Solidifier Product Guide

(for Application Control)
# Table of Contents

**PREFACE** ........................................................................................................... 7  
ABOUT THIS GUIDE ................................................................................................. 7  
AUDIENCE .................................................................................................................. 7  
DOCUMENT ORGANIZATION .................................................................................... 7  
DOCUMENT CONVENTIONS ...................................................................................... 8  
CONTACTING SUPPORT ............................................................................................ 8  

**INTRODUCTION** ..................................................................................................... 9  
THE SOLIDIFIER’S COMMAND SHELL ...................................................................... 9  
HELP FOR SOLIDIFIER COMMANDS ..................................................................... 9  
LICENSEING ............................................................................................................... 10  
  Adding a license........................................................................................................ 10  
  Listing license information ..................................................................................... 10  

**CONCEPTS** .............................................................................................................. 11  
ABOUT SOLIDIFICATION ......................................................................................... 11  
ABOUT RUN TIME CONTROL .................................................................................. 11  
ABOUT SOFTWARE UPDATE ................................................................................... 12  
  The Update Mode .................................................................................................... 12  
  Auto-Updaters (Windows only) ............................................................................. 12  

**SOLIDIFICATION AND INITIAL CONFIGURATION (WINDOWS)** ....................... 13  
SOLIDIFYING A SYSTEM ......................................................................................... 13  
CONFIGURING SOLIDIFIER-CERTIFIED AUTO-UPDATERS .................................. 14  
  Enabling the Solidifier ............................................................................................ 14  
  Rebooting the system ............................................................................................. 15  
CONFIGURING UNCERTIFIED AUTO-UPDATERS .................................................. 15  
  Entering the Update Mode ...................................................................................... 15  
  Executing the normal workload ............................................................................ 15  
  Ending the Update Mode ....................................................................................... 15  
  Diagnosing the update activity ............................................................................. 16  
ABOUT THE SOLIDIFIER’S DIAGNOSIS MECHANISMS ....................................... 16  
  Auto-Updaters that generate new code ................................................................. 16  
  Auto-Updaters that modify existing code ............................................................. 17  
  Applications that stop functioning ...................................................................... 17  

**SOLIDIFICATION AND INITIAL CONFIGURATION (UNIX)** ............................... 19  
SOLIDIFYING A SYSTEM ......................................................................................... 19  
  Enabling the Solidifier ............................................................................................ 20  
  Rebooting the system ............................................................................................. 20  
  Entering the Update Mode ...................................................................................... 20  
  Executing the normal workload ............................................................................ 21  
  Ending the Update Mode ....................................................................................... 21  

**TAMPER-PROOFING CONFIGURATION** ............................................................... 22  
TAMPER-PROOFING OS, APPLICATION CONFIGURATION AND LOG FILES ........ 22  
  Enforcing write-protection ................................................................................... 23  
  Excluding write-protection ................................................................................... 24  
  Removing write-protection rule ........................................................................... 24  
  Listing write-protected files .................................................................................. 25
Removing all write-protection rules .......................................................... 25
Tamper-proofing Critical Files against Read Access .................................. 26
Enforcing read-protection ........................................................................... 26
Excluding read protection ............................................................................ 27
Restoring read access .................................................................................. 28
Listing read-protected files .......................................................................... 28
Removing read-protection rules ................................................................. 29
Tamper-proofing Critical Registry Keys (Windows only) ............................ 29
Enforcing protection on registry ................................................................... 29
Restricted Behavior ..................................................................................... 30
Excluding protection on a registry ............................................................... 30
Removing a registry from protected list ......................................................... 30
Listing protected registries .......................................................................... 31
Removing all registry protection rules ......................................................... 31
Tamper-proofing Solidifier Software and Configuration ................................... 31
Controlling Installation and Uninstallation of Software (Windows only) ....... 33
Exceptions ..................................................................................................... 34

