture image from an existing boot image. Capture images are boot images that start the Windows Deployment Services capture utility instead of starting Setup. When you boot a reference computer (that has been prepared with Sysprep) into a capture image, a wizard creates an install image of the reference computer and saves it as a Windows Image (.wim) file. You can also add the image to media (such as a CD, DVD, or USB drive), and then boot a computer from that media. After you create the install image, you can add the image to the server for PXE boot deployment. For more information, see Creating Images (https://go.microsoft.com/fwlink/?LinkId=115311).

Syntax

```
wdsutil [Options] /New-CaptureImage [/Server:<Server name>]
     /Image:<Image name>
     /Architecture:{x86 | ia64 | x64}
     [/Filename:<File name>]
     /DestinationImage
        /FilePath:<File path and name>
        [/Name:<Name>]
        [/Description:<Description>]
        [/Overwrite:{Yes | No | Append}]
        [/UnattendFilePath:<File path>]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
/Image:<Image name>	Specifies the name of the source boot image.
/Architecture: {x86	ia64
[/Filename: <Filename>]	If the image cannot be uniquely identified by name, you must use this option to specify the file name.

Parameter	Description
/DestinationImage	Specifies the settings for the destination image. You specify the settings using the following options: - /FilePath: <File path and name> Sets the full file path for the new capture image. - [/Name: <Name>] - Sets the display name of the image. If no display name is specified, the display name of the source image will be used. - [/Description: <Description>] - Sets the description of the image. - [/Overwrite: {Yes

Examples

To create a capture image and name it WinPECapture.wim, type:

```
wdsutil /New-CaptureImage /Image:WinPE boot image /Architecture:x86
/DestinationImage /FilePath:C:\Temp\WinPECapture.wim
```

To create a capture image and apply the specified settings, type:

```
wdsutil /Verbose /Progress /New-CaptureImage /Server:MyWDSServer
/Image:WinPE boot image /Architecture:x64 /Filename:boot.wim
/DestinationImage /FilePath:\\Server\Share\WinPECapture.wim /Name:New WinPE
image /Description:WinPE image with capture utility /Overwrite:No
/UnattendFilePath:\\Server\Share\WDSCapture.inf
```

Related links

- Command-Line Syntax Key

new-DiscoverImage

Article • 02/03/2023

Creates a new discover image from an existing boot image. Discover images are boot images that force the Setup.exe program to start in Windows Deployment Services mode and then discover a Windows Deployment Services server. Typically these images are used to deploy images to computers that are not capable of booting to PXE. For more information, see Creating Images (https://go.microsoft.com/fwlink/?LinkId=115311).

Syntax

```
wdsutil [Options] /New-DiscoverImage [/Server:<Server name>]
     /Image:<Image name>
     /Architecture:{x86 | ia64 | x64}
     [/Filename:<File name>]
     /DestinationImage
         /FilePath:<File path and name>
         [/Name:<Name>]
         [/Description:<Description>]
         [/WDSServer:<Server name>]
         [/Overwrite:{Yes | No | Append}]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
/Image:<Image name>	Specifies the name of the source boot image.
/Architecture:{x86	ia64
[/Filename:<File name>]	If the image cannot be uniquely identified by name, you must use this option to specify the file name.

Parameter	Description
/DestinationImage	Specifies the settings for the destination image. You can specify the settings using the following options: - /FilePath:< File path and name> - Sets full file path for the new image. - [/Name:<Name>] - Sets the display name of the image. If no display name is specified, the display name of the source image will be used. - [/Description: <Description>] - Sets the description of the image. - [/WDSServer: <Server name>] - Specifies the name of the server that all clients who boot from the specified image should contact to download the install image. By default, all clients who boot this image will discover a valid Windows Deployment Services server. Using this option bypasses the discovery functionality and forces the booted client to contact the specified server. - [/Overwrite:{Yes

Examples

To create a discover image out of boot image, and name it WinPEDiscover.wim, type:

```
wdsutil /New-DiscoverImage /Image:WinPE boot image /Architecture:x86
/DestinationImage /FilePath:C:\Temp\WinPEDiscover.wim
```

To create a discover image out of boot image, and name it WinPEDiscover.wim with the specified settings, type:

```
wdsutil /Verbose /Progress /New-DiscoverImage /Server:MyWDSServer
/Image:WinPE boot image /Architecture:x64 /Filename:boot.wim
/DestinationImage /FilePath:\\Server\Share\WinPEDiscover.wim
/Name:New WinPE image /Description:WinPE image for WDS Client discovery
/Overwrite:No
```

Related links

- Command-Line Syntax Key

wdsutil new-multicasttransmission

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates a new multicast transmission for an image. This command is equivalent to creating a transmission by using the Windows Deployment Services mmc snap-in (right-click the **Multicast Transmissions** node, and then click **create Multicast Transmission**). You should use this command when you have both the Deployment Server role service and the Transport Server role service installed (which is the default installation). If you have only the Transport Server role service installed, use wdsutilnew-Namespace command.

Syntax

For install images transmissions:

```
wdsutil [Options] /New-MulticastTransmissiomedia:<Image name>
        [/Server:<Server name>]
        /FriendlyName:<Friendly name>
        [/Description:<Description>]
        /Transmissiontype: {AutoCast | ScheduledCast}
            [/time:<YYYY/MM/DD:hh:mm>]
            [/Clients:<Num of Clients>]
      imagetype:Install
       ImageGroup:<Image Group>]
        [/Filename:<File name>]
```

For boot image transmissions (only supported for Windows Server 2008 R2):

```
wdsutil [Options] /New-MulticastTransmissiomedia:<Image name>
        [/Server:<Server name>]
        /FriendlyName:<Friendly name>
        [/Description:<Description>]
        /Transmissiontype: {AutoCast | ScheduledCast}
            [/time:<YYYY/MM/DD:hh:mm>]
            [/Clients:<Num of Clients>]
      imagetype:Boot
        /Architecture:{x86 | ia64 | x64}
        [/Filename:<File name>]
```

Parameters

Parameter	Description
/image:<Image name>	Specifies the name of the image to be transmitted using multicasting.
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
/FriendlyName: <Friendly name>	Specifies the friendly name of the transmission.
[/Description: <Description>]	Specifies the description of the transmission.
/imagetype: {Boot|Install}	Specifies the type of image to be transmitted using multicasting. Note **Boot** is only supported for Windows Server 2008 R2.
/ImageGroup: <Image group name>]	Specifies the image group that contains the image. If no image group name is specified and only one image group exists on the server, that image group is used. If more than one image group exists on the server, you must use this option to specify the image group name.
[/Filename:<File name>]	Specifies the file name. If the source image cannot be uniquely identified by name, you must use this option to specify the file name.
/Transmissiontype: {AutoCast | ScheduledCast}	Specifies whether to start the transmission automatically (AutoCast) or based on the specified start criteria (ScheduledCast). • **Auto-Cast**. This transmission type indicates that as soon as an applicable client requests an install image, a multicast transmission of the selected image begins. As other clients request the same image, they are joined to the transmission that is already started. • **Scheduled-Cast**. This transmission type sets the start criteria for the transmission based on the number of clients that are requesting an image and/or a specific day and time. You can specify the following options: ◦ [/time: <time>] - Sets the time that the transmission should start by using the following format: YYYY/MM/DD:hh:mm. ◦ [/Clients: <Number of clients>] - Sets the minimum number of clients to wait for before the transmission starts.

Parameter	Description
/Architecture:{x86 | ia64 | x64}	Specifies the architecture of the boot image to transmit using multicasting. Because it is possible to have the same name for boot images of different architectures, you should specify the architecture to ensure the correct image is used.
[/Filename:<File name>]	Specifies the file name. If the source image cannot be uniquely identified by name, you must specify the file name.

Examples

To create an Auto-Cast transmission of a boot image in Windows Server 2008 R2, type:

```
wdsutil /New-MulticastTransmission /FriendlyName:WDS Boot Transmission
/Image:X64 Boot imagetype:Boot /Architecture:x64 /Transmissiontype:AutoCast
```

To create an Auto-Cast transmission of an install image, type:

```
wdsutil /New-MulticastTransmission /FriendlyName:WDS AutoCast Transmission
/Image:Vista with Officeimage imagetype:Install /Transmissiontype:AutoCast
```

To create a Scheduled-Cast transmission of an install image, type:

```
wdsutil /New-MulticastTransmission /FriendlyName:WDS SchedCast Transmission
/Server:MyWDSServer Image:Vista with Office imagetype:Install
/Transmissiontype:ScheduledCast /time:2006/11/20:17:00 /Clients:100
```

Related links

- Command-Line Syntax Key
- wdsutil get-allmulticasttransmissions command
- wdsutil get-multicasttransmission command
- wdsutil remove-multicasttransmission command
- wdsutil start-multicasttransmission command

wdsutil new-namespace

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Creates and configures a new namespace. You should use this option when you have only the Transport Server role service installed. If you have both the Deployment Server role service and the Transport Server role service installed (which is the default), use wdsutilnew-MulticastTransmission command. Note that you must register the content provider before you use this option.

Syntax

```
wdsutil [Options] /New-Namespace [/Server:<Server name>]
     /FriendlyName:<Friendly name>
     [/Description:<Description>]
     /Namespace:<Namespace name>
     /ContentProvider:<Name>
     [/ConfigString:<Configuration string>]
     /Namespacetype: {AutoCast | ScheduledCast}
         [/time:<YYYY/MM/DD:hh:mm>]
         [/Clients:<Number of clients>]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
/FriendlyName: <Friendly name>	Specifies the friendly name of the namespace.
[/Description: <Description>]	Sets the description of the namespace.

Parameter	Description
/Namespace:<Namespace name>	Specifies the name of the namespace. Note that this is not the friendly name, and it must be unique. - **Deployment Server role service**: The syntax for this option is /Namespace:WDS:<Image group>/<Image name>/<Index>. For example: **WDS:ImageGroup1/install.wim/1** - **Transport Server role service**: This value should match the name given when the namespace was created on the server.
/ContentProvider:<Name>]	Specifies the name of the content provider that will provide content for the namespace.
[/ConfigString:<Configuration string>]	Specifies the configuration string for the content provider.
/Namespacetype:{AutoCast | ScheduledCast}	Specifies the settings for the transmission. You specify the settings using the following options: - [/time: <time>] - Sets the time that the transmission should start by using the following format: YYYY/MM/DD:hh:mm. This option applies only to Scheduled-Cast transmissions. - [/Clients: <Number of clients>] - Sets the minimum number of clients to wait for before the transmission starts. This option applies only to Scheduled-Cast transmissions.

Examples

To create an Auto-Cast namespace, type:

```
wdsutil /New-Namespace /FriendlyName:Custom AutoCast Namespace
/Namespace:Custom Auto 1 /ContentProvider:MyContentProvider
/Namespacetype:AutoCast
```

To create a Scheduled-Cast namespace, type:

```
wdsutil /New-Namespace /Server:MyWDSServer /FriendlyName:Custom Scheduled
Namespace /Namespace:Custom Auto 1 /ContentProvider:MyContentProvider
/Namespacetype:ScheduledCast /time:2006/11/20:17:00 /Clients:20
```

Related links

- Command-Line Syntax Key
- wdsutil get-allnamespaces command
- wdsutil remove-namespace command
- wdsutil start-namespace command

wdsutil /progress

Article • 02/03/2023

Displays progress while a command is running. You can use **/progress** with any other wdsutil commands that you run. If you want to turn on verbose logging for this command, you must specify **/verbose** and **/progress** directly after **wdsutil**.

Syntax

```
wdsutil /progress <commands>
```

Examples

To initialize the server and display progress, type:

```
wdsutil /verbose /progress /Initialize-Server /Server:MyWDSServer
/RemInst:C:\RemoteInstall
```

Related links

- Command-Line Syntax Key

wdsutil reject-autoadddevices

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Rejects computers that are pending administrative approval. When the Auto-add policy is enabled, administrative approval is required before unknown computers (those that are not prestaged) can install an image. You can enable this policy using the **PXE Response** tab of the server s properties page.

Syntax

```
wdsutil [Options] /Reject-AutoaddDevices [/Server:<Server name>] /RequestId:
<Request ID or ALL>
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
/RequestId:<Request ID | ALL>	Specifies the request ID assigned to the pending computer. To reject all pending computers, specify **ALL**.

Examples

To reject a single computer, type:

```
wdsutil /Reject-AutoaddDevices /RequestId:12
```

To reject all computers, type:

```
wdsutil /verbose /Reject-AutoaddDevices /Server:MyWDSServer /RequestId:ALL
```

Related links

- Command-Line Syntax Key
- wdsutil approve-autoadddevices command
- wdsutil delete-autoadddevices command
- wdsutil get-autoadddevices command

wdsutil remove

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Subcommands

Subommand	Description
wdsutil remove-image command	removes a boot or install image from the server.
wdsutil remove-imagegroup command	removes an image group from the server.
wdsutil remove-multicasttransmission command	Disables multicast transmission of an image.
wdsutil remove-namespace command	removes a namespace from the server.
wdsutil remove-drivergrouppackage command	removes a driver package from a driver group on a server.
wdsutil remove-drivergrouppackages command	removes driver packages from a driver group on a server.
wdsutil remove-driverpackage command	removes a driver package from a server.
wdsutil remove-driverpackages command	removes driver packages from a server.
wdsutil remove-drivergroup command	removes a driver group from a server.
wdsutil remove-drivergroupfilter command	removes a filter rule from a driver group on a server.

remove-DriverGroup

Article • 02/03/2023

Removes a driver group from a server.

Syntax

```
wdsutil /Remove-DriverGroup /DriverGroup:<Group Name> [/Server:<Server
name>]
```

Parameters

Parameter	Description
/DriverGroup:<Group Name>	Specifies the name of the driver group to remove.
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.

Examples

To remove a driver group, type one of the following:

```
wdsutil /Remove-DriverGroup /DriverGroup:PrinterDrivers
```

```
wdsutil /Remove-DriverGroup /DriverGroup:PrinterDrivers /Server:MyWdsServer
```

Related links

- Command-Line Syntax Key

remove-DriverGroupFilter

Article • 02/03/2023

Removes a filter rule from a driver group on a server.

Syntax

```
wdsutil /Remove-DriverGroupFilter /DriverGroup:<Group Name> [/Server:<Server name>] /FilterType:<Filter Type>
```

Parameters

Parameter	Description
/DriverGroup:<Group Name>	Specifies the name of the driver group.
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.
[/FilterType:<FilterType>]	Specifies the type of the filter to remove from the group. <FilterType> can be one of the following: **BiosVendor** **BiosVersion** **ChassisType** **Manufacturer** **Uuid** **OsVersion** **OsEdition** **OsLanguage**

Examples

To remove a filter, type one of the following:

```
wdsutil /Remove-DriverGroupFilter /DriverGroup:PrinterDrivers /FilterType:Manufacturer
```

```
wdsutil /Remove-DriverGroupFilter /DriverGroup:PrinterDrivers
/FilterType:Manufacturer /FilterType:OSLanguage
```

Related links

- Command-Line Syntax Key

remove-DriverGroupPackage

Article • 02/03/2023

Removes a driver package from a driver group on a server.

