Solidifier Command Line Reference Guide
(for Application Control)
Table of Contents

PREFACE .............................................................................................................................................. 1
  ABOUT THIS GUIDE ...................................................................................................................... 1
  AUDIENCE ........................................................................................................................................ 1
  DOCUMENT ORGANIZATION .......................................................................................................... 1
  DOCUMENT CONVENTIONS .............................................................................................................. 1
  PRODUCT FEEDBACK ...................................................................................................................... 2

SOLIDIFIER BASIC COMMAND REFERENCE ............................................................................... 3
  BEGIN-UPDATE (BU) ...................................................................................................................... 3
  DISABLE ......................................................................................................................................... 3
  ENABLE .......................................................................................................................................... 4
  END-UPDATE (EU) .......................................................................................................................... 4
  HELP .............................................................................................................................................. 4
  HELP-ADVANCED ........................................................................................................................... 5
  LICENSE .......................................................................................................................................... 5
  MONITOR (MON) ........................................................................................................................... 6
  PASSWD ......................................................................................................................................... 10
  SOLIDIFY (SO) ............................................................................................................................. 10
  STATUS .......................................................................................................................................... 11
  TRUSTED ........................................................................................................................................ 13
  UNSOLIDIFY (UNSO) ..................................................................................................................... 15
  UPDATER ......................................................................................................................................... 15
  VERSION ......................................................................................................................................... 18

SOLIDIFIER ADVANCED COMMAND REFERENCE ....................................................................... 19
  ATTR .............................................................................................................................................. 19
  AUTH .............................................................................................................................................. 22
  CHECK .......................................................................................................................................... 23
  CERT .............................................................................................................................................. 24
  CONFIG ......................................................................................................................................... 24
  DIAG .............................................................................................................................................. 25
  EVENT ........................................................................................................................................... 25
  FEATURES ...................................................................................................................................... 26
  LIST-SOLIDIFIED (LS) ...................................................................................................................... 27
  LIST-UNSOLIDIFIED (LU) ............................................................................................................... 28
  LOCKDOWN ................................................................................................................................... 28
  READ-PROTECT (RP) ....................................................................................................................... 29
  RECOVER ........................................................................................................................................ 30
  WRITE-PROTECT (WP) ..................................................................................................................... 30
  WRITE-PROTECT-REG (WPR) .......................................................................................................... 31
Preface

About This Guide

The McAfee® Solidifier Command Line Reference Guide (for Application Control) describes the command-line interface commands used to provision and maintain McAfee® Solidifier application for the following product suites:

- McAfee® Application Control

Please refer McAfee® Solidifier Product Guide (for Application Control) for an overview and command usage of the Solidifier CLI.

This guide provides detailed information on each of the CLI commands.

Audience

The McAfee® Solidifier Command Line Reference Guide (for Application Control) is intended for anyone who operates Solidifier application. You are expected to have a general understanding of basic data communication concepts and some practical knowledge of Microsoft Windows and UNIX operating systems.

Document Organization

This guide has the following chapters.

- This chapter describes the objectives of this guide, its audience and organization.
- Chapter “Solidifier Basic Command Reference” describes the basic commands for configuring and controlling Solidifier.
- Chapter “Solidifier Advanced Command Reference” describes the advanced commands for configuring and controlling Solidifier.

Document Conventions

The following conventions distinguish different types of text:

- Commands and keywords are in **boldface**.
- In interactive examples, user input is in **boldface**.
- In command syntax statements
  Parameters (variables for which a specific value is to be typed) are in *italics*.
  Optional arguments are in square braces [ ].
  Alternative arguments are separated by vertical bars, and are grouped within curly braces {a | b | c }
- Names of keys on the keyboard are in square braces, such as the [Tab] key.
A control key is indicated by a caret preceding a letter: ^A means Control-A.

Note means reader take note. Notes contain helpful suggestions or references to material not covered in the guide.

Contacting Support

- World Wide Web: https://mysupport.mcafee.com/
- Phone: +1(408)988-3832
- Product Updates: https://secure.nai.com/apps/downloads/my_products/login.asp
Solidifier Basic Command Reference

**begin–update (bu)**

The `begin-update` command starts Update mode for performing software updates and installations. On issuing this command:

- If the Solidifier is currently in Enabled mode then it begins tracking all file changes.
- If the Solidifier is currently in Disabled mode then after a reboot it will start tracking all file changes.

**OS Platform**

Linux, Solaris, Windows

**Syntax**

```
sadmin begin-update [ workflow-id [ comment ]]
```

**Syntax Description**

- `sadmin begin-update [ workflow-id [ comment ]]`

  Begins the Update mode.

  You can optionally specify an identification ID `workflow-id` and a description `comment` for the current Update mode session. This information can be used for a Change Management or Trouble Ticketing System.

  If you do not provide these options, `workflow-id` is set to an automatically generated string, `AUTO_n`, where `n` is a number that is incremented each time an Update window is opened or an Updater is added.

**Command Mode**

This command is supported in Disabled mode and Enabled mode.

**disable**

The `disable` command disables the Solidifier. It changes the Solidifier’s operational mode from Enabled or Update to Disabled and is effective after the next reboot. The `status` command reflects this change of operational mode.

**OS Platform**

Linux, Solaris, Windows

**Syntax**

```
sadmin disable
```
**Command Mode**

This command is supported in Enabled mode and Update mode.

**enable**

The `enable` command enables the Solidifier. It changes the Solidifier’s operational mode from Disabled mode to Enabled mode and is effective after the next reboot. The `status` command reflects this change of operational mode.

**OS Platforms**

Linux, Solaris, Windows

**Syntax**

```
sadmin enable
```

**Command Mode**

This command is supported in Disabled mode only.

**end-update (eu)**

The `end-update` command ends the Update mode and changes the Solidifier’s operational mode from Update to Enabled thereby preventing further software updates and installations.

**OS Platform**

Linux, Solaris, Windows

**Syntax**

```
sadmin end-update
```

**Syntax Description**

```
sadmin end-update
```

Ends Update mode and moves the Solidifier to Enabled mode.

**Command Mode**

This command is supported in Update mode only.

**help**

The `help` command provides help information for basic Solidifier commands.

**Module Supported**

Change Control Module, Run-time Control Module
OS Platforms
Linux, Solaris, Windows

Syntax
sadmin help
sadmin help command

Syntax Description
sadmin help
Lists the summary description for basic Solidifier CLI commands.
sadmin help command
Lists the detailed help for command command.