Advanced Configuration ............................................................................ 36
Configuring Solidifier Features ................................................................... 36
Enabling a feature ......................................................................................... 36
Disabling a feature ....................................................................................... 36
Listing features ............................................................................................ 36
Configuring a Standard Event Delivery Destination .................................... 36
Assigning an event to a standard destination ............................................... 37
Removing an event from a standard destination .......................................... 37
Viewing event assignments to standard destinations ..................................... 37
Configuring the Event Cache Size ............................................................... 37
Modifying the Event Cache size ................................................................... 38
Setting the high watermark .......................................................................... 38
Setting the low watermark .......................................................................... 38
Configuring Log File Location Path (Windows) .......................................... 38
Configuring Log File Location Path (UNIX) ............................................... 39
Configuring Size of Log File ....................................................................... 39
Configuring Number of Log Files .............................................................. 39
Configuring System Controller Heartbeat Timeout ....................................... 40
Configuring Message Exchange Interval Time .......................................... 40
Configuring Execution Control for Additional Scripts (Windows) ............... 40
Executing Unsolidified Files on Local Shares ............................................. 42
Executing Files on the Remote Shares (Windows) ...................................... 43
Executing Files on the Remote Shares (UNIX) ............................................ 43
Executing files on unsupported volumes (UNIX) ........................................ 44
  On Linux platform: ...................................................................................... 44
  On Solaris platform: .................................................................................... 44
Configuring Password Protection for the CLI ............................................. 45
Setting a password ....................................................................................... 45
Deleting a password ..................................................................................... 45
Managing Mass Deployments and System Upgrades .................................. 45
Exporting Configuration Settings ................................................................ 45
Importing Configuration Settings ................................................................ 46
Configuring Proxy Address for System Controller Communications (Windows) ................................................................. 46
Routine Maintenance of a Solidified System (Windows) .............................. 47
Automated Updates ..................................................................................... 47
Adding Authorized Updaters ...................................................................... 47
Deleting Authorized Updaters ..................................................................... 48
Listing Authorized Updaters ................................................................. 49
Removing All (Flushing) Authorized Updaters ........................................ 49

MANUAL UPDATES ............................................................................. 49
Through an Update Window ................................................................. 49
Precedence of tag reporting ................................................................. 50
Through Incremental Solidification ...................................................... 51
Solidifying a File .................................................................................. 51
Solidifying a Folder ............................................................................. 51
Solidifying a Volume ........................................................................... 51
Listing Solidified Files ......................................................................... 51
Listing Unsolidified Files ..................................................................... 51
Best Practice: Check Modification Attempts on Solidified Files .......... 52

SOLIDIFIER ADMINISTRATION BY FIELD PERSONNEL ................. 52

USERS AS UPDATERS ........................................................................ 53
SCRIPTS AS UPDATERS ..................................................................... 53
APPLICATIONS IN A TRUSTED PATH AS UPDATERS ....................... 54
UPDATING APPLICATIONS IN ENABLED MODE .................................. 55

ROUTINE MAINTENANCE OF A SOLIDIFIED SYSTEM (UNIX) .......... 57

AUTOMATED UPDATES ....................................................................... 57
Adding Authorized Updaters ............................................................... 57
Deleting Authorized Updaters ............................................................. 57
Listing Authorized Updaters ............................................................... 58
Removing All (Flushing) Authorized Updaters ...................................... 58

MANUAL UPDATES ............................................................................. 58
Through an Update Window ................................................................. 58
Precedence of tag reporting ................................................................. 59
Through Incremental Solidification ...................................................... 60
Solidifying a File .................................................................................. 60
Solidifying a Folder ............................................................................. 60
Listing Solidified Files ......................................................................... 60
Listing Unsolidified Files ..................................................................... 60
Best Practice: Check Modification Attempts on Solidified Files .......... 60

APPLICATION CONTROL .................................................................. 62
ABOUT APPLICATION CONTROL ......................................................... 62
USING THE APPLICATION CONTROL FEATURE ............................... 62
DECLARE APPLICATIONS AS ALLOWED APPLICATIONS ................... 62
Declare Applications as Allowed Updater Applications ....................... 63
DECLARE APPLICATIONS AS BANNED APPLICATIONS ....................... 63
LIST ALLOWED/BANNED APPLICATIONS ........................................... 64
UNMARK APPLICATIONS ................................................................. 64