Syntax

```
wdsutil /Remove-DriverGroupPackage /DriverGroup:<Group Name> [/Server:
<Server Name>] {/DriverPackage:<Name> | /PackageId:<ID>}
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.
[/DriverPackage:<Name>]	Specifies the name of the driver package to remove.
[/PackageId:<ID>]	Specifies the Windows Deployment Services ID of the driver package to remove. You must specify this option if the driver package cannot be uniquely identified by name.

Examples

```
wdsutil /Remove-DriverGroupPackage /DriverGroup:PrinterDrivers /PackageId:
{4D36E972-E325-11CE-BFC1-08002BE10318}
```

```
wdsutil /Remove-DriverGroupPackage /DriverGroup:PrinterDrivers
/DriverPackage:XYZ
```

Related links

- Command-Line Syntax Key

wdsutil remove-drivergrouppackages

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes driver packages from a driver group on a server.

Syntax

```
wdsutil /remove-DriverGroupPackages /DriverGroup:<Group Name> [/Server:
<Server Name>] /Filtertype:<Filter type> /Operator:{Equal | NotEqual |
GreaterOrEqual | LessOrEqual | Contains} /Value:<Value> [/Value:<Value> ...]
```

Parameters

Parameter	Description
/DriverGroup: <Group Name>	Specifies the name of the driver group.
[/Server: <Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.

Parameter	Description
/Filtertype: <Filter type>	Specifies the attribute of the driver package to search for. You can specify multiple attributes in a single command. You must also specify **/Operator** and **/Value** with this option. <Filter type> can be one of the following: **PackageId** **PackageName** **PackageEnabled** **Packagedateadded** **PackageInfFilename** **PackageClass** **PackageProvider** **PackageArchitecture** **PackageLocale** **PackageSigned** **PackagedatePublished** **Packageversion** **Driverdescription** **DriverManufacturer** **DriverHardwareId** **DrivercompatibleId** **DriverExcludeId** **DriverGroupId** **DriverGroupName**
/Operator: {Equal | NotEqual | GreaterOrEqual | LessOrEqual | Contains}	Specifies the relationship between the attribute and the values. You can only specify **Contains** with string attributes. You can only specify **GreaterOrEqual** and **LessOrEqual** with date and version attributes.

Parameter	Description
/Value:<Value>	Specifies the value to search for the specified <attribute>. You can specify multiple values for a single **/Filtertype**. The following list outlines the attributes that you can specify for each filter. For more information about these attributes, see Driver and Package attributes (https://go.microsoft.com/fwlink/?LinkId=166895). - PackageId - Specify a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318}. - PackageName Specify any string value. - PackageEnabled - Specify **Yes** or **No**. - Packagedateadded - Specify the date in the following format: YYYY/MM/DD - PackageInfFilename Specify any string value. - PackageClass - Specify a valid class name or class GUID. For example: **DiskDrive**, **Net**, or {4d36e972-e325-11ce-bfc1-08002be10318}. - PackageProvider Specify any string value. - PackageArchitecture - Specify **x86**, **x64**, or **ia64**. - PckageLocale - Specify a valid language identifier. For example: **en-US** or **es-ES**. - PackageSigned - Specify **Yes** or **No**. - PackagedatePublished - Specify the date in the following format: YYYY/MM/DD - Packageversion - Specify the version in the following format: a.b.x.y. For example: 6.1.0.0 - Driverdescription Specify any string value. - DriverManufacturer Specify any string value. - DriverHardwareId - Specify any string value. - DrivercompatibleId - Specify any string value. - DriverExcludeId - Specify any string value. - DriverGroupId - Specify a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318}. - DriverGroupName Specify any string value.

Examples

To remove driver packages from a driver group, type one of the following:

```
wdsutil /verbose /remove-DriverGroupPackages /DriverGroup:printerdrivers
/Filtertype:DriverManufacturer /Operator:NotEqual /Value:Name1 /Value:Name2
```

```
wdsutil /verbose /remove-DriverGroupPackages /DriverGroup:DisplayDrivers
/Filtertype:PackageArchitecture /Operator:Equal /Value:x86
```

```
/Filtertype:Packagedateadded /Operator:LessOrEqual /Value:2008/01/01
```

Related links

- Command-Line Syntax Key
- wdsutil remove-drivergrouppackage command

wdsutil remove-driverpackage

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes a driver package from a server.

Syntax

```
wdsutil /remove-DriverPackage [/Server:<Server name>] {/DriverPackage:
<Package Name> | /PackageId:<ID>}
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.
[/DriverPackage:<Name>]	Specifies the name of the driver package to remove.
[/PackageId:<ID>]	Specifies the Windows Deployment Services ID of the driver package to remove. You must specify the ID if the driver package cannot be uniquely identified by name.

Examples

To view information about the images, type one of the following:

```
wdsutil /remove-DriverPackage /PackageId:{4D36E972-E325-11CE-Bfc1-
08002BE10318}
```

```
```

```
wdsutil /remove-DriverPackage /Server:MyWdsServer
/DriverPackage:MyDriverPackage
```

Related links

- Command-Line Syntax Key
- wdsutil remove-driverpackages command

wdsutil remove-driverpackages

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes driver packages from the server.

Syntax

```
wdsutil /remove-DriverPackages [/Server:<Server name>] /Filtertype:<Filter type> /Operator:{Equal | NotEqual | GreaterOrEqual | LessOrEqual | Contains} /Value:<Value> [/Value:<Value> ...]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.

Parameter	Description
/Filtertype: <Filter type>	Specifies the attribute of the driver package to search for. You can specify multiple attributes in a single command. You must also specify **/Operator** and **/Value** with this option. <Filter type> can be one of the following: • **PackageId** • **PackageName** • **PackageEnabled** • **Packagedateadded** • **PackageInfFilename** • **PackageClass** • **PackageProvider** • **PackageArchitecture** • **PackageLocale** • **PackageSigned** • **PackagedatePublished** • **Packageversion** • **Driverdescription** • **DriverManufacturer** • **DriverHardwareId** • **DrivercompatibleId** • **DriverExcludeId** • **DriverGroupId** • **DriverGroupName**
/Operator: {Equal | NotEqual | GreaterOrEqual | LessOrEqual | Contains}	Specifies the relationship between the attribute and the values. You can only specify **Contains** with string attributes. You can only specify **GreaterOrEqual** and **LessOrEqual** with date and version attributes.

Parameter	Description
/Value:<Value>	Specifies the value to search for the specified <attribute>. You can specify multiple values for a single **/Filtertype**. The following list outlines the attributes that you can specify for each filter. For more information about these attributes, see Driver and Package attributes (https://go.microsoft.com/fwlink/?LinkId=166895). • PackageId - Specify a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318}. • PackageName - Specify any string value. • PackageEnabled - Specify **Yes** or **No**. • Packagedateadded - Specify the date in the following format: YYYY/MM/DD. • PackageInfFilename - Specify any string value. • PackageClass - Specify a valid class name or class GUID. For example: **DiskDrive**, **Net**, or {4d36e972-e325-11ce-bfc1-08002be10318}. • PackageProvider - Specify any string value. • PackageArchitecture - Specify **x86**, **x64**, or **ia64**. • PckageLocale - Specify a valid language identifier. For example: **en-US** or **es-ES**. • PackageSigned - Specify **Yes** or **No**. • PackagedatePublished - Specify the date in the following format: YYYY/MM/DD. • Packageversion - Specify the version in the following format: a.b.x.y. For example: 6.1.0.0. • Driverdescription - Specify any string value. • DriverManufacturer - Specify any string value. • DriverHardwareId - Specify any string value. • DrivercompatibleId - Specify any string value. • DriverExcludeId - Specify any string value. • DriverGroupId - Specify a valid GUID. For example: {4d36e972-e325-11ce-bfc1-08002be10318}. • DriverGroupName - Specify any string value.

Examples

To remove packages, type one of the following:

```
wdsutil /verbose /remove-DriverPackages /Server:MyWdsServer
/Filtertype:PackageProvider /Operator:Equal /Value:Name1 /Value:Name2
```

```
wdsutil /remove-DriverPackages /Filtertype:PackageArchitecture
/Operator:Equal
/Value:x86 /Value:x64 /Filtertype:PackageEnabled /Operator:Equal /Value:No
```

```
wdsutil /verbose /remove-DriverPackages /Server:MyWdsServer
/Filtertype:Packagedateadded /Operator:LessOrEqual /Value:2008/01/01
```

Related links

- Command-Line Syntax Key
- wdsutil remove-driverpackage command

wdsutil remove-image

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Deletes an image from a server.

Syntax

for boot images:

```
wdsutil [Options] /remove-Image:<Image name> [/Server:<Server name>
type:Boot /Architecture:{x86 | ia64 | x64} [/Filename:<Filename>]
```

for install images:

```
wdsutil [Options] /remove-image:<Image name> [/Server:<Server name>
type:Install ImageGroup:<Image group name>] [/Filename:<Filename>]
```

Parameters

Parameter	Description
/remove-image:<Image name>	Specifies the name of the image.
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
mediatype:{Boot | Install}	Specifies the type of image.
/Architecture:{x86 | ia64 | x64}	Specifies the architecture of the image. Because it is possible to have the same image name for different boot images in different architectures, specifying the architecture value ensures that the correct image will be removed.

Parameter	Description
\ImageGroup:<Image group name>]	Specifies the image group that contains the image. If no image group name is specified and only one image group exists on the server, that image group will be used. If more than one image group exists, you must use this option to specify the image group.
[/Filename:<File name>]	if the image cannot be uniquely identified by name, you must use this option to specify the file name.

Examples

To remove a boot image, type:

```
wdsutil /remove-Imagmedia:WinPE Boot Imagemediatype:Boot /Architecture:x86
```

```
wdsutil /verbose /remove-Image:WinPE Boot Image /Server:MyWDSServer
type:Boot /Architecture:x64 /Filename:boot.wim
```

To remove an install image, type:

```
wdsutil /remove-Image:Windows Vista with Officemediatype:Install
```

```
wdsutil /verbose /remove-Image:Windows Vista with Office
/Server:MyWDSServemediatype:Instal ImageGroup:ImageGroup1
/Filename:install.wim
```

Related links

- Command-Line Syntax Key
- wdsutil add-image command
- wdsutil copy-image command
- wdsutil export-image command
- wdsutil get-image command

- wdsutil replace-image command
- wdsutil set-image command

wdsutil remove-imagegroup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes an image group from a server.

Syntax

```
wdsutil [Options] /remove-ImageGroup Group:<Image group name> [/Server:
<Server name>]
```

Parameters

Parameter	Description
imagegroup: <Image group name>	Specifies the name of the image group to be removed
[/Server: <Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Examples

To remove the image group, type one of the following:

```
wdsutil /remove-ImageGroumediaGroup:ImageGroup1
wdsutil /verbose /remove-ImageGroumediaGroup:My Image Group
/Server:MyWDSServer
```

Related links

- Command-Line Syntax Key

- wdsutil add-imagegroup command
- wdsutil get-allimagegroups command
- wdsutil get-imagegroup command
- wdsutil set-imagegroup command

wdsutil remove-multicasttransmission

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Disables multicast transmitting for an image. Unless you specify **/force**, existing clients will complete the image transfer but new clients will not be allowed to join.

Syntax

Windows Server 2008

```
wdsutil /remove-MulticastTransmission:<Image name> [/Server:<Server name>
mediatype:Install Group:<Image Group>] [/Filename:<File name>] [/force]
```

Windows Server 2008 R2 for boot images:

```
wdsutil [Options] /remove-MulticastTransmissiomedia:<Image name>
\x20    [/Server:<Server name>]
\x20  mediatype:Boot
\x20    /Architecture:{x86 | ia64 | x64}
\x20    [/Filename:<File name>]
```

for install images:

```
wdsutil [Options] /remove-MulticastTransmissiomedia:<Image name>
        [/Server:<Server name>]
      mediatype:Install
       mediaGroup:<Image Group
        [/Filename:<File name>]
```

Parameters

Parameter	Description

Parameter	Description
media: <Image name>	Specifies the name of the image.
[/Server: <Server name>]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
mediatype: {Install|Boot}	Specifies the image type. Note that this option must be set to **Install** for Windows Server 2008.
/Architecture: {x86 | ia64 | x64}	Specifies the architecture of the boot image that is associated with the transmission to start. Because it is possible to have the same image name for boot images in different architectures, you should specify the architecture to ensure that the correct transmission is used.
\mediaGroup: <Image group name>]	Specifies the image group that contains the image. If no image group name is specified and only one image group exists on the server, that image group is used. If more than one image group exists on the server, you must use this option to specify the image group name.
[/Filename: <File name>]	Specifies the file name. If the source image cannot be uniquely identified by name, you must use this option to specify the file name.
[/force]	removes the transmission and terminates all clients. Unless you specify a value for the **/force** option, existing clients can complete the image transfer but new clients are not able to join.

Examples

To stop a namespace (current clients will complete the transmission, but new clients will not be able to join), type:

```
wdsutil /remove-MulticastTransmission:Vista with Office
/Imagetype:Install
```

```
wdsutil /remove-MulticastTransmission:x64 Boot Image
/Imagetype:Boot /Architecture:x64
```

To force termination of all clients, type:

```
wdsutil /remove-MulticastTransmission /Server:MyWDSServer
/Image:Vista with Officemediatype:InstalmediaGroup:ImageGroup1
/Filename:install.wim /force
```

Related links

- Command-Line Syntax Key
- wdsutil get-allmulticasttransmissions command
- wdsutil get-multicasttransmission command
- wdsutil new-multicasttransmission command
- wdsutil start-multicasttransmission command

wdsutil remove-namespace

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Removes a custom namespace.

Syntax

```
wdsutil /remove-Namespace /Namespace:<Namespace name> [/Server:<Server name>] [/force]
```

Parameters

Parameter	Description
/Namespace:<Namespace name>	Specifies the name of the namespace. This is not the friendly name, and it must be unique. - **Deployment Server role service**: The syntax for namespace name is /Namespace:WDS:<ImageGroup>/<ImageName>/<Index>. For example: **WDS:ImageGroup1/install.wim/1** - **Transport Server role service**: This value must match the name given to the namespace when it was created on the server.
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server is used.
[/force]	removes the namespace immediately and terminates all clients. Note that unless you specify **/force**, existing clients can complete the transfer, but new clients are not able to join.

Examples

To stop a namespace (current clients can complete the transfer but new clients are not able to join), type:

```
wdsutil /remove-Namespace /Namespace:Custom Auto 1
```

To force termination of all clients, type:

```
wdsutil /remove-Namespace /Server:MyWDSServer /Namespace:Custom Auto 1
/force
```

Related links

- Command-Line Syntax Key
- wdsutil get-allnamespaces command
- wdsutil new-namespace command
- wdsutil start-namespace command

wdsutil replace-image

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Replaces an existing image with a new version of that image.

Syntax

for boot images:

```
wdsutil [Options] /replace-Imagmedia:<Image name> [/Server:<Server name>]
   mediatype:Boot
     /Architecture:{x86 | ia64 | x64}
     [/Filename:<File name>]
     /replacementImage
       mediaFile:<wim file path>
         [/Name:<Image name>]
         [/Description:<Image description>]
```

for install images:

```
wdsutil [Options] /replace-Imagmedia:<Image name> [/Server:<Server name>]
   mediatype:Install
    mediaGroup:<Image group name>]
     [/Filename:<File name>]
     /replacementImage
       mediaFile:<wim file path>
         [/SourceImage:<Source image name>]
         [/Name:<Image name>]
         [/Description:<Image description>]
```

Parameters

Parameter	Description
media:<Image name>	Specifies the name of the image to be replaced.

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
mediatype:{Boot | Install}	Specifies the type of image to be replaced.
/Architecture:{x86 | ia64 | x64}	Specifies the architecture of the image to be replaced. Because it is possible to have the same image name for different boot images in different architectures, specifying the architecture ensures that the correct image is replaced.
[/Filename:<File name>]	if the image cannot be uniquely identified by name, you must use this option to specify the file name.
/replacementImage	Specifies the settings for the replacement image. You set these settings using the following options: - mediaFile: <file path> - Specifies the name and location (full path) of the new .wim file. - [/SourceImage: <image name>] - Specifies the image to be used if the .wim file contains multiple images. This option applies only to install images. - [/Name:<Image name>] Sets the display name of the image. - [/Description:<Image description>] - Sets the description of the image.

Examples

To replace a boot image, type one of the following:

```
wdsutil /replace-Imagmedia:WinPE Boot Imagemediatype:Boot /Architecture:x86
/replacementImagmediaFile:C:\MyFolder\Boot.wim
wdsutil /verbose /Progress /replace-Imagmedia:WinPE Boot Image
/Server:MyWDSServemediatype:Boot /Architecture:x64 /Filename:boot.wim
/replacementImagmediaFile:\\MyServer\Share\Boot.wim /Name:My WinPE Image
/Description:WinPE Image with drivers
```

To replace an install image, type one of the following:

```
wdsutil /replace-Imagmedia:Windows Vista Homemediatype:Install
/replacementImagmediaFile:C:\MyFolder\Install.wim
wdsutil /verbose /Progress /replace-Imagmedia:Windows Vista Pro
/Server:MyWDSServemediatype:InstalmediaGroup:ImageGroup1
```

```
/Filename:Install.wim /replacementImagmediaFile:\\MyServer\Share
\Install.wim /SourceImage:Windows Vista Ultimate /Name:Windows Vista Desktop
/Description:Windows Vista Ultimate with standard business applications.
```

Related links

- Command-Line Syntax Key
- wdsutil add-image command
- wdsutil copy-image command
- wdsutil export-image command
- wdsutil get-image command
- wdsutil replace-image command
- wdsutil set-image command

Using the set command

Article • 07/29/2021

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets properties and attributes for Windows Deployment Services servers, prestaged computers, images, image groups, and Transport Servers.

Subcommands

Subcommand	Description
Subcommand: set-Device	changes the attributes of a prestaged computer. A prestaged computer is a computer that has been linked to a computer account object in active directory Domain Servers (AD DS). Prestaged clients are also called known computers.
Subcommand: set-Image	changes the attributes of an existing image.
Subcommand: set-ImageGroup	changes the attributes of an existing image group.
Subcommand: set-Server	Configures the settings for a Windows Deployment Services server.
Subcommand: set-TransportServer	Configures the settings for a Transport Server.
Subcommand: set-DriverPackage	renames and/or enable/disable a driver package on a server.
Subcommand: set-DriverGroup	Sets the properties of an existing driver group on a server.
Subcommand: set-DriverGroupFilter	adds or removes an existing driver group filter from a driver group.

wdsutil set-device

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the attributes of a prestaged computer. A prestaged computer is a computer that has been linked to a computer account object in active directory Domain Servers (AD DS). Prestaged clients are also called known computers. You can configure properties on the computer account to control the installation for the client. For example, you can configure the network boot program and the unattend file that the client should receive, as well as the server from which the client should download the network boot program.

Syntax