Command Mode
This command can be issued in any mode.

help-advanced
The help-advanced command provides help information for advanced Solidifier commands.

OS Platforms
Linux, Solaris, Windows

Syntax
sadmin help-advanced
sadmin help-advanced command

Syntax Description
sadmin help-advanced
Lists summary description of advanced Solidifier CLI commands.
sadmin help-advanced command
Lists the detailed help for advanced command command.

Command Mode
This command can be issued in any mode.

license
The license command displays the licensing information of the product and also allows you to add the product license.

OS Platforms
Linux, Solaris, Windows
Syntax

sadmin license add licensekey
sadmin license list

Syntax Description

sadmin license add licensekey
   Adds license licensekey.

sadmin license list
   Lists the currently installed licenses.

Command Mode

The sadmin license list command can be issued in any mode. The sadmin license add command can be issued in Disabled mode only.

monitor (mon)

The monitor command helps you to display or modify the rules for monitoring changes. Network monitoring is only supported on Windows.

OS Platforms

Linux, Solaris, Windows

Syntax

sadmin monitor file [ -i ] pathname1 ... pathnameN
sadmin monitor file -e pathname1 ... pathnameN
sadmin monitor file -r pathname1 ... pathnameN
sadmin monitor reg [ -i ] registrykey1 ... registrykeyN
sadmin monitor reg -e registrykey1 ... registrykeyN
sadmin monitor reg -r registrykey1 ... registrykeyN
sadmin monitor reg -f
sadmin monitor extn [ -i ] file-extn1 ... file-extnN
sadmin monitor extn -e file-extn1 ... file-extnN
sadmin monitor extn -r file-extn1 ... file-extnN
sadmin monitor extn -f
sadmin monitor process [ -i ] processname1 ... processnameN
sadmin monitor process -e processname1 ... processnameN
sadmin monitor process -r processname1 ... processnameN
sadmin monitor process -f
sadmin monitor user -e username1 ... usernameN
sadmin monitor user -r username1 ... usernameN
sadmin monitor user -f
sadmin monitor procexec [ -i ]
   pathnamel/processname1 ... pathnamen/processnameN
   | dirnamel ... dirnameN
sadmin monitor procexec -e pathnamel/processname1 ... pathnamen/processnameN
   | dirnamel ... dirnameN
sadmin monitor procexec -r pathnamel/processname1 ... pathnamen/processnameN
   | dirnamel ... dirnameN
sadmin monitor procexec -f
sadmin monitor list
sadmin monitor flush
**Note:** The `sadmin monitor reg` sub-command is available on Windows only.

**Syntax Description**

`sadmin monitor file [ -i ] pathnamel ... pathnameN`

Adds monitoring rules for paths `pathnamel ... pathnameN`.

**Note:** The `-i` argument is optional.

`sadmin monitor file -e pathnamel ... pathnameN`

Adds monitoring rules to exclude paths `pathnamel ... pathnameN` from monitoring.

Use this command to exclude from monitoring specific paths belonging to a monitored set of paths (folders/directories or volumes).

`sadmin monitor file -r pathnamel ... pathnameN`

Deletes all monitoring rules for paths `pathnamel ... pathnameN`.

**Note:** The `-i` argument is optional.

`sadmin monitor file -f`

Deletes all monitoring rules for paths (files, folders/directories, or system volumes).

`sadmin monitor reg [ -i ] registrykeyl ... registrykeyN`

Adds monitoring rules for registry keys `registrykeyl ... registrykeyN`.

**Note:** The `-i` argument is optional.

**Note:** The `sadmin monitor reg` sub-command is available on Windows only.

`sadmin monitor reg -e registrykeyl ... registrykeyN`

Adds monitoring rules to exclude registry keys `registrykeyl ... registrykeyN` from monitoring.

Use this command to exclude from monitoring specific registry keys belonging to a monitored group of registry keys.

**Note:** The `sadmin monitor reg` sub-command is available on Windows only.

`sadmin monitor reg -r registrykeyl ... registrykeyN`

Deletes all monitoring rules for registry keys `registrykeyl ... registrykeyN`.

**Note:** The `sadmin monitor reg` sub-command is available on Windows only.

`sadmin monitor reg -f`

Deletes all registry key monitoring rules.

**Note:** The `sadmin monitor reg` sub-command is available on Windows only.
sadmin monitor extn [ -i ] file-extn1 ... file-extnN

Adds monitoring rules for all files with extensions file-extn1 ... file-extnN.

**Note:** The -i argument is optional.

sadmin monitor extn -e file-extn1 ... file-extnN

Adds monitoring rules to exclude files with extensions file-extn1 ... file-extnN from monitoring.

Use this command to exclude from monitoring files with specific file extensions belonging to a monitored group of file extensions.

sadmin monitor extn -r file-extn1 ... file-extnN

Deletes all monitoring rules for files with extensions file-extn1 ... file-extnN.

These file extension monitoring rules may have been added using the -i argument or the -e argument.

sadmin monitor extn -f

Deletes all file extension monitoring rules.

sadmin monitor process [ -i ] processname1 ... processnameN

Adds monitoring rules for processes processname1 ... processnameN.

**Note:** The -i argument is optional.

sadmin monitor process -e processname1 ... processnameN

Adds monitoring rules to exclude processes processname1 ... processnameN from monitoring.

Use this command to exclude from monitoring specific processes belonging to a monitored group of processes.

sadmin monitor process -r processname1 ... processnameN

Deletes all monitoring rules for processes processname1 ... processnameN.

These process monitoring rules may have been added using the -i argument or the -e argument.

sadmin monitor process -f

Deletes all process monitoring rules.

sadmin monitor user -e username1 ... usernameN

Adds monitoring rules to exclude users username1 ... usernameN from monitoring.

**Note:** All users are monitored by default. Thus, you can only exclude users from monitoring.

Use this command to exclude from monitoring specific users belonging to a monitored group of users.

sadmin monitor user -r username1 ... usernameN

Deletes all monitoring rules for users username1 ... usernameN.

sadmin monitor user -f

Deletes all user monitoring rules.
**sadmin monitor procexec [ -i ] dirnamel/processname1 ... dirnameN/processnameN  
| dirnamel ... dirnameN**

Adds monitoring rules for execution of the following:

- processname1 invoked from dirnamel directory … processnameN invoked from dirnameN directory
- Or, all processes invoked from dirnamel … dirnameN

The execution status of the specified processes will be monitored.