TROUBLESHOOTING ....................................................................... 65
EVENT LOG MESSAGES ...................................................................... 65
TROUBLESHOOTING MICROSOFT WINDOWS RELATED ISSUES ........ 67
OS limitation: Filter Driver Interactions .............................................. 67
Boot failures due to self-modifying drivers .......................................... 67
BOOTING IN SAFE MODE .................................................................. 67
TROUBLESHOOTING SYSTEM CRASHES (WINDOWS) ....................... 68
TROUBLESHOOTING SYSTEM CRASHES (UNIX) ............................... 70
TROUBLESHOOTING ACTIVE DIRECTORY RELATED ISSUES .......... 71
LOG FILE FOR DEBUGGING (WINDOWS) ........................................... 73
ERROR MESSAGES ........................................................................... 73
LEgITIMATE FAILURES THAT ARE NOT ERRORS ............................... 74
Only Solidified Programs Can Be Executed ......................................... 74
Attempt to execute an unsolidified .exe ................................................................. 74
Attempt to execute an unsolidified .vbs script ......................................................... 75
Attempt to execute an unsolidified file (ELF binary) .................................................. 75
Attempt to execute an unsolidified #! script ............................................................. 75

Only supported programs can be installed/uninstalled ............................................... 76
- Attempt to install a MSI based package .................................................................... 76
- Attempt to uninstall a MSI based package .................................................................. 76
- Attempt to install/uninstall Windows optional components ...................................... 76
- Attempt to install an INF based package ..................................................................... 76

Solidified Programs Cannot Be Tampered With (Windows) ........................................ 77
- Attempt to rename a solidified file ............................................................................. 77
- Attempt to move a solidified file .............................................................................. 77
- Attempt to delete a solidified file ............................................................................. 77
- Attempt to overwrite a solidified file ......................................................................... 78
- Attempt to add alternate stream for a solidified file ................................................... 78
- Attempt to delete alternate stream for a solidified file ............................................... 78
- Attempt to rename a registry key ............................................................................. 78
- Attempt to delete a registry key .............................................................................. 78

Solidified Programs Cannot Be Tampered With (UNIX) ............................................ 79
- Attempt to move a solidified file .............................................................................. 79
- Attempt to delete a solidified file ............................................................................. 79
- Attempt to overwrite a solidified file ......................................................................... 79

Vulnerabilities in Solidified Programs Cannot Be Exploited (Windows) ....................... 79

APPENDIX: COMMAND QUICK REFERENCE ................................................................. 81

APPENDIX: DIAGNOSTIC TOOLS .................................................................................. 85

SCAnalyzer ....................................................................................................................... 85
- Usage and Interpretation (Windows) .............................................................. 86
- Usage and Interpretation (UNIX) ................................................................. 86
- Manual Review of ScAnalyzer Reports (Windows) ................................................... 87

GATHERINFO ................................................................................................................. 87
- Usage and Interpretation (Windows) .............................................................. 87
- Usage and Interpretation (UNIX) ................................................................. 88

FINETUNE ......................................................................................................................... 88

APPENDIX: SECURE SIGNED UPDATES REFERENCE .................................................. 89

APPENDIX: ADVANCED CONFIGURATION PARAMETERS ........................................ 91
- Displaying Configuration parameters ......................................................................... 91
- Modifying the value of configuration parameters .................................................... 93

APPENDIX: SOLIDIFIER FEATURE LIST ....................................................................... 94
- Displaying Solidifier features .................................................................................. 94
Preface

About This Guide

The McAfee® Solidifier Product Guide (for Application Control) discusses how users can implement the Solidifier for McAfee® Application Control product suite. It describes the solidification process, the configuration of the Solidifier during the initial implementation and its ongoing maintenance. It also describes techniques for resolving problems encountered in the field. This document is meant to serve as a comprehensive reference for the initial set up and ongoing maintenance and administration of a solidified system.

Audience

The intended audience for this guide is the system administrator who will be responsible for administering the Solidifier. The system administrator is assumed to be familiar with the IT operations on systems including installation, configuration, etc. of application software and monitoring system logs. Advanced knowledge of any specific operating system or application is not required.

Document Organization

This guide is organized as follows:

Chapter, “Introduction” describes the concepts of the Solidifier.