```
wdsutil [Options] /Set-Device /Device:<Device name> [/ID:<UUID | MAC
address>] [/ReferralServer:<Server name>] [/BootProgram:<Relative path>]
[/WdsClientUnattend:<Relative path>] [/User:<Domain\User | User@Domain>]
[/JoinRights:{JoinOnly | Full}] [/JoinDomain:{Yes | No}] [/BootImagepath:
<Relative path>] [/Domain:<Domain>] [/resetAccount]
```

Parameters

Parameter	Description
/Device:<computer name>	Specifies the name of the computer (SAM-Account-Name).
[/ID:<UUID | MAC address>]	Specifies either the GUID/UUID or the MAC address of the computer. This value must be in one of the following three formats: - Binary string: **/ID:ACEFA3E81F20694E953EB2DAA1E8B1B6** - GUID/UUID string: /ID:**E8A3EFAC-201F-4E69-953E-B2DAA1E8B1B6** - MAC address: **00B056882FDC** (no dashes) or **00-B0-56-88-2F-DC** (with dashes)
[/ReferralServer:<Server name>]	Specifies the name of the server to be contacted to download the network boot program and boot image using Trivial File Transfer Protocol (tftp).

Parameter	Description
[/BootProgram: <Relative path>]	Specifies the relative path from the remoteInstall folder to the network boot program that the specified computer will receive. For example: **boot\x86\pxeboot.com**
[/WdsClientUnattend: <Relative path>]	Specifies the relative path from the remoteInstall folder to the unattend file that automates the installation screens for the Windows Deployment Services client.
[/User:<Domain\User | User@Domain>]	Sets permissions on the computer account object to give the specified user the necessary rights to join the computer to the domain.
[/JoinRights: {JoinOnly | Full}]	Specifies the type of rights to be assigned to the user. - **JoinOnly** requires the administrator to reset the computer account before the user can join the computer to the domain. - **Full** gives full access to the user, including the right to join the computer to the domain.
[/JoinDomain:{Yes | No}]	Specifies whether or not the computer should be joined to the domain as this computer account during a Windows Deployment Services installation. The default setting is **Yes**.
[/BootImagepath: <Relative path>]	Specifies the relative path from the remoteInstall folder to the boot image that the computer will use.
[/Domain: <Domain>]	Specifies the domain to be searched for the prestaged computer. The default value is the local domain.
[/resetAccount]	resets the permissions on the specified computer so that anyone with the appropriate permissions can join the domain by using this account.

Examples

To set the network boot program and referral server for a computer, type:

```
wdsutil /Set-Device /Device:computer1 /ReferralServer:MyWDSServer
/BootProgram:boot\x86\pxeboot.n12
```

To set various settings for a computer, type:

```
wdsutil /verbose /Set-Device /Device:computer2 /ID:00-B0-56-88-2F-DC
/WdsClientUnattend:WDSClientUnattend\unattend.xml
```

```
/User:Domain\user /JoinRights:JoinOnly /JoinDomain:No
/BootImagepath:boot\x86\images\boot.wim /Domain:NorthAmerica /resetAccount
```

Related links

- Command-Line Syntax Key
- wdsutil add-device command
- wdsutil get-alldevices command
- wdsutil get-device command

Subcommand: set-DriverGroup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets the properties of an existing driver group on a server.

Syntax

```
wdsutil /Set-DriverGroup /DriverGroup:<Group Name> [/Server:<Server Name>] [/Name:<New Group Name>] [/Enabled:{Yes | No}] [/Applicability:{Matched | All}]
```

Parameters

Parameter	Description
/DriverGroup:<Group Name>	Specifies the name of the driver group.
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.
[/Name:<New Group Name>]	Specifies the new name for the driver group.
[/Enabled:{Yes | No}	Enables or disables the driver group.
[/Applicability:{Matched | All}]	Specifies which packages to install if the filter criteria is met. **Matched** means install only the driver packages that match a client s hardware. **All** means install all packages to clients regardless of their hardware.

Examples

To set the properties for a driver group, type one of the following:

```
wdsutil /Set-DriverGroup /DriverGroup:printerdrivers /Enabled:Yes
```

```
wdsutil /Set-DriverGroup /DriverGroup:printerdrivers
/Name:colorprinterdrivers /Applicability:All
```

Related links

- Command-Line Syntax Key Subcommand: set-DriverGroupFilter

Subcommand: set-DriverGroupFilter

Article • 02/03/2023

Adds or removes an existing driver group filter from a driver group.

Syntax

```
wdsutil /Set-DriverGroupFilter /DriverGroup:<Group Name> [/Server:<Server
name>] /FilterType:<Filter Type> [/Policy:{Include | Exclude}] [/AddValue:
<Value> [/AddValue:<Value> ...]] [/RemoveValue:<Value> [/RemoveValue:<Value>
...]]
```

Parameters

Parameter	Description
/DriverGroup: <Group Name>	Specifies the name of the driver group.
[/Server: <Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.
/FilterType: <FilterType>	Specifies the type of driver group filter to add or remove. You can specify multiple filters in a single command. For each **/FilterType**, you can add or remove multiple values using **/RemoveValue** and **/AddValue**. <FilterType> can be one of the following: **BiosVendor** **BiosVersion** **ChassisType** **Manufacturer** **Uuid** **OsVersion** **OsEdition** **OsLanguage**
[/Policy: {Include	Exclude}]

Parameter	Description
[/AddValue:<Value>]	Specifies the new client value to add to the filter. You can specify multiple values for a single filter type. See the following list for valid attribute values for **ChassisType**. For information about obtaining the values for all other filter types, see Driver Group Filters (https://go.microsoft.com/fwlink/?LinkID=155158). **Other** **UnknownChassis** **Desktop** **LowProfileDesktop** **PizzaBox** **MiniTower** **Tower** **Portable** **Laptop** **Notebook** **Handheld** **DockingStation** **AllInOne** **SubNotebook** **SpaceSaving** **LunchBox** **MainSystemChassis** **ExpansionChassis** **SubChassis** **BusExpansionChassis** **PeripheralChassis** **StorageChassis** **RackMountChassis** **SealedCaseComputer** **MultiSystemChassis** **CompactPci** **AdvancedTca**
[/RemoveValue:<Value>]	Specifies the existing client value to remove from the filter as specified with **/AddValue**.

Examples

To remove a filter, type one of the following:

```
wdsutil /Set-DriverGroupFilter /DriverGroup:PrinterDrivers
/FilterType:Manufacturer /Policy:Include /AddValue:Name1 /RemoveValue:Name2
```

```
wdsutil /Set-DriverGroupFilter /DriverGroup:PrinterDrivers
/FilterType:Manufacturer /Policy:Include /RemoveValue:Name1
/FilterType:ChassisType /Policy:Exclude /AddValue:Tower /AddValue:MiniTower
```

Related links

- Command-Line Syntax Key

Subcommand: set-DriverPackage

Article • 02/03/2023

Renames and/or enables or disables a driver package on a server.

Syntax

```
wdsutil /Set-DriverPackage [/Server:<Server name>] {/DriverPackage:<Name> |
/PackageId:<ID>} [/Name:<New Name>] [/Enabled:{Yes | No}
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be the NetBIOS name or the FQDN. If a server name is not specified, the local server is used.
[/DriverPackage:<Name>]	Specifies the current name of the driver package to modify.
[/PackageId:<ID>]	Specifies the Windows Deployment Services ID of the driver package. You must specify this option if the driver package cannot be uniquely identified by name. To find this ID for a package, click the driver group that the package is in (or the **All Packages** node), right-click the package, and then click **Properties**. The Package ID is listed on the **General** tab. For example: {DD098D20-1850-4FC8-8E35-EA24A1BEFF5E}.
[/Name:<New Name>]	Specifies the new name for the driver package.
[/Enabled:{Yes	No}	

Examples

To change settings about a package, type one of the following:

```
wdsutil /Set-DriverPackage /PackageId:{4D36E972-E325-11CE-BFC1-08002BE10318}
/Name:MyDriverPackage
```

```
wdsutil /Set-DriverPackage /DriverPackage:MyDriverPackage /Name:NewName
/Enabled:Yes
```

Related links

- Command-Line Syntax Key

wdsutil set-image

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the attributes of an image.

Syntax

for boot images:

```
wdsutil /Set-Imagmedia:<Image name> [/Server:<Server name>mediatype:Boot
/Architecture:{x86 | ia64 | x64} [/Filename:<File name>] [/Name:<Name>]
[/Description:<Description>] [/Enabled:{Yes | No}]
```

for install images:

```
wdsutil /Set-Imagmedia:<Image name> [/Server:<Server name>]
   mediatype:InstallmediaGroup:<Image group name>]
     [/Filename:<File name>]
     [/Name:<Name>]
     [/Description:<Description>]
     [/UserFilter:<SDDL>]
     [/Enabled:{Yes | No}]
     [/UnattendFile:<Unattend file path>]
         [/OverwriteUnattend:{Yes | No}]
```

Parameters

Parameter	Description
media:<Image name>	Specifies the name of the image.
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Parameter	Description
mediatype:{Boot | Install}	Specifies the type of image.
/Architecture:{x86 | ia64 | x64}	Specifies the architecture of the image. Because you can have the same image name for different boot images in different architectures, specifying the architecture ensures that the correct image is modified.
[/Filename:<File name>]	if the image cannot be uniquely identified by name, you must use this option to specify the file name.
[/Name]	Specifies the name of the image.
[/Description: <Description>]	Sets the description of the image.
[/Enabled:{Yes | No}]	Enables or disables the image.
\mediaGroup: <Image group name>]	Specifies the image group that contains the image. If no image group name is specified and only one image group exists on the server, that image group will be used. If more than one image group exists on the server, you must use this option to specify the image group.
[/UserFilter:<SDDL>]	Sets the user filter on the image. The filter string must be in Security Descriptor Definition Language (SDDL) format. Note that, unlike the **/Security** option for image groups, this option only restricts who can see the image definition, and not the actual image file resources. To restrict access to the file resources, and therefore access to all images within an image group, you will need to set security for the image group itself.
[/UnattendFile: <Unattend file path>]	Sets the full path to the unattend file to be associated with the image. For example: **D:\Files\Unattend\Img1Unattend.xml**
[/OverwriteUnattend: {Yes | No}]	You can specify **/Overwrite** to overwrite the unattend file if there is already an unattend file associated with the image. Note that the default setting is **No**.

Examples

To set values for a boot image, type one of the following:

```
wdsutil /Set-Imagmedia:WinPE boot imagemediatype:Boot /Architecture:x86
/Description:New description
wdsutil /verbose /Set-Imagmedia:WinPE boot image
/Server:MyWDSServemediatype:Boot /Architecture:x86 /Filename:boot.wim
/Name:New Name /Description:New Description /Enabled:Yes
```

To set values for an install image, type one of the following:

```
wdsutil /Set-Imagmedia:Windows Vista with Officemediatype:Install
/Description:New description
wdsutil /verbose /Set-Imagmedia:Windows Vista with Office
/Server:MyWDSServemediatype:InstalmediaGroup:ImageGroup1
/Filename:install.wim /Name:New name /Description:New description
/UserFilter:O:BAG:DUD:AI(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;0x1200a9;;;AU)
/Enabled:Yes /UnattendFile:\\server\share\unattend.xml
/OverwriteUnattend:Yes
```

Related links

- Command-Line Syntax Key
- wdsutil add-image command
- wdsutil copy-image command
- wdsutil Export-image command
- wdsutil get-image command
- wdsutil remove-image command
- wdsutil replace-image command

wdsutil set-imagegroup

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Changes the attributes of an image group.

Syntax

```
wdsutil [Options] /set-imagegroup:<Image group name> [/Server:<Server name>]
[/Name:<New image group name>] [/Security:<SDDL>]
```

Parameters

Parameter	Description
/set-imagegroup:<Image group name>	Specifies the name of the image group.
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If not specified, the local server will be used.
[/Name:<New image group name>]	Specifies the new name of the image group.
[/Security:<SDDL>]	Specifies the new Security Descriptor of the image group, in security descriptor definition language (SDDL) format.

Examples

To set the name for an image group, type:

```
wdsutil /Set-ImageGroup:ImageGroup1 /Name:New Image Group Name
```

To specify various settings for an image group, type:

```
wdsutil /verbose /Set-ImageGroupGroup:ImageGroup1 /Server:MyWDSServer
/Name:New Image Group Name
/Security:O:BAG:S-1-5-21-2176941838-3499754553-4071289181-513
D:AI(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)
(A;ID;0x1200a9;;;AU)(A;OICIIOID;GXGR;;;AU)
```

Related links

- Command-Line Syntax Key
- wdsutil add-imagegroup command
- wdsutil get-allimagegroups command
- wdsutil get-imagegroup command
- wdsutil remove-imagegroup command

wdsutil set-server

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Configures the settings for a Windows Deployment Services server.