**Note:** The -i argument is optional.

**sadmin monitor procexec -e pathname1/processname1 ... pathnameN/processnameN  
| dirname1 ... dirnameN**

Adds monitoring rules to exclude execution of the following from monitoring:

- processname1 invoked from dirnamel directory … processnameN invoked from dirnameN directory
- Or, all processes invoked from dirnamel … dirnameN

Use this command to exclude from monitoring execution of specific processes belonging to a monitored group of processes.

**sadmin monitor procexec -r pathname1/processname1 ... pathnameN/processnameN  
| dirnamel ... dirnameN**

Deletes all monitoring rules for the following:

- processname1 invoked from dirnamel directory … processnameN invoked from dirnameN directory
- Or, all processes invoked from dirnamel … dirnameN

These process monitoring rules may have been added using the -i argument or the -e argument.

**sadmin monitor procexec -f**

Deletes all process execution monitoring rules.

**sadmin monitor list**

Lists all monitoring rules.

**sadmin monitor flush**

Deletes all monitoring rules.

**Usage Guidelines**

1. For monitoring over mounted network file systems, the network path can be specified with **sadmin monitor file** sub command. For example, on Windows:

   S3> sadmin monitor file -i \server\share  
   S3> sadmin monitor file -i \ipaddress\share

2. For file extension rules, the rule can be specified with or without the dot (.) character. For both cases, the rule is constructed without the dot (.) character.
Command Mode

This command can be issued in any mode.

passwd

The passwd command is used to set password for the Solidifier Command line interface.

Once the password has been set, critical sadmin commands can only be executed on verification of the password.

OS Platforms

Linux, Solaris, Windows

Syntax

sadmin passwd
sadmin passwd -d

Syntax Description

sadmin passwd

Sets the password for Solidifier CLI.

When the sadmin passwd command is executed for the first time, you are prompted for a new password and then prompted to re-enter the new password for re-confirmation. Once a password has been set, subsequent issuance of the sadmin passwd command additionally prompts for the existing password before prompting for the new password twice (for entry and confirmation).

sadmin passwd -d

Clears the password for Solidifier CLI.

Command Mode

This command can be issued in any mode.

solidify (so)

The solidify command solidifies supported files, files in a folder/directory, or files of a system volume.

OS Platforms

Linux, Solaris, Windows

Syntax (Linux, Solaris, Windows)

sadmin solidify
sadmin solidify [ -q | -v ] filename1 ... filenameN
sadmin solidify [ -q | -v ] directoryname1 ... directorynameN
sadmin solidify [ -q | -v ] volumename1 ... volumenameN
Syntax Description (Linux, Solaris, Windows)

**sadmin solidify**
Solidifies all supported files (recursively) on all supported volumes.

```bash
sadmin solidify [ -q | -v ] filename1 ... filenameN
```
Solidifies files `filename1 ... filenameN`.

If the `-q` argument is specified, only error messages are displayed. All other messages are written to the Solidifier Log. If the `-v` argument is specified, all messages are displayed as well as written to the Solidifier Log. If neither the `-q` argument nor the `-v` argument are specified, the messages are only written to the Solidifier Log.

```bash
sadmin solidify [ -q | -v ] directoryname1 ... directorynameN
```
Solidifies all supported files (recursively) under folders/directories `directoryname1 ... directorynameN`.

If the `-q` argument is specified, only error messages are displayed. All other messages are written to the Solidifier Log. If the `-v` argument is specified, all messages are displayed as well as written to the Solidifier Log. If neither the `-q` argument nor the `-v` argument are specified, the messages are only written to the Solidifier Log.

```bash
sadmin solidify [ -q | -v ] volumename1 ... volumenameN
```
Solidifies all supported files (recursively) under system volumes `volumename1 ... volumenameN`.

If the `-q` argument is specified, only error messages are displayed. All other messages are written to the Solidifier Log. If the `-v` argument is specified, all messages are displayed as well as written to the Solidifier Log. If neither the `-q` argument nor the `-v` argument are specified, the messages are only written to the Solidifier Log.

**Command Mode**

This command can be issued in any mode.

**status**

The `status` command displays the current status of the Solidifier in terms of operational mode, its connectivity status with System Controller, access status of the Local CLI, etc.

**OS Platforms**

Linux, Solaris, Windows

**Syntax**

```bash
sadmin status
sadmin status volumename
```

**Syntax Description**

**sadmin status**

Lists the Solidifier status across all supported volumes.

```bash
sadmin status volumename
```
Lists the Solidifier status for system volume *volumename*.

**Usage Details**

1. An example of output of the `sadmin status` command on the Windows platform is as follows:

   McAfee Solidifier: Enabled
   McAfee Solidifier on reboot: Enabled
   System Controller: WWW-DWKJUDHR3PN:3368
   Local CLI access: Recovered

<table>
<thead>
<tr>
<th>fstype</th>
<th>status</th>
<th>[driver status]</th>
<th>[volume]</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Solidified</td>
<td>Attached</td>
<td>C:</td>
</tr>
<tr>
<td>NTFS</td>
<td>Unsolidified</td>
<td>Attached</td>
<td>E:</td>
</tr>
<tr>
<td>NTFS</td>
<td>Solidified</td>
<td>Attached</td>
<td>S:</td>
</tr>
<tr>
<td>NTFS</td>
<td>Solidified</td>
<td>Attached</td>
<td>C:\mount1</td>
</tr>
</tbody>
</table>

   The asterisk (*) character prefix indicates the main filesystem of the primary partition (C:\ for Windows).

   The `fstype` column indicates the filesystem type for the volume as NTFS or FAT (for Windows).

   The `driver status` shows the driver status for the volume - *attached* indicates that driver is loaded for the particular volume and Solidifier is in Enable mode or *unattached* indicates that Solidifier is in Disable mode for the particular volume.

2. An example of output of the `sadmin status` command on the UNIX platforms is as follows:

   McAfee Solidifier: Enabled
   McAfee Solidifier on reboot: Enabled
   System Controller: 192.168.16.163:51827
   Local CLI access: Recovered

<table>
<thead>
<tr>
<th>fstype</th>
<th>status</th>
<th>[driver status]</th>
<th>[volume]</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Solidified</td>
<td>Attached</td>
<td>/</td>
</tr>
<tr>
<td>ext3</td>
<td>Solidified</td>
<td>Attached</td>
<td>/ext2</td>
</tr>
</tbody>
</table>

   The asterisk (*) character prefix indicates the root file system (/ for UNIX).