Chapter, “Concepts” introduces solidification, runtime control and software updates.

Chapter, “Solidification and Initial Configuration” describes solidification, the process for solidifying a system, configuration changes that are necessary for allowing applications that update the system at run time to function, and some advanced configuration options.

Chapter, “Tamper-Proofing Configuration” describes the capability of enforcing control over changes.

Chapter, “Advanced Configuration” describes advanced configuration options that users may optionally choose to apply.

Chapter, “Routine Maintenance of a Solidified System” describes how the system can be updated either manually or using program automation during maintenance windows.

Chapter, “Troubleshooting” describes techniques for resolving problems encountered in the field. It also provides a reference for the event messages and common errors.

“Appendix: Command Quick Reference” provides a quick reference for the CLI commands

“Appendix: Diagnostic Tools” describes several diagnostic tools that are packaged together with the product.
“Appendix: Secure Signed Updates Reference” describes the signing utility.

“Appendix: Advanced Configuration parameters” provides a list of configuration parameters.

“Appendix: Solidifier feature list” provides the list of Solidifier features.

**Document Conventions**

The following conventions distinguish different types of text:

- Commands and keywords are in boldface.
- In interactive examples, user input is in boldface.
- CLI command syntax is preceded by the term “S3>”
- 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.
- 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 should take a note. Notes contain helpful suggestions or references to material not covered in the guide.

**Contacting Support**

- World Wide Web: [https://mysupport.mcafee.com/](https://mysupport.mcafee.com/)
- Phone: +1(408)988-3832
Introduction

IT leaders are recognizing that the largest element in the cost of information security is not the cost of security products, but the operational costs associated with security. One example of such costs is the cost of patching. Patching is an important risk-reduction mechanism. However, to comply with security policies that require implementing the most critical patches in 48 hours, and low priority patches within one week, it is often necessary for the operations staff to spend weekends at the office.

Several operational considerations arise when choosing security products to deploy on infrastructure end-points. How much effort is required in scaling up a pilot deployment of a solution to hundreds and thousands of machines in the field? Is there configuration to be done for each machine? Does it work well in geographically distributed heterogeneous environments? Another dimension of the operational problem is the amount of effort and expertise it takes to maintain the effectiveness of the solution over time, as changes happen to the environment and the image on the machine itself.

McAfee® Solidifier provides Run Time Control for solving the problem of rising operational costs of security. It employs Solidification™: a fundamentally new, persistent and deterministic approach that gives security via control, but with low operating costs. Its genesis is in the best practices that IT departments have followed for years. Operations administrators want to ensure that their systems are in a known and verified state. Solidification ensures this by guaranteeing that only authorized code can run; hence their systems in production are running only the code authorized by them.

The Solidifier's Command Shell

The Solidifier’s command interpreter, sadmin, is invoked in Solidifier’s custom command shell.

To invoke this command shell on Windows platform, double-click on the McAfee Solidifier Command Line icon on the desktop. If such an icon is not found, access it from the Start > Programs > McAfee > Solidifier > McAfee Solidifier Command Line menu option.

To invoke this command shell on UNIX platforms, open a UNIX terminal and start executing Solidifier commands on the command prompt.

Help for Solidifier Commands

Help for the basic Solidifier commands can be obtained in this command shell as follows:

> sadmin help

Help for the advanced Solidifier commands can be obtained as follows:

> sadmin help-advanced
**Licensing**

You can add another license or display licensing information of the product(s) installed on your system. Currently, there are separate licenses for enabling the Change Control and Runtime Control modules of the Solidifier.

**Adding a license**

Issue the command given below to add another license `license_key`.

```bash
> sadmin license add license_key
```

The features already installed on the system will retain the same state (enabled or disabled) after the new license has been added. These new features may require additional configuration for the Solidifier to work properly. Refer “Advanced Configuration” section for more details.

A reboot is required to activate the new features in Solidifier on Windows platform, as per the license added.

On UNIX platforms, no reboot is required to activate the new features in the Solidifier, as per the license added.