Syntax

```
wdsutil [Options] /Set-Server [/Server:<Server name>]
    [/Authorize:{Yes | No}]
    [/RogueDetection:{Yes | No}]
    [/AnswerClients:{All | Known | None}]
    [/Responsedelay:<time in seconds>]
    [/AllowN12forNewClients:{Yes | No}]
    [/ArchitectureDiscovery:{Yes | No}]
    [/resetBootProgram:{Yes | No}]
    [/DefaultX86X64Imagetype:{x86 | x64 | Both}]
    [/UseDhcpPorts:{Yes | No}]
    [/DhcpOption60:{Yes | No}]
    [/RpcPort:<Port number>]
    [/PxepromptPolicy
        [/Known:{OptIn | Noprompt | OptOut}]
        [/New:{OptIn | Noprompt | OptOut}]
    [/BootProgram:<Relative path>]
         /Architecture:{x86 | ia64 | x64}
    [/N12BootProgram:<Relative path>]
         /Architecture:{x86 | ia64 | x64}
    [/BootImage:<Relative path>]
         /Architecture:{x86 | ia64 | x64}
    [/PreferredDC:<DC Name>]
    [/PreferredGC:<GC Name>]
    [/PrestageUsingMAC:{Yes | No}]
    [/NewMachineNamingPolicy:<Policy>]
    [/NewMachineOU]
         [/type:{Serverdomain | Userdomain | UserOU | Custom}]
         [/OU:<Domain name of OU>]
    [/DomainSearchOrder:{GCOnly | DCFirst}]
    [/NewMachineDomainJoin:{Yes | No}]
    [/OSCMenuName:<Name>]
    [/WdsClientLogging]
         [/Enabled:{Yes | No}]
         [/LoggingLevel:{None | Errors | Warnings | Info}]
    [/WdsUnattend]
         [/Policy:{Enabled | Disabled}]
```

```
          [/CommandlinePrecedence:{Yes | No}]
          [/File:<path>]
              /Architecture:{x86 | ia64 | x64}
     [/AutoaddPolicy]
          [/Policy:{AdminApproval | Disabled}]
          [/PollInterval:{time in seconds}]
          [/MaxRetry:{Retries}]
          [/Message:<Message>]
          [/RetentionPeriod]
              [/Approved:<time in days>]
              [/Others:<time in days>]
     [/AutoaddSettings]
          /Architecture:{x86 | ia64 | x64}
          [/BootProgram:<Relative path>]
          [/ReferralServer:<Server name>
          [/WdsClientUnattend:<Relative path>]
          [/BootImage:<Relative path>]
          [/User:<Owner>]
          [/JoinRights:{JoinOnly | Full}]
          [/JoinDomain:{Yes | No}]
     [/BindPolicy]
          [/Policy:{Include | Exclude}]
          [/add]
               /address:<IP or MAC address>
               /addresstype:{IP | MAC}
          [/remove]
               /address:<IP or MAC address>
               /addresstype:{IP | MAC}
     [/RefreshPeriod:<time in seconds>]
     [/BannedGuidPolicy]
          [/add]
               /Guid:<GUID>
          [/remove]
              /Guid:<GUID>
     [/BcdRefreshPolicy]
          [/Enabled:{Yes | No}]
          [/RefreshPeriod:<time in minutes>]
     [/Transport]
          [/ObtainIpv4From:{Dhcp | Range}]
              [/start:<start IP address>]
              [/End:<End IP address>]
          [/ObtainIpv6From:Range]
              [/start:<start IP address>]
              [/End:<End IP address>]
          [/startPort:<start Port>
              [/EndPort:<start Port>
         [/Profile:{10Mbps | 100Mbps | 1Gbps | Custom}]
         [/MulticastSessionPolicy]
              [/Policy:{None | AutoDisconnect | Multistream}]
                  [/Threshold:<Speed in KBps>]
                  [/StreamCount:{2 | 3}]
                  [/Fallback:{Yes | No}]
         [/forceNative]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
[/Authorize:{Yes | No}]	Specifies whether to authorize this server in Dynamic Host Control Protocol (DHCP).
[/RogueDetection:{Yes | No}]	Enables or disables DHCP rogue detection.
[/AnswerClients:{All | Known | None}]	Specifies which clients this server will answer. If you set this value to **Known**, a computer must be prestaged in active directory Domain Services (AD DS) before it will be answered by the Windows Deployment Services server.
[/Responsedelay:<time in seconds>]	The amount of time that the server will wait before answering a booting client. This setting does not apply to prestaged computers.
[/AllowN12forNewClients:{Yes | No}]	for Windows Server 2008, specifies that unknown clients will not have to press the F12 key to initiate a network boot. Known clients will receive the boot program specified for the computer or, if not specified, the boot program specified for the architecture. for Windows Server 2008 R2, this option has been replaced with the following command: wdsutil /Set-Server /PxepromptPolicy /New:Noprompt
[/ArchitectureDiscovery:{Yes | No}]	Enables or disables architecture discovery. This facilitates the discovery of x64-based clients that do not broadcast their architecture correctly.
[/resetBootProgram:{Yes | No}]	Determines whether the boot path will be erased for a client that has just booted without requiring an F12 key press.
[/DefaultX86X64Imagetype:{x86 | x64 | Both}]	Controls which boot images will be shown to x64-based clients.
[/UseDhcpPorts:{Yes | No}]	Specifies whether or not the PXE server should attempt to bind to the DHCP port, TCP port 67. If DHCP and Windows Deployment Services are running on the same computer, you should set this option to **No** to enable the DHCP server to utilize the port, and set the **/DhcpOption60** parameter to **Yes**. The default setting for this value is **Yes**.

Parameter	Description
[/DhcpOption60:{Yes | No}]	Specifies whether DHCP option 60 should be configured for PXE support. If DHCP and Windows Deployment Services are running on the same server, set this option to **Yes** and set the **/UseDhcpPorts** option to **No**. The default setting for this value is **No**.
[/RpcPort:<Port number>]	Specifies the TCP port number to be used to service client requests.
[/PxepromptPolicy]	Configures how known (prestaged) and new clients initiate a PXE boot. This option only applies to Windows Server 2008 R2. You set the settings using the following options: - [/Known:{OptIn|OptOut|Noprompt}] - Sets the policy for prestaged clients. - [/New:{OptIn|OptOut|Noprompt}] - Sets the policy for new clients. **OptIn** means the client needs to press a key in order to PXE boot, otherwise it will fall back to the next boot device. **Noprompt** means the client will always PXE Boot. **OptOut** means the client will PXE boot unless the Esc key is pressed.
[/BootProgram:<Relative path>] /Architecture:{x86 | ia64 | x64}	Specifies the relative path to the boot program in the remoteInstall folder (for example, **boot\x86\pxeboot.n12**), and specifies the architecture of the boot program.
[/N12BootProgram:<Relative path>] /Architecture:{x86 | ia64 | x64}	Specifies the relative path to the boot program that does not require pressing the F12 key (for example, **boot\x86\pxeboot.n12**), and specifies the architecture of the boot program.
[/BootImage:<Relative path>] /Architecture:{x86 | ia64 | x64}	Specifies the relative path to the boot image that booting clients should receive, and specifies the architecture of the boot image. You can specify this for each architecture.
[/PreferredDC:<DC Name>]	Specifies the name of the domain controller that Windows Deployment Services should use. This can be either the NetBIOS name or the FQDN.
[/PreferredGC:<GC Name>]	Specifies the name of the global catalog server that Windows Deployment Services should use. This can be either the NetBIOS name or the FQDN.
[/PrestageUsingMAC:{Yes | No}]	Specifies whether Windows Deployment Services, when creating computer accounts in AD DS, should use the MAC address rather than the GUID/UUID to identify the computer.

Parameter	Description
[/NewMachineNamingPolicy: <Policy>]	Specifies the format to use when generating computer names for clients. For information about the format to use for <policy>, right-click the server in the mmc snap-in, click **Properties**, and view the **directory Services** tab. For example, **/NewMachineNamingPolicy: %61Username%#**.
[/NewMachineOU]	Used to specify the location in AD DS where client computer accounts will be created. You specify the location using the following options. - [/type: Serverdomain | Userdomain | UserOU | Custom] Specifies the type of location. **Serverdomain** creates accounts in the same domain as the Windows Deployment Services server. **Userdomain** creates accounts in the same domain as the user performing the installation. **UserOU** creates accounts in the organizational unit of the user performing the installation. **Custom** allows you to specify a custom location (you must also specify a value for **/OU** with this option). - [/OU:<Domain name of OU>] - if you specify **Custom** for the **/type** option, this option specifies the organizational unit where computer accounts should be created.
[/DomainSearchOrder: {GCOnly | DCFirst}]	Specifies the policy for searching computer accounts in AD DS (global catalog or domain controller).
[/NewMachineDomainJoin: {Yes | No}]	Specifies whether or not a computer that is not already prestaged in AD DS should be joined to the domain during installation. The default setting is **Yes**.
[/WdsClientLogging]	Specifies the logging level for the server. - [/Enabled:{Yes | No}] - Enables or disables logging of Windows Deployment Services client actions. - [/LoggingLevel: {None | Errors | Warnings | Info} - Sets the logging level. **None** is equivalent to disabling logging. **Errors** is the lowest level of logging and indicates that only errors will be logged. **Warnings** includes both warnings and errors. **Info** is the highest level of logging and includes errors, warnings, and informational events.

Parameter	Description
[/WdsUnattend]	These settings control the unattended installation behavior of Windows Deployment Services client. You set the settings using the following options: - [/Policy:{Enabled | Disabled}] - Specifies whether or not unattended installation is used. - [/CommandlinePrecedence: {Yes | No}] - Specifies whether an Autounattend.xml file (if present on the client) or an unattended setup file that was passed directly to the Windows Deployment Services client with the /Unattend option will be used instead of an image unattend file during a client installation. The default setting is **No**. - [/File:<Relative path> /Architecture:{x86 | ia64 | x64}] - Specifies the file name, path, and architecture of the unattend file.
[/AutoaddPolicy]	These settings control the Auto-add policy. You define the settings using the following options: - [/Policy: {AdminApproval | Disabled}] - **AdminApprove** causes all unknown computers to be added to a pending queue, where the administrator can then review the list of computers and approve or reject each request, as appropriate. **Disabled** indicates that no additional action is taken when an unknown computer attempts to boots to the server. - [/PollInterval:{time in seconds}] - Specifies the interval (in seconds) at which the network boot program should poll the Windows Deployment Services server. - [/MaxRetry: <Number>] - Specifies the number of times the network boot program should poll the Windows Deployment Services server. This value, along with **/PollInterval**, dictates how long the network boot program will wait for an administrator to approve or reject the computer before timing out. For example, a **MaxRetry** value of 10 and a **PollInterval** vlue of 60 would indicate that the client should poll the server 10 times, waiting 60 seconds between tries. Therefore, the client would time out after 10 minutes (10 x 60 seconds = 10 minutes). - [/Message: <Message>] - Specifies the message that is displayed to the client on the network boot program dialog page. - [/RetentionPeriod] - Specifies the number of days a computer can be in a pending state before being automatically purged. - [/Approved: <time in days>] - Specifies the retention period for approved computers. You must use this parameter with the **/RetentionPeriod** option. - [/Others: <time in days>] - Specifies the retention period for unapproved computers (rejected or pending). You must use this parameter with the **/RetentionPeriod** option.

Parameter	Description
[/AutoaddSettings]	Specifies the default settings to be applied to each computer. You define the settings using the following options: - /Architecture: {x86 | ia64 | x64} - Specifies the architecture. - [/BootProgram: <Relative path>] - Specifies the boot program sent to the approved computer. If no boot program is specified, the default for the architecture of the computer (as specified on the server) will be used. - [/WdsClientUnattend: <Relative path>] - Sets the relative path to the unattend file that the approved client should receive. - [/ReferralServer: <Server name>] - Specifies the Windows Deployment Services server that the client will use to download images. - [/BootImage: <Relative path>] - Specifies the boot image that the approved client will receive. - [/User: <Domain\User | User@Domain>] - Sets permissions on the computer account object to give the specified user the necessary rights to join the computer to the domain. - [JoinRights: {JoinOnly | Full}] - Specifies the type of rights to be assigned to the user. **JoinOnly** requires the administrator to reset the computer account before the user can join the computer to the domain. **Full** gives full access to the user, including the right to join the computer to the domain. - [/JoinDomain: {Yes | No}] - Specifies whether or not the computer should be joined to the domain as this computer account during a Windows Deployment Services installation. The default setting is **Yes**.
[/BindPolicy]	Configures the network interfaces for the PXE provider to listen on. You define the policy using the following options: - [/Policy: {Include | Exclude}] - Sets the interface bind policy to include or exclude the addresses on the interface list. - [/add] - adds an interface to the list. You must also specify /addresstype and /address. - [/remove] - removes an interface from the list. You must also specify /addresstype and /address. - /address:<IP or MAC address> - Specifies the IP or MAC address of the interface to add or remove. - /addresstype: {IP | MAC} - Indicates the type of address specified in the **/address** option.
[/RefreshPeriod: <seconds>]	Specifies how often (in seconds) the server will refreshes its settings.

Parameter	Description
[/BannedGuidPolicy]	Manages the list of banned GUIDs using the following options: - [/add] /Guid:<GUID> - adds the specified GUID to the list of banned GUIDs. Any client with this GUID will be identified by its MAC address instead. - [/remove] /Guid:<GUID> - removes the specified GUID from the list of banned GUIDs.
[/BcdRefreshPolicy]	Configures the settings for refreshing Bcd files using the following options: - [/Enabled:{Yes | No}] - Specifies the Bcd refreshing policy. When **/Enabled** is set to **Yes**, Bcd files are refreshed at the specified time interval. - [/RefreshPeriod:<time in minutes>] - Specifies the time interval at which Bcd files are refreshed.
[/Transport]	Configures the following options: • [/ObtainIpv4From: {Dhcp | Range}] - Specifies the source of IPv4 addresses. ◦ [/start: <starting Ipv4 address>] - Specifies the start of the IP address range. This option is required and valid only if **/ObtainIpv4From** is set to **Range** ◦ [/End: <Ending Ipv4 address>] - Specifies the end of the IP address range. This option is required and valid only if **/ObtainIpv4From** is set to **Range**. • [/ObtainIpv6From:Range] [/start:<start IP address>] [/End: <End IP address>] Specifies the source of IPv6 addresses. This option only applies to Windows Server 2008 R2 and the only supported value is Range. • [/startPort: <starting port>] - Specifies the start of the port range. • [/EndPort: <Ending port>] - Specifies the end of the port range. • [/Profile: {10Mbps | 100Mbps | 1Gbps | Custom}] - Specifies the network profile to be used. This option is only supported forservers running Windows Server 2008. • [/MulticastSessionPolicy] Configures the transfer settings for multicast transmissions. This command is only available for Windows Server 2008 R2. ◦ [/Policy:{None | AutoDisconnect | Multistream}] - Determines how to handle slow clients. None means to keep all clients in one session at the same speed. AutoDisconnect means that any clients that drop below the specified /Threshold will be disconnected. Multistream means clients will be separated into multiple sessions as specified by /StreamCount. ◦ [/Threshold:<Speed in KBps>] - for /Policy:AutoDisconnect, this option sets the minimum

Parameter	Description
	transfer rate in KBps. Clients that drop below this rate will be disconnected from multicast transmissions. ◦ [/StreamCount:{2 | 3}] [/Fallback:{Yes | No}] - for /Policy:Multistream, this option determines the number of sessions. 2 means two sessions (fast and slow) 3 means three sessions (slow, medium, fast). ◦ [/Fallback:{Yes | No}] - Determines whether clients that are disconnected will continue the transfer using another method (if supported by the client). If you are using the WDS client, the computer will fallback to unicasting. Wdsmcast.exe does not support a fallback mechanism. This option also applies to clients that do not support Multistream. In that case, the computer will fall back to another method instead of moving to a slower transfer session.

Examples

To set the server to answer only known clients, with a response delay of 4 minutes, type:

```
wdsutil /Set-Server /AnswerClients:Known /Responsedelay:4
```

To set the boot program and architecture for the server, type:

```
wdsutil /Set-Server /BootProgram:boot\x86\pxeboot.n12 /Architecture:x86
```

To enable logging on the server, type:

```
wdsutil /Set-Server /WdsClientLogging /Enabled:Yes /LoggingLevel:Warnings
```

To enable unattend on the server, as well as the architecture and the client unattend file, type:

```
wdsutil /Set-Server /WdsUnattend /Policy:Enabled /File:WDSClientUnattend
\unattend.xml /Architecture:x86
```

To set the Pre-Boot execution Environment (PXE) server to attempt to bind to TCP ports 67 and 60, type:

```
wdsutil /Set-server /UseDhcpPorts:No /DhcpOption60:Yes
```

Related links

- Command-Line Syntax Key
- wdsutil disable-server command
- wdsutil enable-server command
- wdsutil get-server command
- wdsutil initialize-server command
- wdsutil start-server command
- wdsutil stop-server command
- wdsutil uninitialize-server command

wdsutil set-transportserver

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Sets configuration settings for a Transport Server.

Syntax

```
wdsutil [Options] /Set-TransportServer [/Server:<Server name>]
     [/ObtainIpv4From:{Dhcp | Range}]
        [/start:<starting IP address>]
        [/End:<Ending IP address>]
     [/ObtainIpv6From:Range]\n\
        [/start:<start IP address>]\n\
        [/End:<End IP address>]
     [/startPort:<starting port>
        [/EndPort:<starting port>
     [/Profile:{10Mbps | 100Mbps | 1Gbps | Custom}]
     [/MulticastSessionPolicy]
             [/Policy:{None | AutoDisconnect | Multistream}]
                 [/Threshold:<Speed in KBps>]
                 [/StreamCount:{2 | 3}]
                 [/Fallback:{Yes | No}]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the Transport Server. This can be the NetBIOS name or the fully qualified domain name (FQDN). If no Transport Server name is specified, the local server is used.
[/ObtainIpv4From:{Dhcp | Range}]	Sets the source of the IPv4 addresses as follows: - [/start: <IP address>] Sets the start of the IP address range. This is required and valid only if this option is set to **Range**. - [/End: <IP address>] Sets the end of the IP address range. This is required and valid only if this option is set to **Range**. - [/startPort: <port>] Sets the start of the port range. - [/EndPort: <port>] Sets the end of the port range.

Parameter	Description
[/ObtainIpv6From:Range]	Specifies the source of IPv6 addresses. This option only applies to Windows Server 2008 R2 and the only supported value is **Range**. - [/start: <IP address>] Sets the start of the IP address range. This is required and valid only if this option is set to **Range**. - [/End: <IP address>] Sets the end of the IP address range. This is required and valid only if this option is set to **Range**. - [/startPort: <port>] Sets the start of the port range. - [/EndPort: <port>] Sets the end of the port range.
[/Profile: {10Mbps | 100Mbps | 1Gbps | Custom}]	Specifies the network profile to be used. This option is only available for servers running Windows Server 2008 or Windows Server 2003.
[/MulticastSessionPolicy]	Configures the transfer settings for multicast transmissions. This command is only available for Windows Server 2008 R2. - [/Policy:{None | AutoDisconnect | Multistream}] Determines how to handle slow clients. **None** means to keep all clients in one session at the same speed. **AutoDisconnect** means that any clients that drop below the specified **/Threshold** are disconnected. **Multistream** means clients will be separated into multiple sessions as specified by **/StreamCount**. - [/Threshold:<Speed in KBps>] Sets the minimum transfer rate in KBps for **/Policy:AutoDisconnect**. Clients that drop below this rate are disconnected from multicast transmissions. - [/StreamCount:{2 | 3}] [/Fallback:{Yes | No}] Determines the number of sessions for **/Policy:Multistream**. **2** means two sessions (fast and slow), and **3** means three sessions (slow, medium, fast). - [/Fallback:{Yes | No}] Determines whether clients tha are disconnected will continue the transfer by using another method (if supported by the client). If you are using the WDS client, the computer will fall back to unicasting. Wdsmcast.exe does not support a fallback mechanism. This option also applies to clients that do not support **Multistream**. In that case, the computer will fall back to another method instead of moving to a slower transfer session.

Examples

To set the IPv4 address range for the server, type:

```
wdsutil /Set-TransportServer /ObtainIpv4From:Range /start:239.0.0.1
/End:239.0.0.100
```

To set the IPv4 address range, port range, and profile for the server, type:

```
wdsutil /Set-TransportServer /Server:MyWDSServer /ObtainIpv4From:Range
/start:239.0.0.1 /End:239.0.0.100 /startPort:12000 /EndPort:50000
/Profile:10mbps
```

Related links

- Command-Line Syntax Key
- wdsutil disable-transportserver command
- wdsutil enable-transportserver command
- wdsutil get-transportserver command
- wdsutil start-transportserver command
- wdsutil stop-transportserver command

wdsutil start-multicasttransmission

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Starts a Scheduled-Cast transmission of an image.