   The `fstype` column indicates the filesystem type for the volume.

   The `driver status` shows the driver status for the volume - *attached* indicates that driver is loaded for the particular volume and Solidifier is in Enable mode or *unattached* indicates that Solidifier is in Disable mode for the particular volume.

**Command Mode**

This command can be issued in any mode.
trusted

The **trusted** command allows execution of files located on the remote share by establishing it as a trusted volume set. Using this command, you can include, exclude, remove, list or flush trusted volumes.

**OS Platforms**

Linux, Solaris, Windows

**Syntax (Windows)**

```
sadmin trusted -i volumesetname1 ... volumesetnameN
sadmin trusted -i pathname1 ... pathnameN
sadmin trusted -e volumesetname1 ... volumesetnameN
sadmin trusted -e pathname1 ... pathnameN
sadmin trusted -r volumesetname1 ... volumesetnameN
sadmin trusted -r pathname1 ... pathnameN
sadmin trusted [-1]
sadmin trusted -f
```

**Syntax (Linux, Solaris)**

```
sadmin trusted -i pathname1 ... pathnameN
sadmin trusted -e pathname1 ... pathnameN
sadmin trusted [-1]
sadmin trusted -f
```

**Syntax Description (Windows)**

- `sadmin trusted -i volumesetname1 ... volumesetnameN`
  
  Adds trusted volume rules for volumes `volumesetname1 ... volumesetnameN` and allows execution of all files on these volumes.

- `sadmin trusted -i pathname1 ... pathnameN`
  
  Adds trusted path rules for paths `pathname1 ... pathnameN` and allows execution of all files on these paths.

- `sadmin trusted -e volumesetname1 ... volumesetnameN`
  
  Adds trusted volume rules to exclude volumes `volumesetname1 ... volumesetnameN` from the trusted volumes list.

  Use this command to exclude from the trusted volumes list those volumes belonging to a trusted group of volumes.

- `sadmin trusted -e pathname1 ... pathnameN`
  
  Adds trusted path rules to exclude paths `pathname1 ... pathnameN` from the trusted paths list.

  Use this command to exclude from the trusted paths list those paths belonging to a trusted group of paths.

- `sadmin trusted -r volumesetname1 ... volumesetnameN`
  
  Removes trusted volume rules for volumes `volumesetname1 ... volumesetnameN`.  

- `sadmin trusted -r pathname1 ... pathnameN`
  
  Removes trusted path rules for paths `pathname1 ... pathnameN`.  

These trusted volume rules may have been added using the –i argument or the –e argument.

```bash
sadmin trusted -r pathname1 ... pathnameN
```

Removes trusted path rules for paths `pathname1 ... pathnameN`.
These trusted path rules may have been added using the –i argument or the –e argument.

```bash
sadmin trusted [-l]
```
Lists all trusted volume and path rules.

**Note:** The list sub-command is optional.

```bash
sadmin trusted -f
```
Deletes all trusted volume and path rules.

### Syntax Description (Linux, Solaris)

```bash
sadmin trusted -i pathname1 ... pathnameN
```
Adds trusted path rules for paths `pathname1 ... pathnameN` and allows execution of all files on these paths.

```bash
sadmin trusted -e pathname1 ... pathnameN
```
Adds trusted path rules to exclude paths `pathname1 ... pathnameN` from the trusted path list.
Use this command to exclude from the trusted path list those paths belonging to a trusted group of paths.

```bash
sadmin trusted -r pathname1 ... pathnameN
```
Removes trusted path rules for paths `pathname1 ... pathnameN`.
These trusted path rules may have been added using the –i argument or the –e argument.

```bash
sadmin trusted [-l]
```
Lists all trusted path rules.

**Note:** The list sub-command is optional.

```bash
sadmin trusted -f
```
Deletes all trusted path rules.

### Usage Guidelines

1. The volume names `volumesetname` can be specified on the Windows platform in any of the following ways:

   - `\servername\sharename` – specific share `sharename` exported by the server `servername`
   - `\servername` - all shares exported by server `servername`
   - `\*` - all shares exported by all servers

2. The pathname `pathname` can be specified on Windows platform in the following way:

   - `C:\Windows\*\drivers`
3. The pathname *pathname* can be specified on UNIX platform in the following way:

```
/usr/local/
```

**Command Mode**

This command can be issued in any mode.

**unsolidify (unso)**

The *unsolidify* command unsolidifies solidified files.

**OS Platforms**

Linux, Solaris, Windows

**Syntax (Linux, Solaris, Windows)**

```
sadmin unsolidify filename1 ... filenameN
```

**Syntax Description (Linux, Solaris, Windows)**

```
sadmin unsolidify filename1 ... filenameN
```

Un-solidifies solidified files *filename1 … filenameN*.

**Command Mode**

This command can be issued in any mode.

**updaters**

The *updaters* command adds, deletes, lists or flushes programs in the list of authorized updaters.

**OS Platforms**

Linux, Solaris, Windows

**Syntax (Windows)**

```
sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] exename
sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] -l libraryname exename
sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] -p parent-exename exename
sadmin updaters add [ -t rule-id ] -u username
sadmin updaters add scriptname
sadmin updaters remove exename
sadmin updaters remove -l libraryname exename
sadmin updaters remove -p parent-exename exename
sadmin updaters remove -u username
sadmin updaters remove scriptname
sadmin updaters list
sadmin updaters flush
```
Syntax (Linux, Solaris)

```
sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] { binaryname | scriptname }
sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] [ -p parent-programname ] { binaryname | scriptname }
sadmin updaters remove { binaryname | scriptname }
sadmin updaters remove [ -p parent-programname ] { binaryname | scriptname }
sadmin updaters list
sadmin updaters flush
```