**Note:** You can add product license only when the Solidifier is running in Disabled mode.

**Listing license information**

Issue the command given below to display the list of licenses installed on your system:

```bash
> sadmin license list
```

The following listing is printed for the Change Control module license:

```
xxxx-xxxx-xxxx-xxxx-xxxx (Change Control, Unlimited)
```

The following listing is printed for the limited period Change Control module license:

```
xxxx-xxxx-xxxx-xxxx-xxxx (Change Control, 30 Day Trial)
```

In case, you also have a Runtime Control module license installed along with the Change Control module license, both licenses are printed as follows:

```
xxxx-xxxx-xxxx-xxxx-xxxx (Change Control, Unlimited)
xxxx-xxxx-xxxx-xxxx-xxxx (Runtime Control, Unlimited)
```

**Note:** The `sadmin license list` command can be issued in all modes.
Concepts

About Solidification

Solidification™ is the name for the mechanism that takes an initial snapshot of the software implemented on a system, and creates a Solidifier File Inventory (inventory) of program code, including binary executables (for example, .exe, .dll), and scripts (.bat, .cmd, .vbs) for Windows platform and binary executables (elf format), and scripts (containing #!) for supported local file systems viz. reiserfs, ext2 and ext3 for UNIX platforms.

The inventory is closed, i.e., only the fixed set of software that is allowed to run on the host computer is enumerated. The members of this inventory are called authorized or solidified program code. Solidification does not change the files that are listed in the inventory.

Note: On Windows platform, files that are open in exclusive mode at solidification time, cannot be solidified and are skipped from solidification e.g. pagefile.sys, hiberfil.sys.

About Run Time Control

The Solidifier employs solidification for enforcing the following types of control over program code in execution, or resident on the disk:

<table>
<thead>
<tr>
<th>Type of Control</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution Control</td>
<td>Only authorized code can run</td>
</tr>
<tr>
<td>Memory Control (Windows only)</td>
<td>Vulnerabilities in authorized code that is running cannot be exploited</td>
</tr>
<tr>
<td>Tamper-proofing</td>
<td>Prevent deletion, renaming, overwriting of authorized code</td>
</tr>
</tbody>
</table>

Once a system has been solidified and the Solidifier is enabled, the system is said to be in the Solidified Mode. In this mode, only programs contained in the inventory are allowed to execute. Any other programs are considered unauthorized and their execution is prevented, and their failure to execute is logged. This enforcement prevents unauthorized programs such as worms, viruses, spyware, etc., which install themselves, from executing illegitimately.

Memory Control (on Windows platform only) protects running processes from malicious attempts to hijack them. Unauthorized code injected into a running process is trapped, halted and logged. In this fashion, attempts to gain control of a system through buffer overflow and similar exploits are rendered ineffective, and logged.

Tamper-proofing prevents intentional and unintentional changes to files that are in the inventory by users or programs.
About Software Update

The Update Mode

Systems managed by IT periodically require the installation of updates to existing software. A solidified system must be placed in the Update Mode before software maintenance is performed. The Update Mode allows all update actions to be bracketed within an update window, including addition, removal or modification of software on the system. It tracks every update action (change) to automatically update the Solidifier Inventory. It ensures that only those executables that are added or modified during the Update Mode are solidified upon its completion. This enables the new or modified software to run when the system returns to normal operation. Some of the files may be changed by patches that are applied. However, as with initial solidification, the Update Mode does not change any file. It only updates the inventory to include metadata for the changed files.

Auto-Updaters (Windows only)

The Solidifier’s default configuration may have to be updated to permit Auto-Updaters, which are applications that update the system at run time, to continue to function. Typical examples are:

- Software provisioning systems that download install and run new code, e.g., Microsoft software update, Tivoli, custom scripts.
- Self updating applications, e.g., anti virus.
- Applications that create executable code at run time, e.g., anti virus, custom applications.
- Applications that write to existing system or application code on disk (binaries, DLL’s, scripts etc), e.g., backup agents, anti virus.
Solidification and Initial Configuration (Windows)

Solidifier can be installed using a standard commercial installer (based on InstallShield) or using an alternate installation kit. You interact with Solidifier using the Solidifier’s command interpreter sadmin, which provides the Command Line Interface (CLI) for administering a solidified system.