Syntax

Windows Server 2008

```
wdsutil /start-MulticastTransmissiomedia:<Image name> [/Server:<Server
namemediatype:InstallmediaGroup:<Image group name>] [/Filename:<File name>]
```

Windows Server 2008 R2 for boot images:

```
wdsutil [Options] /start-MulticastTransmissiomedia:<Image name>
        [/Server:<Server name>]
      mediatype:Boot
        /Architecture:{x86 | ia64 | x64}
        [/Filename:<File name>]
```

for install images:

```
wdsutil [Options] /start-MulticastTransmissiomedia:<Image name>
        [/Server:<Server name>]
      mediatype:Install
       mediaGroup:<Image Group>]
        [/Filename:<File name>]
```

Parameters

Parameter	Description

Parameter	Description
media: <Image name>	Specifies the name of the image.
[/Server: <Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.
mediatype: {Install|Boot}	Specifies the image type. Note that this option must be set to **Install** for Windows Server 2008.
/Architecture: {x86 | ia64 | x64}	The architecture of the boot image that is associated with the transmission to start. Since it is possible to have the same image name for boot images in different architectures, you should specify the architecture to ensure that the correct transmission is used.
\mediaGroup: <Image group name>]	Specifies the image group of the image. If no image group name is specified and only one image group exists on the server, that image group will be used. If more than one image group exists on the server, you must use this option to specify the image group name.
[/Filename: <File name>]	Specifies the name of the file that contains the image. If the image cannot be uniquely identified by name, you must use this option to specify the file name.

Examples

To start a multicast transmission, type one of the following:

```
wdsutil /start-MulticastTransmissiomedia:Vista with Office
/Imagetype:Install
wdsutil /start-MulticastTransmission /Server:MyWDSServemedia:Vista with
Officemediatype:InstalmediaGroup:ImageGroup1 /Filename:install.wim
```

To start a boot image multicast transmission for Windows Server 2008 R2, type:

```
wdsutil /start-MulticastTransmission /Server:MyWDSServemedia:X64 Boot
Imagemediatype:Boot /Architecture:x64
/Filename:boot.wim\n\
```

Related links

- Command-Line Syntax Key
- wdsutil get-allmulticasttransmissions command
- wdsutil get-multicasttransmission command
- wdsutil new-multicasttransmission command
- wdsutil remove-multicasttransmission command

wdsutil start-namespace

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Starts a Scheduled-Cast namespace.

Syntax

```
wdsutil /start-Namespace /Namespace:<Namespace name[/Server:<Server name>]
```

Parameters

Parameter	Description
/Namespace:<Namespace name>	Specifies the name of the namespace. Note that this is not the friendly name, and it must be unique. - **Deployment Server**: The syntax for namespace name is /Namspace:WDS:<Image group>/<Image name>/<Index>. For example: **WDS:ImageGroup1/install.wim/1** - **Transport Server**: This name must match the name given to the namespace when it was created on the server.
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Examples

To start a namespace, type one of the following:

```
wdsutil /start-Namespace /Namespace:Custom Auto 1
wdsutil /start-Namespace /Server:MyWDSServer /Namespace:Custom Auto 1
```

Related links

- Command-Line Syntax Key
- wdsutil get-allnamespaces command
- wdsutil new-namespace command
- wdsutil remove-namespace command

wdsutil start-server

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Starts all services for a Windows Deployment Services server.

Syntax

```
wdsutil [Options] /start-Server [/Server:<Server name>]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server to be started. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Examples

To start the server, type one of the following:

```
wdsutil /start-Server
wdsutil /verbose /start-Server /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key
- wdsutil disable-server command
- wdsutil enable-server command
- wdsutil get-server command
- wdsutil initialize-server command

- wdsutil set-server command
- wdsutil stop-server command
- wdsutil start-server command
- wdsutil uninitialize-server command

wdsutil start-transportserver

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Starts all services for a Transport Server.

Syntax

```
wdsutil [Options] /start-TransportServer [/Server:<Server name>]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the Transport Server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Examples

To start the server, type one of the following:

```
wdsutil /start-TransportServer
wdsutil /verbose /start-TransportServer /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key
- wdsutil disable-transportserver command
- wdsutil enable-transportserver command
- wdsutil get-transportserver command
- wdsutil set-transportserver command

- wdsutil stop-transportserver command

wdsutil stop-server

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Stops all services on a Windows Deployment Services server.

Syntax

```
wdsutil [Options] /Stop-Server [/Server:<Server name>]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Examples

To stop the services, type one of the following:

```
wdsutil /Stop-Server
wdsutil /verbose /Stop-Server /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key
- wdsutil disable-server command
- wdsutil enable-server command
- wdsutil get-server command
- wdsutil initialize-server command

- wdsutil set-server command
- wdsutil start-server command
- wdsutil uninitialize-server command

wdsutil stop-transportserver

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Stops all services on a Transport Server.

Syntax

```
wdsutil [Options] /Stop-TransportServer [/Server:<Server name>]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the Transport Server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no Transport Server is specified, the local server will be used.

Examples

To stop the services, type one of the following:

```
wdsutil /Stop-TransportServer
wdsutil /verbose /Stop-TransportServer /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key
- wdsutil disable-transportserver command
- wdsutil enable-transportserver command
- wdsutil get-transportserver command
- wdsutil set-transportserver command

- wdsutil start-transportserver command

wdsutil uninitialize-server

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Reverts changes made to the server during the initial server configuration. This includes changes made by either the **/initialize-server** option or the Windows Deployment Services mmc snap-in. Note that this command resets the server to an unconfigured state. This command does not modify the contents of the remoteInstall shared folder. Rather, it resets the server's state so that you can reinitialize the server.

Syntax

```
wdsutil [Options] /Uninitialize-Server [/Server:<Server name>]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Examples

To reinitialize the server, type one of the following:

```
wdsutil /Uninitialize-Server
wdsutil /verbose /Uninitialize-Server /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key

- wdsutil disable-server command
- wdsutil enable-server command
- wdsutil get-server command
- wdsutil initialize-server command
- wdsutil set-server command
- wdsutil start-server command
- wdsutil stop-server command

Update-ServerFiles

Article • 02/03/2023

Updates files in the REMINST shared folder by using the latest files that are stored in the server's %Windir%\System32\RemInst folder. To ensure the validity of your Windows Deployment Services installation, you should run this command once after each server upgrade, service pack installation, or update to Windows Deployment Services files.

Syntax

```
wdsutil [Options] /Update-ServerFiles [/Server:<Server name>]
```

Parameters

Parameter	Description
[/Server:<Server name>]	Specifies the name of the server. This can be either the NetBIOS name or the fully qualified domain name (FQDN). If no server name is specified, the local server will be used.

Examples

To update the files, type one of the following:

```
wdsutil /Update-ServerFiles
wdsutil /Verbose /Progress /Update-ServerFiles /Server:MyWDSServer
```

Related links

- Command-Line Syntax Key

Using the verbose command

Article • 03/03/2021

Displays verbose output for a specified command. You can use **/verbose** with any other wdsutil commands that you run. Note that you must specify **/verbose** and **/progress** directly after **wdsutil**.

Syntax

```
wdsutil /verbose <commands>
```

Examples

To delete approved computers from the Auto-Add database and show verbose output, type:

```
wdsutil /Verbose /progress /Delete-AutoAddDevices /Server:MyWDSServer
/DeviceType:ApprovedDevices
```

wecutil

Article • 02/03/2023

Enables you to create and manage subscriptions to events that are forwarded from remote computers. The remote computer must support the WS-Management protocol.

> **Important**
>
> If you receive the message, "The RPC server is unavailable? when you try to run wecutil, you need to start the Windows Event Collector service (wecsvc). To start wecsvc, at an elevated command prompt type `net start wecsvc`.

Syntax

command

```
wecutil [{es | enum-subscription}] [{gs | get-subscription} <Subid> [/f:
<Format>] [/uni:<Unicode>]] [{gr | get-subscriptionruntimestatus} <Subid>
[<Eventsource> …]] [{ss | set-subscription} [<Subid> [/e:[<Subenabled>]]
[/esa:<Address>] [/ese:[<Srcenabled>]] [/aes] [/res] [/un:<Username>] [/up:
<Password>] [/d:<Desc>] [/uri:<Uri>] [/cm:<Configmode>] [/ex:<Expires>] [/q:
<Query>] [/dia:<Dialect>] [/tn:<Transportname>] [/tp:<Transportport>] [/dm:
<Deliverymode>] [/dmi:<Deliverymax>] [/dmlt:<Deliverytime>] [/hi:
<Heartbeat>] [/cf:<Content>] [/l:<Locale>] [/ree:[<Readexist>]] [/lf:
<Logfile>] [/pn:<Publishername>] [/essp:<Enableport>] [/hn:<Hostname>] [/ct:
<Type>]] [/c:<Configfile> [/cun:<Username> /cup:<Password>]]] [{cs | create-
subscription} <Configfile> [/cun:<Username> /cup:<Password>]] [{ds | delete-
subscription} <Subid>] [{rs | retry-subscription} <Subid> [<Eventsource>…]]
[{qc | quick-config} [/q:[<quiet>]]]
```

Parameters

Parameter	Description
`{es | enum-subscription}`	Displays the names of all remote event subscriptions that exist.
`{gs | get-subscription} <Subid> [/f:<Format>] [/uni:<Unicode>]`	Displays remote subscription configuration information. `<Subid>` is a string that uniquely identifies a subscription. It's the same as the string that was specified in the `<SubscriptionId>` tag of the XML configuration file, which was used to create the subscription.

Parameter	Description
`{gr | get-subscriptionruntimestatus} <Subid> [<Eventsource> …]`	Displays the runtime status of a subscription. `<Subid>` is a string that uniquely identifies a subscription. It's the same as the string that was specified in the `<SubscriptionId>` tag of the XML configuration file, which was used to create the subscription. `<Eventsource>` is a string that identifies a computer that serves as a source of events. It should be a fully qualified domain name, a NetBIOS name, or an IP address.
`{ss | set-subscription} <Subid> [/e:[<Subenabled>]] [/esa:<Address>] [/ese:[<Srcenabled>]] [/aes] [/res] [/un:<Username>] [/up:<Password>] [/d:<Desc>] [/uri:<Uri>] [/cm:<Configmode>] [/ex:<Expires>] [/q:<Query>] [/dia:<Dialect>] [/tn:<Transportname>] [/tp:<Transportport>] [/dm:<Deliverymode>] [/dmi:<Deliverymax>] [/dmlt:<Deliverytime>] [/hi:<Heartbeat>] [/cf:<Content>] [/l:<Locale>] [/ree:[<Readexist>]] [/lf:<Logfile>] [/pn:<Publishername>] [/essp:<Enableport>] [/hn:<Hostname>] [/ct:<Type>]` **OR** `{ss | set-subscription /c:<Configfile> [/cun:<Comusername> /cup:<Compassword>]`	Changes the subscription configuration. You can specify the subscription ID and the appropriate options to change subscription parameters, or you can specify an XML configuration file to change subscription parameters.
`{cs | create-subscription} <Configfile> [/cun:<Username> /cup:<Password>]`	Creates a remote subscription. `<Configfile>` specifies the path to the XML file that contains the subscription configuration. The path can be absolute or relative to the current directory.
`{ds | delete-subscription} <Subid>`	Deletes a subscription and unsubscribes from all event sources that deliver events into the event log for the subscription. Any events already received and logged are not deleted. `<Subid>` is a string that uniquely identifies a subscription. It's the same as the string that was specified in the `<SubscriptionId>` tag of the XML configuration file, which was used to create the subscription.

Parameter	Description
`{rs | retry-subscription} <Subid> [<Eventsource>…]`	Retries to establish a connection and send a remote subscription request to an inactive subscription. Attempts to reactivate all event sources or specified event sources. Disabled sources are not retried. `<Subid>` is a string that uniquely identifies a subscription. It's the same as the string that was specified in the `<SubscriptionId>` tag of the XML configuration file, which was used to create the subscription. `<Eventsource>` is a string that identifies a computer that serves as a source of events. It should be a fully qualified domain name, a NetBIOS name, or an IP address.
`{qc | quick-config} [/q:[<Quiet>]]`	Configures the Windows Event Collector service to ensure a subscription can be created and sustained through reboots. This includes the following steps: 1. Enable the ForwardedEvents channel if it is disabled. 2. Set the Windows Event Collector service to delay start. 3. Start the Windows Event Collector service if it is not running.

Options

Option	Description
/f:`<Format>`	Specifies the format of the information that is displayed. `<Format>` can be XML or Terse. If it's **XML**, the output is displayed in XML format. If it's **Terse**, the output is displayed in name-value pairs. The default is **Terse**.
/c:`<Configfile>`	Specifies the path to the XML file that contains a subscription configuration. The path can be absolute or relative to the current directory. This option can only be used with the **/cun** and **/cup** options and is mutually exclusive with all other options.
/e:[`<Subenabled>`]	Enables or disables a subscription. `<Subenabled>` can be true or false. The default value of this option is **true**.

Option	Description
/esa:`<Address>`	Specifies the address of an event source. `<Address>` is a string that contains a fully qualified domain name, a NetBIOS name, or an IP address, which identifies a computer that serves as a source of events. This option should be used with the **/ese**, **/aes**, **/res**, or **/un** and **/up** options.
/ese:[`<Srcenabled>`]	Enables or disables an event source. `<Srcenabled>` can be true or false. This option is allowed only if the **/esa** option is specified. The default value of this option is **true**.
/aes	Adds the event source that is specified by the **/esa** option if it is not already a part of the subscription. If the address specified by the **/esa** option is already a part of the subscription, an error is reported. This option is only allowed if the **/esa** option is specified.
/res	Removes the event source that is specified by the **/esa** option if it is already a part of the subscription. If the address specified by the **/esa** option is not a part of the subscription, an error is reported. This option is only allowed if **/esa** option is specified.
/un:`<Username>`	Specifies the user credential to use with the event source specified by the **/esa** option. This option is only allowed if the **/esa** option is specified.
/up:`<Password>`	Specifies the password that corresponds to the user credential. This option is only allowed if the **/un** option is specified.
/d:`<Desc>`	Provides a description for the subscription.
/uri:`<Uri>`	Specifies the type of the events that are consumed by the subscription. `<Uri>` contains a URI string that is combined with the address of the event source computer to uniquely identify the source of the events. The URI string is used for all event source addresses in the subscription.
/cm:`<Configmode>`	Sets the configuration mode. `<Configmode>` can be one of the following strings: **Normal**, **Custom**, **MinLatency** or **MinBandwidth**. The **Normal**, **MinLatency**, and **MinBandwidth** modes set delivery mode, delivery max items, heartbeat interval, and delivery max latency time. The **/dm**, **/dmi**, **/hi** or **/dmlt** options may only be specified if the configuration mode is set to **Custom**.
/ex:`<Expires>`	Sets the time when the subscription expires. `<Expires>` should be defined in standard XML or ISO8601 date-time format: `yyyy-MM-ddThh:mm:ss[.sss][Z]`, where *T* is the time separator and *Z* indicates UTC time.
/q:`<Query>`	Specifies the query string for the subscription. The format of `<Query>` may be different for different URI values and applies to all sources in the subscription.
/dia:`<Dialect>`	Defines the dialect that the query string uses.

Option	Description
/tn:`<Transportname>`	Specifies the name of the transport that is used to connect to a remote event source.
/tp:`<Transportport>`	Sets the port number that is used by the transport when connecting to a remote event source.
/dm:`<Deliverymode>`	Specifies the delivery mode. `<Deliverymode>` can be either pull or push. This option is only valid if the **/cm** option is set to **Custom**.
/dmi:`<Deliverymax>`	Sets the maximum number of items for batched delivery. This option is only valid if **/cm** is set to **Custom**.
/dmlt:`<Deliverytime>`	Sets the maximum latency in delivering a batch of events. `<Deliverytime>` is the number of milliseconds. This option is only valid if **/cm** is set to Custom.
/hi:`<Heartbeat>`	Defines the heartbeat interval. `<Heartbeat>` is the number of milliseconds. This option is only valid if **/cm** is set to **Custom**.
/cf:`<Content>`	Specifies the format of the events that are returned. `<Content>` can be Events or RenderedText. When the value is **RenderedText**, the events are returned with the localized strings (such as event description) attached to the event. The default value is **RenderedText**.
/l:`<Locale>`	Specifies the locale for delivery of the localized strings in RenderedText format. `<Locale>` is a language and country/region identifier, for example, EN-us. This option is only valid if the **/cf** option is set to **RenderedText**.
/ree:[`<Readexist>`]	Identifies the events that are delivered for the subscription. `<Readexist>` can true or false. When the `<Readexist>` is true, all existing events are read from the subscription event sources. When the `<Readexist>` is false, only future (arriving) events are delivered. The default value is **true** for a **/ree** option without a value. If no **/ree** option is specified, the default value is **false**.
/lf:`<Logfile>`	Specifies the local event log that is used to store events received from the event sources.
/pn:`<Publishername>`	Specifies the publisher name. It must be a publisher that owns or imports the log specified by the **/lf** option.
/essp:`<Enableport>`	Specifies that the port number must be appended to the service principal name of the remote service. `<Enableport>` can be true or false. The port number is appended when `<Enableport>` is true. When the port number is appended, some configuration may be required to prevent the access to event sources from being denied.