Syntax Description (Windows)

```
sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] exename

    Adds an updater rule for execution file `exename`.
    If the `–d` argument is specified, the child processes of execution file `exename` are not
    included in the updater rule.
    If the `–n` argument is specified, the logging is disabled.
    If the `–t` argument is specified, the tag `rule-id` will be present in the Event Log for all the
    files processed due to this updater rule.

sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] -l libraryname exename

    Adds an updater rule for execution file `exename`.
    The updater rule is applicable only when the associated library `libraryname` is also
    loaded.
    If the `–d` argument is specified, the child processes of execution file `exename` are not
    included in the updater rule.
    If the `–n` argument is specified, the logging is disabled.
    If the `–t` argument is specified, the tag `rule-id` will be present in the Event Log for all the
    files processed due to this updater rule.

sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] -p parent-exename exename

    Adds an updater rule for execution file `exename`.
    The updater is applicable only when the parent execution file `parent-exename` is also
    running.
    If the `–d` argument is specified, the child processes of execution file `exename` are not
    included in the updater rule.
    If the `–n` argument is specified, the logging is disabled.
    If the `–t` argument is specified, the tag `rule-id` will be present in the Event Log for all the
    files processed due to this updater rule.

sadmin updaters add [ -t rule-id ] -u username

    Adds an updater rule for user `username` so that all update events by the user are
    authorized.
    If the `–t` argument is specified, the tag `rule-id` will be present in the Event Log for all the
    files processed due to this updater rule.

sadmin updaters add scriptname
```
Adds an updater rule for script *scriptname* so that all update events by the scripts are authorized.

```
sadmin updaters remove exename
```
Removes the updater rule for execution file *exename*.

```
sadmin updaters remove -u username
```
Removes the updater rule for user *username*.

```
sadmin updaters remove -l libraryname exename
```
Removes the updater rule for execution file *exename* having associated library *libraryname*.

```
sadmin updaters remove -p parent-exename exename
```
Removes the updater rule for execution file *exename* having associated parent execution file *parent-exename*.

```
sadmin updaters remove scriptname
```
Removes the updater rule for script *scriptname*.

```
sadmin updaters list
```
Lists all updater rules.

```
sadmin updaters flush
```
Deletes all updater rules.

**Syntax Description (Linux, Solaris)**

```
sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] { binaryname | scriptname }
```
Adds an updater rule for execution file *binaryname* or *scriptname*.

- If the `-d` argument is specified, the child processes of execution file *binaryname* or *scriptname* are not included in the updater rule.
- If the `-n` argument is specified, the logging is disabled.
- If the `-t` argument is specified, the tag `rule-id` will be present in the Event Log for all the files processed due to this updater rule.

```
sadmin updaters add [ -d ] [ -n ] [ -t rule-id ] { -p parent-programname } { binaryname | scriptname }
```
Adds an updater rule for execution file *binaryname* or *scriptname*.

The updater is applicable only when the parent execution file *parent-programname* is also running.

- If the `-d` argument is specified, the child processes of execution file *binaryname* or *scriptname* are not included in the updater rule.
- If the `-n` argument is specified, the logging is disabled.
- If the `-t` argument is specified, the tag `rule-id` will be present in the Event Log for all the files processed due to this updater rule.

```
sadmin updaters remove { binaryname | scriptname }
```
Removes the updater rule for execution file *binaryname* or *scriptname*.

```
sadmin updaters remove [ -p parent-programname ] { binaryname | scriptname }
```
Removes the updater rule for execution file *binaryname* or *scriptname*.
Removes the updater rule for execution file *binaryname* or *scriptname* having associated parent execution file *parent-programname*.

**sadmin updaters list**

Lists all updater rules.

**sadmin updaters flush**

Deletes all updater rules.

**Usage Guidelines**

The absolute path of the executable should be specified. Either the file name alone or one or more folders/directories up the tree is specified. If 'dir\file.exe' is specified, the rule applies if and only if, 'file.exe' is in a folder/directory named 'dir'. On Windows, full path names containing the drive letter or starting with a slash character are not a valid entry for the rule names; such names are ignored. For example, if you specify ‘c:\foo\bar.exe’, the updater rule is added for \foo\bar.exe ignoring the drive letter.

**Command Mode**

This command can be issued in any mode.

**version**

The **version** command displays the version of the Solidifier installed on the system.

**OS Platforms**

Linux, Solaris, Windows

**Syntax**

sadmin version

**Command Mode**

This command can be issued in any mode.
Solidifier Advanced Command Reference

**attr**

The **attr** command is used to modify or list the Solidifier’s configuration attributes list.

The following configuration attributes are supported by the **attr** command:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Argument</th>
<th>Windows (x86)</th>
<th>Windows (x64)</th>
<th>UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>always authorized attribute</td>
<td>-a</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>bypassed from memory control attribute</td>
<td>-b</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Bypass from mp-casp</td>
<td>-c</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>bypassed from process stack randomization attribute</td>
<td>-d</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>rebase dll attribute</td>
<td>-e</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>full crawl attribute</td>
<td>-f</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>bypassed from installer detection attribute</td>
<td>-i</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Bypass from anti-debug</td>
<td>-l</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Process context file operations bypass attribute</td>
<td>-p</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Process context file operations bypass attribute (conditional)</td>
<td>-o</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>bypassed from dll relocation attribute</td>
<td>-r</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>always unauthorized attribute</td>
<td>-u</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
### Supported Configuration Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>bypassed from DEP protection attribute</td>
<td>-n</td>
</tr>
</tbody>
</table>

**Note:** You can specify one or more configuration attributes in any combination.

The second column lists the corresponding argument to be used for the attributes.

#### OS Platforms

Linux, Solaris, Windows

##### Syntax (Windows)

```
sadmin attr add [-a | -b | -d | -e | -f | -i | -p | -r | -u | -n] filename1 ... filenameN

sadmin attr add -o parent=filename2 -p filename1 (Windows only)

sadmin attr remove [-a | -b | -d | -e | -f | -i | -p | -r | -u | -n] filename1 ... filenameN

sadmin attr list [-a | -b | -d | -e | -f | -i | -p | -r | -u | -n] filename1 ... filenameN

sadmin attr flush [-a | -b | -d | -e | -f | -i | -p | -r | -u | -n]
```

##### Syntax (Linux, Solaris)

```
sadmin attr add [-a | -p | -u] filename1 ... filenameN

sadmin attr add -o parent=filename2 -p filename1

sadmin attr remove [-a | -p | -u] filename1 ... filenameN

sadmin attr list [-a | -p | -u] filename1 ... filenameN

sadmin attr flush [-a | -p | -u]
```

##### Syntax Description (Windows)

```
sadmin attr add [-a | -b | -d | -e | -f | -i | -p | -r | -u | -n] filename1 ... filenameN
```

Adds a Solidifier Configuration attribute to solidified files `filename1 ... filenameN`.

Use the attribute argument based on “Table 1: Supported Configuration Attributes”.