Solidifying a system

All local drives on a system are solidified using the command:

```
S3> sadmin solidify
```

or in its abbreviated form, simply,

```
S3> sadmin so
```

Alternatively, a specific volume is solidified independently. For example, the following command is used to solidify all the program files on the volume C:

```
S3> sadmin so c:
```

The duration for the solidification process can range between a few minutes to an hour, depending upon the nature of the system – its CPU speed, RAM, installed applications, etc. When solidification is complete, the following message is displayed.

```
Solidifying volume c:\
00:04:11: Total files scanned 12265, solidified 6342
```

Solidification also generates an Application log entry as shown below:

```
Local Administrator executed command 'sadmin so c:' at Thu Nov 15 2007 17:40:21 (Return status: 0).
```

You can view the list of solidified files using the following command:

```
S3> sadmin list-solidified c:
```

Or in its abbreviated form, simply,

```
S3> sadmin ls c:
```

You can view the list of unsolidified files using the following command:

```
S3> sadmin list-unsolidified c:
```

Or in its abbreviated form, simply,

```
S3> sadmin lu c:
```
Note: Since the `sadmin` command prints out a list of unsolidified files, you may find it convenient to redirect its output to a file that can be viewed after the command completes.

The Solidification Process is designed to ensure that a system in daily production use continues to function as before after it has been solidified. It consists of two distinct configuration phases, at the end of which the solidified system is ready for production use.

<table>
<thead>
<tr>
<th>Configuration Phase</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soldicore-certified Auto-Updaters</td>
<td>Update default the Solidifier configuration, to permit Commercial-Off-The-Shelf (COTS) Auto-Updaters certified by Solidifier to continue to function.</td>
</tr>
<tr>
<td>All other Auto-Updaters</td>
<td>Discover and review other Auto-Updaters. Updates the the Solidifier configuration to permit them to continue to function.</td>
</tr>
</tbody>
</table>

### Configuring Solidifier-certified Auto-Updaters

This phase involves the following activities:

- Commercial Off-The-Shelf (COTS) Auto-updater applications certified by Solidifier are added to the Solidifier Configuration
- The Solidifier is enabled

The default system configuration is updated to permit selected COTS software, typically found in a customer’s environment, as Auto-Updaters so that they can perform updates at run time. This configuration change is achieved using the `finetune` utility, which utilizes a knowledge base incorporating the applications certified by Solidifier. The utility is implemented as a batch file, named `finetune.bat`, and is available in the folder where the Solidifier software is installed. However, the default configuration of `finetune.bat` is run at the time of installation.

You can get help for the commands and options supported by `finetune` by executing it on the `sadmin` command line without providing any parameters as shown below:

```bash
> sadmin finetune.bat
```

For example, when either McAfee or ETrust or Norton Antivirus software is installed on a system, they are added as Auto-Updaters in the Solidifier’s configuration as follows:

```bash
finetune.bat add A-McAfee
finetune.bat add A-ETrust
finetune.bat add A-NAV
```

### Enabling the Solidifier

The Solidifier is enabled using the following command.

```bash
S3> sadmin enable
```

The execution of this command causes the following message to be displayed.
McAfee Solidifier will be enabled on next reboot.

The log entry is also generated as follows:

**Local Administrator executed command 'sadmin enable' at Thu Nov 15 2007 17:43:14 (Return status: 0).**

**Rebooting the system**

After the system is rebooted, the Solidifier Service is started; the system (OS plus applications) is solidified and has the following properties:

- Only solidified code can run. Any code that is created or modified at run-time, after the solidification step completes is considered unauthorized and not allowed to run.
- Authorized code cannot be tampered with. Any OS or application code cannot be deleted, renamed or otherwise updated in any fashion.
- Vulnerabilities in solidified code cannot be exploited.

**Configuring Uncertified Auto-Updaters**

**Entering the Update Mode**

The Update Mode allows a user to bracket all update actions including addition, removal or modification of software on the system. It provides a mechanism to automatically update the Solidifier Inventory and ensure that only those executables that are added or modified during the Update Mode are solidified. This enables the new or modified software to execute when the system returns to normal operation after the execution of sadmin end-update command.