Option	Description
/hn:`<Hostname>`	Specifies the DNS name of the local computer. This name is used by remote event source to push back events and must be used only for a push subscription.
/ct:`<Type>`	Sets the credential type for the remote source access. `<Type>` should be one of the following values: **default**, **negotiate**, **digest**, **basic** or **localmachine**. The default value is **default**.
/cun:`<Comusername>`	Sets the shared user credential to be used for event sources that do not have their own user credentials. If this option is specified with the **/c** option, UserName and UserPassword settings for individual event sources from the configuration file are ignored. If you want to use a different credential for a specific event source, you should override this value by specifying the **/un** and **/up** options for a specific event source on the command line of another **ss** command.
/cup:`<Compassword>`	Sets the user password for the shared user credential. When `<Compassword>` is set to * (asterisk), the password is read from the console. This option is only valid when the **/cun** option is specified.
/q:[`<Quiet>`]	Specifies whether the configuration procedure prompts for confirmation. `<Quiet>` can be true or false. If `<Quiet>` is true, the configuration procedure does not prompt for confirmation. The default value of this option is **false**.

Examples

To show the contents of a configuration file, type:

XML

```
<Subscription
xmlns=https://schemas.microsoft.com/2006/03/windows/events/subscription>
<Uri>https://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</Uri>
<!-- Use Normal (default), Custom, MinLatency, MinBandwidth -->
<ConfigurationMode>Normal</ConfigurationMode>
  <Description>Forward Sample Subscription</Description>
  <SubscriptionId>SampleSubscription</SubscriptionId>
  <Query><![CDATA[
    <QueryList>
      <Query Path=Application>
        <Select>*</Select>
      </Query>
    </QueryList>]]
  </Query>
<EventSources>
  <EventSource Enabled=true>
    <Address>mySource.myDomain.com</Address>
```

```
    <UserName>myUserName</UserName>
    <Password>*</Password>
  </EventSource>
</EventSources>
<CredentialsType>Default</CredentialsType>
<Locale Language=EN-US></Locale>
</Subscription>
```

To view the output configuration information for a subscription named *sub1*, type:

command

```
wecutil gs sub1
```

Example output:

Output

```
EventSource[0]:
Address: localhost
Enabled: true
Description: Subscription 1
Uri: wsman:microsoft/logrecord/sel
DeliveryMode: pull
DeliveryMaxSize: 16000
DeliveryMaxItems: 15
DeliveryMaxLatencyTime: 1000
HeartbeatInterval: 10000
Locale:
ContentFormat: renderedtext
LogFile: HardwareEvents
```

To display the runtime status of a subscription named sub1, type:

command

```
wecutil gr sub1
```

To update the subscription configuration named *sub1* from a new XML file called *WsSelRg2.xml*, type:

command

```
wecutil ss sub1 /c:%Windir%system32WsSelRg2.xml
```

To update the subscription configuration named *sub2* with multiple parameters, type:

command

```
wecutil ss sub2 /esa:myComputer /ese /un:uname /up:* /cm:Normal
```

To delete a subscription named *sub1*, type:

```
wecutil ds sub1
```

Related links

- Command-Line Syntax Key

wevtutil

Article • 02/03/2023

Enables you to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, to run queries, and to export, archive, and clear logs.

Syntax

```
wevtutil [{el | enum-logs}] [{gl | get-log} <Logname> [/f:<Format>]]
[{sl | set-log} <Logname> [/e:<Enabled>] [/i:<Isolation>] [/lfn:<Logpath>]
[/rt:<Retention>] [/ab:<Auto>] [/ms:<MaxSize>] [/l:<Level>] [/k:<Keywords>]
[/ca:<Channel>] [/c:<Config>]]
[{ep | enum-publishers}]
[{gp | get-publisher} <Publishername> [/ge:<Metadata>] [/gm:<Message>] [/f:
<Format>]]
[{im | install-manifest} <Manifest>] [/rf:<Path>] [/mf:<Path>] [/pf:<Path>]
[{um | uninstall-manifest} <Manifest>] [{qe | query-events} <Path> [/lf:
<Logfile>] [/sq:<Structquery>] [/q:<Query>] [/bm:<Bookmark>] [/sbm:<Savebm>]
[/rd:<Direction>] [/f:<Format>] [/l:<Locale>] [/c:<Count>] [/e:<Element>]]
[{gli | get-loginfo} <Logname> [/lf:<Logfile>]]
[{epl | export-log} <Path> <Exportfile> [/lf:<Logfile>] [/sq:<Structquery>]
[/q:<Query>] [/ow:<Overwrite>]]
[{al | archive-log} <Logpath> [/l:<Locale>]]
[{cl | clear-log} <Logname> [/bu:<Backup>]] [/r:<Remote>] [/u:<Username>]
[/p:<Password>] [/a:<Auth>] [/uni:<Unicode>]
```

Parameters

Parameter	Description
{el | enum-logs}	Displays the names of all logs.
{gl | get-log} <Logname> [/f:<Format>]	Displays configuration information for the specified log, which includes whether the log is enabled or not, the current maximum size limit of the log, and the path to the file where the log is stored.

Parameter	Description
{sl | set-log} <Logname> [/e:<Enabled>] [/i:<Isolation>] [/lfn:<Logpath>] [/rt:<Retention>] [/ab:<Auto>] [/ms:<MaxSize>] [/l:<Level>] [/k:<Keywords>] [/ca:<Channel>] [/c:<Config>]	Modifies the configuration of the specified log.
{ep | enum-publishers}	Displays the event publishers on the local computer.
{gp | get-publisher} <Publishername> [/ge:<Metadata>] [/gm:<Message>] [/f:<Format>]]	Displays the configuration information for the specified event publisher.
{im | install-manifest} <Manifest> [/{rf | resourceFilePath}:value] [/{mf | messageFilePath}:value] [/{pf | parameterFilePath}:value]	Installs event publishers and logs from a manifest. For more information about event manifests and using this parameter, see the Windows Event Log SDK at the Microsoft Developers Network (MSDN) Web site (https://msdn.microsoft.com). The **value** is the full path to the mentioned file.
{um | uninstall-manifest} <Manifest>	Uninstalls all publishers and logs from a manifest. For more information about event manifests and using this parameter, see the Windows Event Log SDK at the Microsoft Developers Network (MSDN) Web site (https://msdn.microsoft.com).
{qe | query-events} <Path> [/lf:<Logfile>] [/sq:<Structquery>] [/q:<Query>] [/bm:<Bookmark>] [/sbm:<Savebm>] [/rd:<Direction>] [/f:<Format>] [/l:<Locale>] [/c:<Count>] [/e:<Element>]	Reads events from an event log, from a log file, or using a structured query. By default, you provide a log name for <Path>. However, if you use the **/lf** option, then <Path> must be a path to a log file. If you use the **/sq** parameter, <Path> must be a path to a file that contains a structured query.
{gli | get-loginfo} <Logname> [/lf:<Logfile>]	Displays status information about an event log or log file. If the **/lf** option is used, <Logname> is a path to a log file. You can run **wevtutil el** to obtain a list of log names.
{epl | export-log} <Path> <Exportfile> [/lf:<Logfile>] [/sq:<Structquery>] [/q:<Query>] [/ow:<Overwrite>]	Exports events from an event log, from a log file, or using a structured query to the specified file. By default, you provide a log name for <Path>. However, if you use the **/lf** option, then <Path> must be a path to a log file. If you use the **/sq** option, <Path> must be a path to a file that contains a structured query. <Exportfile> is a path to the file where the exported events will be stored.

Parameter	Description
{al | archive-log} <Logpath> [/l:<Locale>]	Archives the specified log file in a self-contained format. A subdirectory with the name of the locale is created and all locale-specific information is saved in that subdirectory. After the directory and log file are created by running **wevtutil al**, events in the file can be read whether the publisher is installed or not.
{cl | clear-log} <Logname> [/bu:<Backup>]	Clears events from the specified event log. The **/bu** option can be used to back up the cleared events.

Options

Option	Description
/f:<Format>	Specifies that the output should be either XML or text format. If <Format> is XML, the output is displayed in XML format. If <Format> is Text, the output is displayed without XML tags. The default is Text.
/e:<Enabled>	Enables or disables a log. <Enabled> can be true or false.
/i:<Isolation>	Sets the log isolation mode. <Isolation> can be system, application or custom. The isolation mode of a log determines whether a log shares a session with other logs in the same isolation class. If you specify system isolation, the target log will share at least write permissions with the System log. If you specify application isolation, the target log will share at least write permissions with the Application log. If you specify custom isolation, you must also provide a security descriptor by using the **/ca** option.
/lfn: <Logpath>	Defines the log file name. <Logpath> is a full path to the file where the Event Log service stores events for this log.
/rt: <Retention>	Sets the log retention mode. <Retention> can be true or false. The log retention mode determines the behavior of the Event Log service when a log reaches its maximum size. If an event log reaches its maximum size and the log retention mode is true, existing events are retained, and incoming events are discarded. If the log retention mode is false, incoming events overwrite the oldest events in the log.
/ab:<Auto>	Specifies the log auto-backup policy. <Auto> can be true or false. If this value is true, the log will be backed up automatically when it reaches the maximum size. If this value is true, the retention (specified with the **/rt** option) must also be set to true.
/ms: <MaxSize>	Sets the maximum size of the log in bytes. The minimum log size is 1048576 bytes (1024KB) and log files are always multiples of 64KB, so the value you enter will be rounded off accordingly.

Option	Description
/l:<Level>	Defines the level filter of the log. <Level> can be any valid level value. This option is only applicable to logs with a dedicated session. You can remove a level filter by setting <Level> to 0.
/k: <Keywords>	Specifies the keywords filter of the log. <Keywords> can be any valid 64-bit keyword mask. This option is only applicable to logs with a dedicated session.
/ca: <Channel>	Sets the access permission for an event log. <Channel> is a security descriptor that uses the Security Descriptor Definition Language (SDDL). For more information about SDDL format, see the Microsoft Developers Network (MSDN) Web site (https://msdn.microsoft.com).
/c:<Config>	Specifies the path to a configuration file. This option will cause log properties to be read from the configuration file defined in <Config>. If you use this option, you must not specify a <Logname> parameter. The log name will be read from the configuration file.
/ge: <Metadata>	Gets metadata information for events that can be raised by this publisher. <Metadata> can be true or false.
/gm: <Message>	Displays the actual message instead of the numeric message ID. <Message> can be true or false.
/lf:<Logfile>	Specifies that the events should be read from a log or from a log file. <Logfile> can be true or false. If true, the parameter to the command is the path to a log file.
/sq: <Structquery>	Specifies that events should be obtained with a structured query. <Structquery> can be true or false. If true, <Path> is the path to a file that contains a structured query.
/q:<Query>	Defines the XPath query to filter the events that are read or exported. If this option is not specified, all events will be returned or exported. This option is not available when **/sq** is true.
/bm: <Bookmark>	Specifies the path to a file that contains a bookmark from a previous query.
/sbm: <Savebm>	Specifies the path to a file that is used to save a bookmark of this query. The file name extension should be .xml.
/rd: <Direction>	Specifies the direction in which events are read. <Direction> can be true or false. If true, the most recent events are returned first.
/l:<Locale>	Defines a locale string that is used to print event text in a specific locale. Only available when printing events in text format using the **/f** option.
/c:<Count>	Sets the maximum number of events to read.

Option	Description
/e:<Element>	Includes a root element when displaying events in XML. <Element> is the string that you want within the root element. For example, **/e:root** would result in XML that contains the root element pair <root>.
/ow:<Overwrite>	Specifies that the export file should be overwritten. <Overwrite> can be true or false. If true, and the export file specified in <Exportfile> already exists, it will be overwritten without confirmation.
/bu:<Backup>	Specifies the path to a file where the cleared events will be stored. Include the .evtx extension in the name of the backup file.
/r:<Remote>	Runs the command on a remote computer. <Remote> is the name of the remote computer. The **im** and **um** parameters do not support remote operation.
/u:<Username>	Specifies a different user to log on to a remote computer. <Username> is a user name in the form domain\user or user. This option is only applicable when the **/r** option is specified.
/p:<Password>	Specifies the password for the user. If the **/u** option is used and this option is not specified or <Password> is *, the user will be prompted to enter a password. This option is only applicable when the **/u** option is specified.
/a:<Auth>	Defines the authentication type for connecting to a remote computer. <Auth> can be Default, Negotiate, Kerberos or NTLM. The default is Negotiate.
/uni:<Unicode>	Displays the output in Unicode. <Unicode> can be true or false. If <Unicode> is true then the output is in Unicode.

Remarks

- Using a configuration file with the sl parameter

  The configuration file is an XML file with the same format as the output of wevtutil gl <Logname> /f:xml. To shows the format of a configuration file that enables retention, enables autobackup, and sets the maximum log size on the Application log:

```
<?xml version=1.0 encoding=UTF-8?>
<channel name=Application isolation=Application
xmlns=https://schemas.microsoft.com/win/2004/08/events>
<logging>
<retention>true</retention>
<autoBackup>true</autoBackup>
<maxSize>9000000</maxSize>
</logging>
```

```
<publishing>
</publishing>
</channel>
```

Examples

List the names of all logs:

```
wevtutil el
```

Display configuration information about the System log on the local computer in XML format:

```
wevtutil gl System /f:xml
```

Use a configuration file to set event log attributes (see Remarks for an example of a configuration file):

```
wevtutil sl /c:config.xml
```

Display information about the Microsoft-Windows-Eventlog event publisher, including metadata about the events that the publisher can raise:

```
wevtutil gp Microsoft-Windows-Eventlog /ge:true
```

Install publishers and logs from the myManifest.xml manifest file:

```
wevtutil im myManifest.xml
```

Uninstall publishers and logs from the myManifest.xml manifest file:

```
```

```
wevtutil um myManifest.xml
```

Display the three most recent events from the Application log in textual format:

```
wevtutil qe Application /c:3 /rd:true /f:text
```

Display the status of the Application log:

```
wevtutil gli Application
```

Export events from System log to C:\backup\system0506.evtx:

```
wevtutil epl System C:\backup\system0506.evtx
```

Clear all of the events from the Application log after saving them to C:\admin\backups\a10306.evtx:

```
wevtutil cl Application /bu:C:\admin\backups\a10306.evtx
```

Archive the specified (*.evtx*) log file in a self-contained format. A subdirectory (LocaleMetaData) is created and all locale-specific information is saved in that subdirectory:

```
wevtutil archive-log "C:\backup\Application.evtx" /locale:en-us
```

Related links

- Command-Line Syntax Key

where

Article • 02/03/2023

Displays the location of files that match the given search pattern.

Syntax

```
where [/r <Dir>] [/q] [/f] [/t] [$<ENV>:|<Path>:]<Pattern>[ ...]
```

Parameters

Parameter	Description
/r <Dir>	Indicates a recursive search, starting with the specified directory.
/q	Returns an exit code (**0** for success, **1** for failure) without displaying the list of matched files.
/f	Displays the results of the **where** command in quotation marks.
/t	Displays the file size and the last modified date and time of each matched file.
[$<ENV>:|<Path>:]<Pattern>[...]	Specifies the search pattern for the files to match. At least one pattern is required, and the pattern can include wildcard characters (***** and **?**). By default, **where** searches the current directory and the paths that are specified in the PATH environment variable. You can specify a different path to search by using the format $*ENV*:*Pattern* (where *ENV* is an existing environment variable containing one or more paths) or by using the format *Path*:*Pattern* (where *Path* is the directory path you want to search). These optional formats should not be used with the **/r** command-line option.
/?	Displays help at the command prompt.

Remarks

- If you do not specify a file name extension, the extensions listed in the PATHEXT environment variable are appended to the pattern by default.
- **Where** can run recursive searches, display file information such as date or size, and accept environment variables in place of paths on local computers.

Examples

To find all files named Test in drive C of the current computer and its subdirectories, type:

```
where /r c:\ test
```

To list all files in the Public directory, type:

```
where $public:*.*
```

To find all files named Notepad in drive C of the remote computer, Computer1, and its subdirectories, type:

```
where /r \\computer1\c notepad.*
```

Related links

- Command-Line Syntax Key

whoami

Article • 02/03/2023

Displays user, group and privileges information for the user who is currently logged on to the local system. If used without parameters, **whoami** displays the current domain and user name.