**Note:** You must specify the argument for at least one configuration attribute with the `sadmin attr add` command.

```
sadmin attr add -o parent=filename2 -p filename1
```

(Windows only) Adds the `-p` Solidifier Configuration attribute to solidified file `filename1` so that it can pass thru if and only if it was invoked by `filename2`.

```
sadmin attr remove [-a | -b | -d | -e | -f | -i | -p | -r | -u | -n] filename1 ... filenameN
```

Removes the Solidifier Configuration attribute set on solidified files `filename1 ... filenameN`.

Use the attribute argument based on “Table 1: Supported Configuration Attributes”.

**Note:** You need not specify any argument for configuration attributes with the `sadmin attr remove` command. When no arguments for any configuration attribute are
specified, it is assumed that arguments for all configuration attributes have been specified.

```bash
sadmin attr list [ -a | -b | -d | -e | -f | -i | -p | -r | -u | -n ]
[ filename1 ... filenameN ]
```

Lists Solidifier Configuration attributes set on solidified files `filename1 ... filenameN`.

Use the attribute argument based on “Table 1: Supported Configuration Attributes”.

If file names are not specified, the configuration attributes for all solidified files are listed.

**Note:** You need not specify any argument for configuration attributes with the `sadmin attr list` command. When no arguments for any configuration attribute are specified, it is assumed that arguments for all configuration attributes have been specified.

```bash
sadmin attr flush [ -a | -b | -d | -e | -f | -i | -p | -r | -u | -n ]
```

Removes the specified Solidifier Configuration attribute(s) from all files.

Use the attribute argument based on “Table 1: Supported Configuration Attributes”.

**Note:** When no arguments for any configuration attribute are specified with the `sadmin attr flush` command, it is assumed that arguments for all configuration attributes have been specified and hence, all Solidifier Configuration attributes from all files are removed.

**Syntax Description (Linux, Solaris)**

```bash
sadmin attr add [ -a | -p | -u ] filename1 ... filenameN
```

Adds a Solidifier Configuration attribute to solidified files `filename1 ... filenameN`.

Use the attribute argument based on “Table 1: Supported Configuration Attributes”.

**Note:** You must specify the argument for at least one configuration attribute with the `sadmin attr add` command.

```bash
sadmin attr add -o parent=filename2 -p filename1
```

Adds the `-p` Solidifier Configuration attribute to solidified file `filename1` so that it can passthru if and only if it was invoked by `filename2`.

```bash
sadmin attr remove [ -a | -p | -u ] filename1 ... filenameN
```

Removes the Solidifier Configuration attribute set on solidified files `filename1 ... filenameN`.

Use the attribute argument based on “Table 1: Supported Configuration Attributes”.

**Note:** You need not specify any argument for configuration attributes with the `sadmin attr remove` command. When no arguments for any configuration attribute are specified, it is assumed that arguments for all configuration attributes have been specified.

```bash
sadmin attr list [ -a | -p | -u ] [ filename1 ... filenameN ]
```

Lists Solidifier Configuration attributes set on solidified files `filename1 ... filenameN`.

Use the attribute argument based on “Table 1: Supported Configuration Attributes”.

---

21
If file names are not specified, the configuration attributes for all solidified files are listed.

**Note:** You need not specify any argument for configuration attributes with the `sadmin attr list` command. When no arguments for any configuration attribute are specified, it is assumed that arguments for *all* configuration attributes have been specified.

```
sadmin attr flush [ -a | -p | -u ]
```

Removes the specified Solidifier Configuration attribute(s) from all files.

Use the attribute argument based on “Table 1: Supported Configuration Attributes”.

**Note:** When no arguments for any configuration attribute are specified with the `sadmin attr flush` command, it is assumed that arguments for *all* configuration attributes have been specified and hence, all Solidifier Configuration attributes from all files are removed.

**Command Mode**

This command can be issued in any mode.

**auth**

The `auth` command is used to declare applications that are allowed to be run on your system (whitelist applications) and applications that are banned from running on your system (blacklist applications). You can declare any application (executables, installers, or batch files) as a whitelist application or a blacklist application. These applications may be locally installed or invoked applications or may be installed in or invoked from a shared drive.

**OS Platforms**

Windows

**Syntax**

```
sadmin auth -a [ -u ] -c CHECKSUM | -v VERSION
sadmin auth -b -c CHECKSUM | -v VERSION
sadmin auth -r CHECKSUM | VERSION
sadmin auth -l
sadmin auth -f
```

**Syntax Description**

```
sadmin auth -a [ -u ] -c CHECKSUM | -v VERSION
```

Declares application indicated by CHECKSUM or VERSION as an authorized application.

CHECKSUM is the SHA1 hash value of the application file. VERSION is the application version details in `Product name\Product version` format.

If the `-u` argument is specified, the application is registered as an authorized updater application.

```
sadmin auth -b -c CHECKSUM | -v VERSION
``
Declares application indicated by CHECKSUM or VERSION as a banned application.

CHECKSUM is the SHA1 hash value of the application file. VERSION is the application version details in Product name\Product version format.

```
sadmin auth -r CHECKSUM | VERSION
```

Removes the registration of application indicated by CHECKSUM or VERSION as an authorized or a banned application.

```
sadmin auth -l
```

Lists all registrations added till now.

```
sadmin auth -f
```

Removes all registrations.

### check

The `check` command checks consistency of the specified file set (solidified files) with the stored file checksum, etc. in inventory. If no file set is specified, then all supported volumes are checked for consistency.

#### OS Platforms

Linux, Solaris, Windows

#### Syntax

```
sadmin check [ -r ]
sadmin check [ -r ] filename1 ... filenameN
sadmin check [ -r ] directoryname1 ... directorynameN
sadmin check [ -r ] volumename1 ... volumenameN
```

#### Syntax Description

```
sadmin check [ -r ]
```

Checks file consistency of all solidified files in all supported volumes against the stored file information.

If the `-r` argument is specified, any inconsistencies found are also fixed.

```
sadmin check [ -r ] filename1 ... filenameN
```

Checks file consistency of solidified files `filename1 ... filenameN` against the stored file information.

If the `-r` argument is specified, any inconsistencies found are also fixed.

```
sadmin check [ -r ] directoryname1 ... directorynameN
```

Checks file consistency of all solidified files under folders/directories `directoryname1 ... directorynameN` against the stored file information.

If the `-r` argument is specified, any inconsistencies found are also fixed.