Syntax

```
whoami [/upn | /fqdn | /logonid]
whoami {[/user] [/groups] [/priv]} [/fo <Format>] [/nh]
whoami /all [/fo <Format>] [/nh]
```

Parameters

Parameter	Description
/upn	Displays the user name in user principal name (UPN) format.
/fqdn	Displays the user name in fully qualified domain name (FQDN) format.
/logonid	Displays the logon ID of the current user.
/user	Displays the current domain and user name and the security identifier (SID).
/groups	Displays the user groups to which the current user belongs.
/priv	Displays the security privileges of the current user.
/fo <Format>	Specifies the output format. Valid values include: **table** Displays output in a table. This is the default value. **list** Displays output in a list. **csv** Displays output in comma-separated value (CSV) format.
/all	Displays all information in the current access token, including the current user name, security identifiers (SID), privileges, and groups that the current user belongs to.
/nh	Specifies that the column header should not be displayed in the output. This is valid only for table and CSV formats.
/?	Displays help at the command prompt.

Examples

To display the domain and user name of the person who is currently logged on to this computer, type:

```
whoami
```

Output similar to the following appears:

```
DOMAIN1\administrator
```

To display all of the information in the current access token, type:

```
whoami /all
```

Related links

- Command-Line Syntax Key

winnt

Article • 05/03/2023

Applies to: Windows Server (All supported versions)

The winnt command is deprecated and might not be supported in future releases of Windows.

This tool is included in Windows Server 2003. For more information, see Winnt

winnt32

Article • 02/03/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Performs an installation of or upgrade to a product in Windows Server 2003. You can run **winnt32** at the command prompt on a computer running Windows 95, Windows 98, Windows Millennium edition, Windows NT, Windows 2000, Windows XP, or a product in the Windows Server 2003. If you run **winnt32** on a computer running Windows NT version 4.0, you must first apply Service Pack 5 or later.

Syntax

```
winnt32 [/checkupgradeonly] [/cmd: <CommandLine>] [/cmdcons] [/copydir:
{i386|ia64}\<FolderName>] [/copysource: <FolderName>] [/debug[<Level>]:[
<FileName>]] [/dudisable] [/duprepare: <pathName>] [/dushare: <pathName>]
[/emsport:{com1|com2|usebiossettings|off}] [/emsbaudrate: <BaudRate>] [/m:
<FolderName>]  [/makelocalsource] [/noreboot] [/s: <Sourcepath>] [/syspart:
<DriveLetter>] [/tempdrive: <DriveLetter>] [/udf: <ID>[,<UDB_File>]]
[/unattend[<Num>]:[ <AnswerFile>]]
```

Parameters

Parameter	Description
/checkupgradeonly	Checks your computer for upgrade compatibility with products in Windows Server 2003. if you use this option with **/unattend**, no user input is required. Otherwise, the results are displayed on the screen, and you can save them under the file name you specify. The default file name is **upgrade.txt** in the systemroot folder.
/cmd	Instructs setup to carry out a specific command before the final phase of setup. This occurs after your computer has restarted and after setup has collected the necessary configuration information, but before setup is complete.
<CommandLine>	Specifies the commandline to be carried out before the final phase of setup.

Parameter	Description
/cmdcons	On an x86-based computer, installs the recovery Console as a startup option. The recovery Console is a command-line interface from which you can perform tasks such as starting and stopping services and accessing the local drive (including drives formatted with NTFS). You can only use the **/cmdcons** option after setup is finished.
/copydir	creates an additional folder within the folder in which the operating system files are installed. for example, for x86 and x64-based computers, you could create a folder called *Private_drivers* within the i386 source folder for your installation, and place driver files in the folder. type **/copydir:i386***Private_drivers* to have setup copy that folder to your newly installed computer, making the new folder location **systemroot***Private_drivers*. - **i386** specifies i386 - **ia64** specifies ia64 You can use **/copydir** to create as many additional folders as you want.
<FolderName>	Specifies the folder that you created to hold modifications for your site.
/copysource	creates a temporary additional folder within the folder in which the operating system files are installed. You can use **/copysource** to create as many additional folders as you want. Unlike the folders **/copydir** creates, **/copysource** folders are deleted after Setup completes.
/debug	creates a debug log at the level specified, for example, **/debug4:Debug.log**. The default log file is **C:\ systemroot\winnt32.log**, and
<level>	Level Values and descriptions - 0: Severe Errors - 1: Errors - 2: Default level. Warnings - 3: Information - 4: detailed information for debugging Each level includes the levels below it.
/dudisable	Prevents Dynamic Update from running. Without Dynamic Update, setup runs only with the original setup files. This option will disable Dynamic Update even if you use an answer file and specify Dynamic Update options in that file.
/duprepare	Carries out preparations on an installation share so that it can be used with Dynamic Update files that you downloaded from the Windows Update Web site. This share can then be used for installing Windows XP for multiple clients.

Parameter	Description
<pathName>	Specifies full path name.
/dushare	Specifies a share on which you previously downloaded Dynamic Update files (updated files for use with Setup) from the Windows Update Web site, and on which you previously ran **/duprepare:**< *pathName*>. When run on a client, specifies that the client installation will make use of the updated files on the share specified in <pathName>.
/emsport	Enables or disables Emergency Management Services during setup and after the server operating system has been installed. With Emergency Management Services, you can remotely manage a server in emergency situations that would typically require a local keyboard, mouse, and monitor, such as when the network is unavailable or the server is not functioning properly. Emergency Management Services has specific hardware requirements, and is available only for products in Windows Server 2003. - **com1** is applicable only for x86-based computers (not Itanium architecture-based computers). - **com2**is applicable only for x86-based computers (not Itanium architecture-based computers). - Default. Uses the setting specified in the BIOS Serial Port Console Redirection (SPCR) table, or, in Itanium architecture-based systems, through the EFI console device path. If you specify **usebiossettings** and there is no SPCR table or appropriate EFI console device path, Emergency Management Serices will not be enabled. - **off** disables Emergency Management Services. You can later enable it by modifying the boot settings.
/emsbaudrate	for x86-based computers, specifies the baud rate for Emergency Management Services. (The option is not applicable for Itanium architecture-based computers.) Must be used with **/emsport:com1** or **/emsport:com2** (otherwise, **/emsbaudrate** is ignored).
<BaudRate>	Specifies baudrate of 9600, 19200, 57600, or 115200. 9600 is the default.
/m	Specifies that setup copies replacement files from an alternate location. Instructs setup to look in the alternate location first, and if files are present, to use them instead of the files from the default location.
/makelocalsource	Instructs setup to copy all installation source files to your local hard disk. Use **/makelocalsource** when installing from a cd to provide installation files when the cd is not available later in the installation.
/noreboot	Instructs setup to not restart the computer after the file copy phase of setup is completed so that you can run another command.

Parameter	Description
/s	Specifies the source location of the files for your installation. To simultaneously copy files from multiple servers, type the **/s:**<Sourcepath> option multiple times (up to a maximum of eight). If you type the option multiple times, the first server specified must be available, or setup will fail.
<Sourcepath>	Specifies full source path name.
/syspart	On an x86-based computer, specifies that you can copy setup startup files to a hard disk, mark the disk as active, and then install the disk into another computer. When you start that computer, it automatically starts with the next phase of setup. You must always use the **/tempdrive** parameter with the **/syspart** parameter. You can start **winnt32** with the **/syspart** option on an x86-based computer running Windows NT 4.0, Windows 2000, Windows XP, or a product in Windows Server 2003. If the computer is running Windows NT version 4.0, it requires Service Pack 5 or later. The computer cannot be running Windows 95, Windows 98, or Windows Millennium edition.
<DriveLetter>	Specifies the drive letter.
/tempdrive	directs setup to place temporary files on the specified partition. for a new installation, the server operating system will also be installed on the specified partition. for an upgrade, the **/tempdrive** option affects the placement of temporary files only; the operating system will be upgraded in the partition from which you run **winnt32**.
/udf	Indicates an identifier (<ID>) that setup uses to specify how a Uniqueness Database (UDB) file modifies an answer file (see the **/unattend** option). The UDB overrides values in the answer file, and the identifier determines which values in the UDB file are used. For example, **/udf:RAS_user,Our_company.udb** overrides settings specified for the RAS_user identifier in the Our_company.udb file. If no <UDB_file> is specified, setup prompts the user to insert a disk that contains the **$Unique$.udb** file.
<ID>	Indicates an identifier used to specify how a Uniqueness Database (UDB) file modifies an answer file.
<UDB_file>	Specifies a Uniqueness Database (UDB) file.
/unattend	On an x86-based computer, upgrades your previous version of Windows NT 4.0 Server (with Service Pack 5 or later) or Windows 2000 in unattended setup mode. All user settings are taken from the previous installation, so no user intervention is required during setup.

Parameter	Description
<num>	Specifies the number of seconds between the time that setup finishes copying the files and when it restarts your computer. You can use <Num> on any computer running Windows 98, Windows Millennium edition, Windows NT, Windows 2000, Windows XP, or a product in Windows Server 2003 . If the computer is running Windows NT version 4.0, it requires Service Pack 5 or later.
<AnswerFile>	Provides setup with your custom specifications
/?	Displays help at the command prompt.

Remarks

If you are deploying Windows XP on client computers, you can use the version of winnt32.exe that comes with Windows XP. Another way to deploy Windows XP is to use winnt32.msi, which works through Windows Installer, part of the IntelliMirror set of technologies. For more information about client deployments, see the Windows Server 2003 Deployment Kit, which is described in Using the Windows Deployment and Resource Kits.

On an Itanium-based computer, **winnt32** can be run from the Extensible Firmware Interface (EFI) or from Windows Server 2003 Enterprise, Windows Server 2003 R2 Enterprise, Windows Server 2003 R2 Datacenter, or Windows Server 2003 Datacenter. Also, on an Itanium architecture-based computer, **/cmdcons** and **/syspart** are not available, and options relating to upgrades are not available. for more information about hardware compatibility, see Hardware compatibility. for more detailed information about using Dynamic Update and installing multiple clients, see the Windows Server 2003 Deployment Kit, which is described in Using the Windows Deployment and Resource Kits. for information about modifying boot settings, see the Windows Deployment and Resource Kits for Windows Server 2003. For more information, see Using the Windows Deployment and Resource Kits. Using the **/unattend** command-line option to automate setup affirms that you have read and accepted the Microsoft License Agreement for Windows Server 2003. Before using this command-line option to install Windows Server 2003 on behalf of an organization other than your own, you must confirm that the end user (whether an individual, or a single entity) has received, read, and accepted the terms of the Microsoft License Agreement for that product. OEMs may not specify this key on machines being sold to end users.

Related links

- Command-Line Syntax Key

winrs

Article • 05/04/2023

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

Windows remote Management using the winrs command enables you to manage and execute programs remotely.

Syntax

```
winrs [/<parameter>[:<value>]] <command>
```

Parameters

Parameter	Description
/remote: <endpoint>	Specifies the target endpoint using a NetBIOS name or the standard connection: - <url>: [<transport>://]<target>[:<port>] if not specified, **/r:localhost** is used.
/unencrypted	Specifies that the messages to the remote shell aren't encrypted. This parameter is useful for troubleshooting or when the network traffic is already encrypted using **ipsec**, or when physical security is enforced. By default, the messages are encrypted using Kerberos or NTLM keys. This command-line option is ignored when HTTPS transport is selected.
/username: <username>	Specifies username on command line. If not specified, the tool uses Negotiate authentication or prompt for the name. If **/username** is specified, **/password** must also be specified.
/password: <password>	Specifies password on command line. If **/password** isn't specified but **/username** is, the tool prompts for the password. If **/password** is specified, **/username** must also be specified.
/timeout: <seconds>	This option is deprecated.

Parameter	Description
/directory: <path>	Specifies starting directory for remote shell. If not specified, the remote shell starts in the user's home directory defined by the environment variable **%USERPROFILE%**.
/environment: <string>= <value>	Specifies a single environment variable to be set when shell starts, which allows changing default environment for shell. Multiple occurrences of this switch must be used to specify multiple environment variables.
/noecho	Specifies that echo should be disabled. noecho may be necessary to ensure that user's answers to remote prompts aren't displayed locally. By default echo is on.
/noprofile	Specifies that the user's profile shouldn't be loaded. By default, the server attempts to load the user profile. If the remote user isn't a local administrator on the target system, then this option is required (the default results in error.)
/allowdelegate	Specifies that the user's credentials can be used to access a remote share, for example, a different machine than the target endpoint.
/compression	Turn on compression. Older installations on remote machines might not support compression. Default setting is off because older installations on remote machines might not support compression.
/usessl	Use an SSL connection when using a remote endpoint. Specifying SSL instead of the transport **https:** uses the default **WinRM** default port.
/?	Displays help at the command prompt.

Remarks

- All command-line options accept either short form or long form. For example, both **/r** and **/remote** are valid.
- To terminate the **/remote** command, the user can type **Ctrl-C** or **Ctrl-break**, which is sent to the remote shell. The second **Ctrl-C** forces termination of **winrs.exe**.
- To manage active remote shells or winrs configuration, use the WinRM tool. The URI alias to manage active shells is **shell/cmd**. The URI alias for winrs configuration is **winrm/config/winrs**.

Examples

```
```

```
winrs /r:https://contoso.com command
```

```
winrs /r:contoso.com /usessl command
```

```
winrs /r:myserver command
```

```
winrs /r:http://127.0.0.1 command
```

```
winrs /r:http://169.51.2.101:80 /unencrypted command
```

```
winrs /r:https://[::FFFF:129.144.52.38] command
```

```
winrs /r:http://[1080:0:0:0:8:800:200C:417A]:80 command
```

```
winrs /r:https://contoso.com /t:600 /u:administrator /p:$%fgh7 ipconfig
```

```
winrs /r:myserver /env:path=^%path^%;c:\tools /env:TEMP=d:\temp config.cmd
```

```
winrs /r:myserver netdom join myserver /domain:testdomain /userd:johns
/passwordd:$%fgh789
```

```
winrs /r:myserver /ad /u:administrator /p:$%fgh7 dir \\anotherserver\share
```

Related links

- Command-Line Syntax Key

winsat mem

Article • 05/04/2023

Applies to: Windows Server (All supported versions)

The `winsat mem` command tests system memory bandwidth using a process similar to the large memory-to-memory buffer copies in multimedia processing.

Syntax

CLI

```
winsat mem <parameters>
```

Parameters

Parameter	Description
`-up`	Force memory testing with only one thread. The default is to run one thread per physical CPU or core.
`-rn`	Specify that the assessment's threads should run at normal priority. The default is to run at priority 15.
`-nc`	Specify that the assessment should allocate memory and flag it as uncached. This flag means that the processor's caches is bypassed for copy operations. The default is to run in cached space.
`-do <n>`	Specify the distance in bytes, between the end of the source buffer and the beginning of the destination buffer. The default is 64 bytes. The maximum allowable destination offset is 16 MB. Specifying an invalid destination offset results in an error. Note: Zero is a valid value for `<n>`, but negative numbers aren't.
`-mint <n>`	Specify the minimum run time in seconds for the assessment. The default is 2.0. The minimum value is 1.0. The maximum value is 30.0. Note: Specifying a `-mint` value greater than the `-maxt` value when the two parameters are used in combination results in an error.

Parameter	Description
`-maxt <n>`	Specify the maximum run time in seconds for the assessment. The default is 5.0. The minimum value is 1.0. The maximum value is 30.0. If used in combination with the `-mint` parameter, the assessment will begin to do periodic statistical checks of its results after the period of time specified in `-mint`. If the statistical checks pass, then the assessment finishes before the period of time specified in `-maxt` has elapsed. If the assessment runs for the period of time specified in `-maxt` without satisfying the statistical checks, then the assessment finishes at that time and return the results it has collected.
`-buffersize <n>`	Specify the buffer size that the memory copy test should use. Twice this amount is allocated per CPU, which determines the amount of data copied from one buffer to another. The default is 16 MB. This value is rounded to the nearest 4-KB boundary. The maximum value is 32 MB. The minimum value is 4 KB. Specifying an invalid buffer size results in an error.
`-v`	Send verbose output to STDOUT, including status and progress information. Any errors are also be written to the command window.
`-xml <file name>`	Save the output of the assessment as the specified XML file. If the specified file exists, it will be overwritten.
`-idiskinfo`	Save information about physical volumes and logical disks as part of the `<SystemConfig>` section in the XML output.
`-iguid`	Create a globally unique identifier (GUID) in the XML output file.
`-note <note text>`	Add the note text to the `<note text>` section in the XML output file.
`-icn`	Include the local computer name in the XML output file.
`-eef`	Enumerate extra system information in the XML output file.

Examples

- To run the assessment for a minimum of 4 seconds and no longer than 12 seconds, using a 32-MB buffer size and saving the results in XML format to the file `memtest.xml`:

CLI

```
winsat mem -mint 4.0 -maxt 12.0 -buffersize 32MB -xml memtest.xml
```

Remarks

- Minimum requirement to use the `winsat mem` command is membership in the local Administrators group (or equivalent). `Winsat mem` must be executed from an elevated command prompt window.
- To open an elevated command prompt window, select **Start**, select **Accessories**, right-select **Command Prompt**, and select **Run as administrator**.

winsat mfmedia

Article • 02/03/2023

Measures the performance of video decoding (playback) using the Media Foundation framework.