```
sadmin check [ -r ] volumename1 ... volumenameN
```

Checks file consistency of all solidified files under system volumes `volumename1 ... volumenameN` against the stored file information.
If the \texttt{--r} argument is specified, any inconsistencies found are also fixed.

**Command Mode**

This command can be issued in any mode.

**cert**

The \texttt{cert} command is used to manage certificate files for digitally-signed files. The command adds, removes, or lists certificate files to Solidifier Certificates store (the \texttt{<ss-install-dir>/Certificates} folder).

\textbf{Note}: Use the \texttt{scgetcerts.exe} utility to generate certificate files for signed installers.

**OS Platforms**

Windows

**Syntax**

\begin{verbatim}
sadmin cert add certfilename
sadmin cert remove certfilename
sadmin cert list
\end{verbatim}

**Syntax Description**

\begin{verbatim}
sadmin cert add certfilename
          Adds certificate file \texttt{certfilename} to Solidifier Certificates store.
sadmin cert remove certfilename
          Removes certificate file \texttt{certfilename} from Solidifier Certificates store.
sadmin cert list
          Lists all certificates registered in Solidifier Certificates store.
\end{verbatim}

**config**

The \texttt{config} command is used to export configuration of Solidifier installation to a file or import configuration from a file. The configuration settings are applied to current installation once the import operation completes successfully.

**OS Platforms**

Linux, Solaris, Windows

**Syntax**

\begin{verbatim}
sadmin config export filename
sadmin config import [ -a ] filename
sadmin config set NAME=VALUE
sadmin config show
\end{verbatim}

**Syntax Description**

\begin{verbatim}
sadmin config export filename
\end{verbatim}
Exports the current configuration settings to file `filename`.

```
sadmin config import [ -a ] filename
```

Imports the configuration settings of file `filename`.

Then, the existing configuration settings are overwritten by the configuration settings available in the file `filename`.

If you specify the `-a` argument, the configuration settings available in the file `filename` are appended to the existing configuration settings.

```
sadmin config set NAME=VALUE
```

Sets the value of the configuration setting `NAME` to `VALUE`.

```
sadmin config show
```

Lists the configuration settings.

**Command Mode**

This command can be issued in any mode.

**diag**

The `diag` command determines interoperability configuration for programs on the system.

**OS Platforms**

Windows

**Syntax**

```
sadmin diag
sadmin diag fix [ -f ]
```

**Syntax Description**

```
sadmin diag
```

Identifies candidate Auto-Updaters and provides the command syntax for authorizing such programs to perform updates when they execute.

```
sadmin diag fix [ -f ]
```

Identifies and applies candidate Auto-Updaters for authorizing such programs to perform updates when they execute.

If the `-f` argument is specified, the restricted programs are also included.

**Command Mode**

This command can be issued in Enabled mode and Update mode only.

**event**

The `event` command lets you configure the log targets (sinks) for generated change events.
OS Platforms

Linux, Solaris, Windows

Syntax

\texttt{\texttt{sadmin} \texttt{event sink}}
\texttt{\texttt{sadmin event sink} \texttt{eventname}}
\texttt{\texttt{sadmin event sink -a \{ eventname | ALL \} \{ sinkname | ALL \}}
\texttt{\texttt{sadmin event sink -r \{ eventname | ALL \} \{ sinkname | ALL \}}

\texttt{sinkname \texttt{(on Windows):= debuglog | oslog | sc | popup}}
\texttt{sinkname \texttt{(on UNIX):= debuglog | oslog | sc}}

Syntax Description

\texttt{sadmin event sink}

Lists all Solidifier events and their associated sink types.

\texttt{sadmin event sink \texttt{eventname}}

Lists the associated sink types for event \texttt{eventname}.

\texttt{sadmin event sink -a \{ eventname | ALL \} \{ sinkname | ALL \}}

Specifies that the event \texttt{eventname} should be logged in sink type \texttt{sinkname}.

You can also specify \texttt{ALL} as the event name so that the specified sink type is applicable for all events. Similarly, you can specify \texttt{ALL} as the sink type name so that the specified event is logged with all sink types. Also, you can specify \texttt{ALL} as both the event name and the sink type name so that all events are logged with all sink types.

You can also specify the command multiple times to add more than one sink type for an event.

\texttt{sadmin event sink -r \{ eventname | ALL \} \{ sinkname | ALL \}}

Removes the association of event \texttt{eventname} with sink type \texttt{sinkname} so that event \texttt{eventname} is no longer logged with sink type \texttt{sinkname}.

You can also specify \texttt{ALL} as the event name so that all events are disassociated from the specified sink type. Similarly, you can specify \texttt{ALL} as the sink type name so that the specified event is disassociated from all sink types.

\textbf{Note}: While you can specify \texttt{ALL} as both the event name and the sink type name so that all event-sink associations are removed, it is not a recommended use model.

You can also specify the command multiple times to disassociate more than one user-specified sink type for an event.

Command Mode

This command can be issued in any mode.

features

The \texttt{features} command can be used to enable or disable a feature. A complete listing of the features along with their operational state can also be obtained using this command.
OS Platform

Linux, Solaris, Windows

Syntax

```
sadmin features enable featurename
sadmin features disable featurename
sadmin features [ list ]
```

Syntax Description

```
sadmin features enable featurename
   Adds feature featurename to the allowed features list.

sadmin features disable featurename
   Removes feature featurename from the allowed features list.

sadmin features [ list ]
   Lists all Solidifier features and their current status (allowed or not allowed).
   
   **Note:** The list argument is optional.
```

Command Mode

This command can be issued in any mode.

**list-solidified (ls)**

The list-solidified command displays the list of solidified files, folders/directories, or volumes (Windows only).

**OS Platforms**

Linux, Solaris, Windows

Syntax

```
sadmin list-solidified [ -l ]
sadmin list-solidified [ -l ] filename1 ... filenameN
sadmin list-solidified [ -l ] directoryname1 ... directorynameN
sadmin list-solidified [ -l ] volumename1 ... volumenameN
```

Syntax Description

```
sadmin list-solidified [ -l ]
   Lists all solidified files, folders/directories, and volumes.
   
   If the -l argument is specified, solidification details are also listed.

sadmin list-solidified [ -l ] filename1 ... filenameN
   Lists all solidified files out of files filename1 ... filenameN.
   
   If the -l argument is specified, solidification details are also listed.

sadmin list-solidified [ -l ] directoryname1 ... directorynameN
   Lists all solidified directories.
   
   If the -l argument is specified, solidification details are also listed.
```

...
Lists all solidified files under folders/directories `directoryname1 ... directorynameN`.

If the `-l` argument is specified, solidification details are also listed.

```
sadmin list-solidified [ -l ] volumename1 ... volumenameN
```

Lists all solidified files under volumes `volumename1 ... volumenameN`.

If the `-l` argument is specified, solidification details are also listed.

**Command Mode**

This command can be issued in any mode.

**list-unsolidified (lu)**

The `list-unsolidified` command lists unsolidified files.

**OS Platforms**

Linux, Solaris, Windows

**Syntax**

```
sadmin list-unsolidified
sadmin list-unsolidified filename1 ... filenameN
sadmin list-unsolidified directoryname1 ... directorynameN
sadmin list-unsolidified volumename1 ... volumenameN
```

**Syntax Description**

```
sadmin list-unsolidified
    Lists all unsolidified files, folders/directories, and volumes.
sadmin list-unsolidified filename1 ... filenameN
    Lists all unsolidified files out of files `filename1 ... filenameN`.
sadmin list-unsolidified directoryname1 ... directorynameN
    Lists all unsolidified files under folders/directories `directoryname1 ... directorynameN`.
sadmin list-unsolidified volumename1 ... volumenameN
    Lists all unsolidified files under volumes `volumename1 ... volumenameN`.
```

**Command Mode**

This command can be issued in any mode.

**lockdown**

The `lockdown` command disables the local CLI.

Under the lockdown, no commands (other than `help`, `help-advanced`, `status`, `version`, `lockdown`, `recover`, and `license`) can be executed.
OS Platforms
Linux, Solaris, Windows

Syntax
sadmin lockdown

Command Mode
This command can be issued in any mode.

**read-protect (rp)**

The read-protect command modifies or displays the read protection rules.

*Note:* Unlike other commands, you must specify complete file or folder/directory names with the read-protect command.

OS Platforms
Linux, Solaris, Windows

Syntax
```plaintext
sadmin read-protect [-i ] pathname1 ... pathnameN
sadmin read-protect -e pathnamel ... pathnamen
sadmin read-protect -r pathnamel ... pathnamen
sadmin read-protect -l
sadmin read-protect -f
```

Syntax Description
```plaintext
sadmin read-protect [-i ] pathname1 ... pathnamen
```
Adds read-protection rules for paths pathnamel ... pathnamen.

These paths can be simple file names, complete file names, folder/directory names, and volume names.

*Note:* The `-i` argument is optional.

```plaintext
sadmin read-protect -e pathnamel ... pathnamen
```
Adds read-protection rules to exclude paths pathnamel ... pathnamen from read-protection.

Use this command to exclude from read-protection specific paths belonging to a read-protected group of paths (folders/directories and volumes).

```plaintext
sadmin read-protect -r pathnamel ... pathnamen
```
Deletes all read-protection rules for paths pathnamel ... pathnamen.

These read-protection rules may have been added using the `-i` argument or the `-e` argument.

```plaintext
sadmin read-protect -l
```
Lists all read-protection rules.
**sadmin read-protect -f**

Removes all read-protection rules.

**Command Mode**

This command can be issued in any mode.

**recover**

The `recover` command enables a local administrator to recover the local CLI. It should be used when Solidifier-System Controller communication is down. It prompts for master password if it has been set.

**OS Platforms**

Linux, Solaris, Windows

**Syntax**

`sadmin recover`

**Command Mode**

This command can be issued in any mode.

**write-protect (wp)**

The `write-protect` command write-protects specified files including solidified files.

**Note**: Unlike other commands, you must specify complete file or folder/directory names with the `write-protect` command.

**OS Platforms**

Linux, Solaris, Windows

**Syntax**

```bash
sadmin write-protect [-i] pathname1 ... pathnameN
sadmin write-protect -e pathname1 ... pathnameN
sadmin write-protect -r pathname1 ... pathnameN
sadmin write-protect -l
sadmin write-protect -f
```

**Syntax Description**

```bash
sadmin write-protect [-i] pathname1 ... pathnameN
```

Adds write protection rules for paths `pathname1 ... pathnameN`.

These paths can be simple file names, complete file names, folder/directory names, and volume names.

**Note**: The `-i` argument is optional.
**sadmin write-protect -e pathname1 ... pathnameN**

Adds write protection rules to exclude paths `pathname1 ... pathnameN` from write protection.

Use this command to exclude from write-protection specific paths belonging to a write-protected group of paths (folders/directories and volumes).

**sadmin write-protect -r pathname1 ... pathnameN**

Deletes all write-protection rules for paths `pathname1 ... pathnameN`.

These write-protection rules may have been added using the `-i` argument or the `-e` argument.

**sadmin write-protect -l**

Lists all write-protection rules.

**sadmin write-protect -f**

Removes all write-protection rules.

**Command Mode**

This command can be issued in any mode.

**write-protect-reg (wpr)**

The `write-protect-reg` command is used to modify or display the enforcement protection rules.

**OS Platforms**

Windows

**Syntax**

```
sadmin write-protect-reg [ -i ] registrykeyname1 ... registrykeynameN
sadmin write-protect-reg -e registrykeyname1 ... registrykeynameN
sadmin write-protect-reg -r registrykeyname1 ... registrykeynameN
sadmin write-protect-reg -l
sadmin write-protect-reg -f
```

**Syntax Description**

**sadmin write-protect-reg [ -i ] registrykeyname1 ... registrykeynameN**

Includes registry keys `registrykeyname1 ... registrykeynameN` for enforcement protection.

**Note:** The `-i` argument is optional.

**sadmin write-protect-reg -e registrykeyname1 ... registrykeynameN**

Excludes registry keys `registrykeyname1 ... registrykeynameN` from enforcement protection.

Use this command to exclude from enforcement protection specific registry keys belonging to a protected group of registry keys.

**sadmin write-protect-reg -r registrykeyname1 ... registrykeynameN**
Removes the enforcement protection rules corresponding to registry keys
registrykeyname1 ... registrykeynameN.

\texttt{sadmin write-protect-reg -l}

Lists all enforcement protection rules.

\texttt{sadmin write-protect-reg -f}

Deletes all enforcement protection rules.

\textbf{Command Mode}

This command can be issued in any mode.