Syntax

```
winsat mfmedia <parameters>
```

Parameters

Parameters	Description
-input <file name>	Required: Specify the file containing the video clip to be played or encoded. The file can be in any format that can be rendered by Media Foundation.
-dumpgraph	Specify that the filter graph should be saved to a GraphEdit-compatible file before the assessment starts.
-ns	Specify that the filter graph should run at the normal playback speed of the input file. By default, the filter graph runs as fast as possible, ignoring presentation times.
-play	Run the assessment in decode mode and play any supplied audio content in the file specified in **-input** using the default DirectSound device. By default, audio playback is disabled.
-nopmp	Do not make use of the Media Foundation Protected Media Pipeline (MFPMP) process during the assessment.
-pmp	Always make use of the MFPMP process during the assessment. Note: If **-pmp** or **-nopmp** is not specified, MFPMP will be used only when necessary.
-v	Send verbose output to STDOUT, including status and progress information. Any errors will also be written to the command window.
-xml <file name>	Save the output of the assessment as the specified XML file. If the specified file exists, it will be overwritten.
-idiskinfo	Save information about physical volumes and logical disks as part of the **<SystemConfig>** section in the XML output.

Parameters	Description
-iguid	Create a globally unique identifier (GUID) in the XML output file.
-note note text	Add the note text to the **<note>** section in the XML output file.
-icn	Include the local computer name in the XML output file.
-eef	Enumerate extra system information in the XML output file.

Examples

- To runs the assessment with the input file that is used during a **winsat formal** assessment, without employing the Media Foundation Protected Media Pipeline (MFPMP), on a computer where c:\windows is the location of the Windows folder.

```
winsat mfmedia -input c:\windows\performance\winsat\winsat.wmv -nopmp
```

Remarks

- Membership in the local Administrators group, or equivalent, is the minimum required to use **winsat**. The command must be executed from an elevated command prompt window.
- To open an elevated command prompt window, click **Start**, click **Accessories**, right-click **Command Prompt**, and click **Run as administrator**.

Related links

wmic

Article • 02/03/2023

Displays WMI information inside an interactive command shell.

> **ⓘ Important**
>
> The WMI command-line (WMIC) utility is deprecated as of Windows 10, version 21H1, and as of the 21H1 semi-annual channel release of Windows Server. This utility is superseded by Windows PowerShell for WMI (see **Chapter 7—Working with WMI**). This deprecation applies only to the WMI command-line (WMIC) utility; Windows Management Instrumentation (WMI) itself is not affected. Also see **Windows 10 features we're no longer developing**.

Syntax

Windows Command Prompt

```
wmic </parameter>
```

Sub-commands

The following sub-commands are available:

Sub-command	Description
class	Escapes from the default alias mode of WMIC to access classes in the WMI schema directly.
path	Escapes from the default alias mode of WMIC to access instances in the WMI schema directly.
context	Displays the current values of all global switches.
[quit | exit]	Exits the WMIC command shell.

Examples

To display the current values of all global switches, type:

Windows Command Prompt

```
wmic context
```

Output similar to the following displays:

Windows Command Prompt

```
NAMESPACE    : root\cimv2
ROLE         : root\cli
NODE(S)      : BOBENTERPRISE
IMPLEVEL     : IMPERSONATE
[AUTHORITY   : N/A]
AUTHLEVEL    : PKTPRIVACY
LOCALE       : ms_409
PRIVILEGES   : ENABLE
TRACE        : OFF
RECORD       : N/A
INTERACTIVE  : OFF
FAILFAST     : OFF
OUTPUT       : STDOUT
APPEND       : STDOUT
USER         : N/A
AGGREGATE    : ON
```

To change the language ID used by the command line to English (locale ID 409), type:

Windows Command Prompt

```
wmic /locale:ms_409
```

Related links

- Command-Line Syntax Key

wscript

Article • 05/22/2023

Applies to: Windows Server (All supported versions)

Windows Script Host provides an environment in which users can execute scripts in various languages that use various object models to perform tasks.

Syntax

```
wscript [<scriptname>] [/b] [/d] [/e:<engine>] [{/h:cscript|/h:wscript}]
[/i] [/job:<identifier>] [{/logo|/nologo}] [/s] [/t:<number>] [/x] [/?]
[<ScriptArguments>]
```

Parameters

Parameter	Description
`scriptname`	Specifies the path and file name of the script file.
`/b`	Specifies batch mode, which doesn't display alerts, scripting errors, or input prompts. The /b parameter is the opposite of **/i**.
`/d`	Starts the debugger.
`/e`	Specifies the engine that is used to run the script. This parameter lets you run scripts that use a custom file name extension. Without the /e parameter, you can only run scripts that use registered file name extensions. For example, if you try to run this command: `cscript test.admin` You receive this error message: Input Error: There's no script engine for file extension `.admin`. One advantage of using nonstandard file name extensions is that it guards against accidentally double-selecting a script and running something you didn't actually want to run. Using this extension doesn't create a permanent association between the `.admin` file name extension and VBScript. Each time you run a script that uses a `.admin` file name extension, you need to use the /e parameter.
`/h:cscript`	Registers **cscript.exe** as the default script host for running scripts.

Parameter	Description
`/h:wscript`	Registers **wscript.exe** as the default script host for running scripts. This behavior is the default when the **/h** option is omitted.
`/i`	Specifies interactive mode, which displays alerts, scripting errors, and input prompts. The /i parameter is the default and the opposite of **/b**.
`/job:\<identifier>`	Runs the job identified by *identifier* in a **.wsf** script file.
`/logo`	Specifies that the Windows Script Host banner is displayed in the console before the script runs. The /logo parameter is the default and the opposite of **/nologo**.
`/nologo`	Specifies that the Windows Script Host banner isn't displayed before the script runs. The /nologo parameter is the opposite of **/logo**.
`/s`	Saves the current command prompt options for the current user.
`/t:\<number>`	Specifies the maximum time the script can run (in seconds). You can specify up to 32,767 seconds. The default is no time limit.
`/x`	Starts the script in the debugger.
`ScriptArguments`	Specifies the arguments passed to the script. Each script argument must be preceded with a slash (/).
`/?`	Displays Help at the command prompt.

Remarks

- Performing this task doesn't require you to have administrative credentials. Consider performing this task as a user without administrative credentials as a security best practice.
- To open a command prompt, on the **Start** screen, type **cmd**, and then select **command prompt**.
- Each parameter is optional. However you can't specify script arguments without specifying a script. If you don't specify a script or any script arguments, **wscript.exe** displays the **Windows Script Host Settings** dialog box. Use the dialog box to set global scripting properties for all scripts that **wscript.exe** runs on the local computer.
- The **/t** parameter prevents excessive running of scripts by setting a timer. When the time exceeds the specified value, **wscript** interrupts the script engine and ends

the process.

- Windows script files usually have one of the following file name extensions: **.wsf**, **.vbs**, **.js**.
- If you double-select a script file with an extension that has no association, the **Open With** dialog box appears. Select **wscript** or **cscript**, and then select **Always use this program to open this file type**. This registers **wscript.exe** or **cscript.exe** as the default script host for files of this file type.
- You can set properties for individual scripts. For more information about Windows Script Host, see Windows Script Host overview.
- Windows Script Host can use **.wsf** script files. Each **.wsf** file can use multiple scripting engines and perform multiple jobs.

Related links

- Command-Line Syntax Key

xcopy

Article • 05/28/2024

Copies files and directories, including subdirectories.

For examples of how to use this command, see Examples.

Syntax

```
xcopy <Source> [<Destination>] [/w] [/p] [/c] [/v] [/q] [/f] [/l] [/g] [/d
[:MM-DD-YYYY]] [/u] [/i] [/s [/e]] [/t] [/k] [/r] [/h] [{/a | /m}] [/n] [/o]
[/x] [/exclude:FileName1[+[FileName2]][+[FileName3]]] [{/y | /-y}] [/z] [/b]
[/j] [/compress]
```

Parameters

Expand table

Parameter	Description
<Source>	Required. Specifies the location and names of the files you want to copy. This parameter must include either a drive or a path.
[<Destination>]	Specifies the destination of the files you want to copy. This parameter can include a drive letter and colon, a directory name, a file name, or a combination of these.
/w	Displays the following message and waits for your response before starting to copy files: **Press any key to begin copying file(s)**
/p	Prompts you to confirm whether you want to create each destination file.
/c	Ignores errors.
/v	Verifies each file as it is written to the destination file to make sure that the destination files are identical to the source files.
/q	Suppresses the display of `xcopy` messages.
/f	Displays source and destination file names while copying.

Parameter	Description
/l	Generates a list of files that are to be copied, but doesn't actively copy the files.
/g	Creates decrypted *destination* files when the destination doesn't support encryption.
/d [:MM-DD-YYYY]	Copies source files changed on or after the specified date only. If you don't include a *MM-DD-YYYY* value, `xcopy` copies all *source* files that are newer than existing *destination* files. This command-line option allows you to update files that have changed.
/u	Copies files from *source* that exist on *destination* only.
/i	If *source* is a directory or contains wildcards and *destination* doesn't exist, `xcopy` assumes *destination* specifies a directory name and creates a new directory. Then, `xcopy` copies all specified files into the new directory. By default, `xcopy` prompts you to specify whether *destination* is a file or a directory.
/s	Copies directories and subdirectories, unless they're empty. If you omit **/s**, `xcopy` works within a single directory.
/e	Copies all subdirectories, even if they're empty. Use **/e** with the **/s** and **/t** command-line options.
/t	Copies the subdirectory structure (that is, the tree) only, not files. To copy empty directories, you must include the **/e** command-line option.
/k	Copies files and retains the read-only attribute on *destination* files if present on the *source* files. By default, `xcopy` removes the read-only attribute.
/r	Copies read-only files.
/h	Copies files with hidden and system file attributes. By default, `xcopy` doesn't copy hidden or system files
/a	Copies only *source* files that have their archive file attributes set. **/a** doesn't modify the archive file attribute of the source file. For information about how to set the archive file attribute by using **attrib**, see Related links.
/m	Copies *source* files that have their archive file attributes set. Unlike **/a**, **/m** turns off archive file attributes in the files that are specified in the source. For information about how to set the archive file attribute by using **attrib**, see Related links.

Parameter	Description
/n	Creates copies by using the NTFS short file or directory names. **/n** is required when you copy files or directories from an NTFS volume to a FAT volume or when the FAT file system naming convention (that is, 8.3 characters) is required on the *destination* file system. The *destination* file system can be FAT or NTFS.
/o	Copies file ownership and discretionary access control list (DACL) information.
/x	Copies file audit settings and system access control list (SACL) information (implies **/o**).
/exclude:FileName1[+ [FileName2]][+ [FileName3]( )]	Specifies a list of files. At least one file must be specified. Each file contains search strings with each string on a separate line in the file. When any of the strings match any part of the absolute path of the file to be copied, that file is excluded from being copied. For example, specifying the string **obj** will exclude all files underneath the directory **obj** or all files with the **.obj** extension.
/y	Suppresses prompting to confirm that you want to overwrite an existing destination file.
/-y	Prompts to confirm that you want to overwrite an existing destination file.
/z	Copies over a network in restartable mode.
/b	Copies the symbolic link instead of the files. This parameter was introduced in Windows Vista®.
/j	Copies files without buffering. Recommended for very large files. This parameter was added in Windows Server 2008 R2.
/compress	Request network compression during file transfer where applicable.
/[-]sparse	Enables or disables retaining the sparse state of files during copy process. If both parameters are specified, **/-sparse** overrides **/sparse**.
/noclone	Doesn't attempt block cloning as an optimization.
/?	Displays help at the command prompt.

Remarks

- Using **/z**

  If you lose your connection during the copy phase (for example, if the server going offline severs the connection), it resumes after you reestablish the connection. **/z**

also displays the percentage of the copy operation completed for each file.

- Using **/y** in the COPYCMD environment variable.

  You can use **/y** in the COPYCMD environment variable. You can override this command by using **/-y** on the command line. By default, you're prompted to overwrite.

- Copying encrypted files

  Copying encrypted files to a volume that doesn't support EFS results in an error. Decrypt the files first or copy the files to a volume that does support EFS.

- Appending files

  To append files, specify a single file for destination, but multiple files for source (that is, by using wildcards or file1+file2+file3 format).

- Default value for *destination*

  If you omit *destination*, the `xcopy` command copies the files to the current directory.

- Specifying whether *destination* is a file or directory

  If *destination* doesn't contain an existing directory and doesn't end with a backslash (), the following message appears:

  ```
  Does <Destination> specify a file name or directory name on the
  target(F = file, D = directory)?
  ```

  Press F if you want the file or files to be copied to a file. Press D if you want the file or files to be copied to a directory.

  You can suppress this message by using the **/i** command-line option, which causes `xcopy` to assume that the destination is a directory if the source is more than one file or a directory.

- Using the `xcopy` command to set archive attribute for *destination* files

  The `xcopy` command creates files with the archive attribute set, whether or not this attribute was set in the source file. For more information about file attributes and **attrib**, see Related links.

- Comparing `xcopy` and `diskcopy`

  If you have a disk that contains files in subdirectories and you want to copy it to a disk that has a different format, use the `xcopy` command instead of `diskcopy`. Because the `diskcopy` command copies disks track by track, your source and destination disks must have the same format. The `xcopy` command doesn't have this requirement. Use `xcopy` unless you need a complete disk image copy.

- Insufficient memory error

  An "insufficient memory" error may occur if running `xcopy` to copy a file or folder whose filename path is greater than 255 characters.

- Exit codes for `xcopy`

  To process exit codes returned by `xcopy`, use the **ErrorLevel** parameter on the **if** command line in a batch program. For an example of a batch program that processes exit codes using **if**, see Related links. The following table lists each exit code and a description.

Expand table

Exit code	Description
0	Files were copied without error.
1	No files were found to copy.
2	The user pressed CTRL+C to terminate `xcopy`.
4	Initialization error occurred. There isn't enough memory or disk space, or you entered an invalid drive name or invalid syntax on the command line.
5	Disk write error occurred.

Examples

1. To copy all the files and subdirectories (including any empty subdirectories) from drive A to drive B, type:

```
xcopy a: b: /s /e
```

2. To include any system or hidden files in the previous example, add the **/h** command-line option as follows:

```
xcopy a: b: /s /e /h
```

3. To update files in the \Reports directory with the files in the \Rawdata directory that have changed since December 29, 1993, type:

```
xcopy \rawdata \reports /d:12-29-1993
```

4. To update all the files that exist in \Reports in the previous example, regardless of date, type:

```
xcopy \rawdata \reports /u
```

5. To obtain a list of the files to be copied by the previous command (that is, without actually copying the files), type:

```
xcopy \rawdata \reports /d:12-29-1993 /l > xcopy.out
```

The file xcopy.out lists every file that is to be copied.

6. To copy the \Customer directory and all subdirectories to the directory \\Public\Address on network drive H:, retain the read-only attribute, and be prompted when a new file is created on H:, type:

```
xcopy \customer h:\public\address /s /e /k /p
```

7. To issue the previous command, ensure that `xcopy` creates the \Address directory if it doesn't exist, and suppress the message that appears when you create a new directory, add the **/i** command-line option as follows:

```
xcopy \customer h:\public\address /s /e /k /p /i
```

8. You can create a batch program to perform `xcopy` operations and use the batch **if** command to process the exit code if an error occurs. For example, the following batch program uses replaceable parameters for the `xcopy` source and destination parameters:

```
@echo off
rem COPYIT.BAT transfers all files in all subdirectories of
rem the source drive or directory (%1) to the destination
rem drive or directory (%2)
xcopy %1 %2 /s /e
if errorlevel 4 goto lowmemory
if errorlevel 2 goto abort
if errorlevel 0 goto exit
:lowmemory
echo Insufficient memory to copy files or
echo invalid drive or command-line syntax.
goto exit
:abort
echo You pressed CTRL+C to end the copy operation.
goto exit
:exit
```

To use the preceding batch program to copy all files in the C:\Prgmcode directory and its subdirectories to drive B, type:

```
copyit c:\prgmcode b:
```

The command interpreter substitutes **C:\Prgmcode** for *%1* and **B:** for *%2*, then uses `xcopy` with the **/e** and **/s** command-line options. If `xcopy` encounters an error, the batch program reads the exit code and goes to the label indicated in the appropriate **IF ERRORLEVEL** statement, then displays the appropriate message and exits from the batch program.

9. This example copies all the non-empty directories, plus files with the associated file extension after the asterisk symbol.

```
xcopy .\toc*.yml ..\..\Copy-To\ /S /Y

rem Output example.
```

```
rem  .\d1\toc.yml
rem  .\d1\d12\toc.yml
rem  .\d2\toc.yml
rem  3 File(s) copied
```

In the preceding example, this particular source parameter value **.\toc*.yml** copies the same 3 files even if its two path characters **.** were removed. However, no files would be copied if the asterisk wildcard was removed from the source parameter, making it just **.\toc.yml**.

Related links

- Copy
- Move
- Dir
- Attrib
- Diskcopy
- If
- Command-Line Syntax Key