**S3> sadmin begin-update**

Or in its abbreviated form, simply,

**S3> sadmin bu**

**Executing the normal workload**

The purpose of executing the normal workload is to exercise all applications and let them perform their normal tasks. During the Update Mode, all the updates performed by them are tracked and when the Update Mode ends, are recorded in a log file.

**Ending the Update Mode**

The following command ends the Update Mode:

**S3> sadmin end-update**
Diagnosing the update activity

The diagnosis for the update activity is provided by the `diag` command, which determines the configuration for the Solidifier in the presence of programs that perform updates to the system when they run.

```
S3> sadmin diag
```

The output identifies candidate Auto-Updaters and provides the command syntax for authorizing such programs to perform updates when they execute. Users are advised to review the candidate Auto-Updaters to ensure that no critical system processes or programs with generic names, e.g., setup.exe, are set as authorized updaters. The output of executing this command displays configuration rules.

- An exclamation bar (!) indicates that a configuration for the program already exists. The existing configuration is shown on the next line within square brackets.
- An asterisk (*) indicates that the configuration is for a restricted program, which may provide a user with capabilities to change the system. Hence, such programs should have restricted configuration.
- Both * and ! together indicate that the configuration of the program already exists but some modifications are required in the configuration for successful execution of the program.

You can apply the configuration changes diagnosed by executing this command as follows:

```
S3> sadmin diag fix
```

Configuration changes may need a system reboot. The `sadmin diag fix` command does not fix rules marked with *.

To apply configuration changes for restricted program, execute the following command:

```
S3> sadmin diag fix -f
```

Configuration changes may need a system reboot. The rules marked with * get fixed using the above command.

About the Solidifier’s diagnosis mechanisms

The Solidifier examines the Event Log and internal logs of changes to identify applications that are attempting to perform updates, or fail to run when they execute, as described in the following sections.

Auto-Updaters that generate new code

The Solidifier examines log messages of the following form:

```
McAfee Solidifier prevented unauthorized execution of 'E:\Documents and Settings\Administrator\Application Data\Adobe\Acrobat\7.0\Updater\Ac705Rdp_fegj.exe' by process E:\Program Files\Adobe\Acrobat 7.0\Reader\AdobeUpdateManager.exe (Process Id: 2204, User: STAGE-12\Administrator).
```
The keywords *prevented unauthorized execution* show that the application Adobe Acrobat is attempting to update Acrobat Reader by executing a new program Ac705RdP_efgj.exe. The fact that the application AdobeUpdateManager.exe can execute means that it is solidified and authorized to do so, otherwise the Solidifier would have prevented its execution. Normally, after the Solidifier is enabled, such an update would be permitted only when the Solidifier is in the Update Mode. The Solidifier suggests the following configuration change using the `diag` command:

```
S3> sadmin diag

updaters add -t "DIAG:AdobeUpdateManager.exe" "AdobeUpdateManager.exe"
```

To explicitly authorize Adobe’s Update manager to perform the update while the Solidifier is in Enabled Mode.

### Auto-Updaters that modify existing code

The Solidifier examines the log message of the following form:

```
McAfee Solidifier prevented an attempt to modify file 'C:\Program Files\Yahoo\Messenger\yupdater.exe' by process 'C:\Program Files\Symantec_Client_Security\Symantec AntiVirus\VPC32.exe' (Process Id: 2420, User: STAGE-12\Administrator).
```

The keywords *prevented an attempt to modify file* indicate that Symantec Antivirus’ run time virus scanner program VPC32.exe, attempted to modify the program yupdater.exe. This update violates the Solidifier’s tamper-proofing protection for programs and is prevented in real time. In order to permit Antivirus to function, the Solidifier suggests the following configuration change using the `diag` command:

```
S3> sadmin diag

updaters add -t "DIAG:VPC32.exe" "VPC32.exe"
```

to explicitly authorize Symantec Antivirus to perform the update while the Solidifier is in Enabled mode.

### Applications that stop functioning

The Solidifier offers very conservative memory protection techniques for preventing exploits from propagating further. There are some custom and commercial off-the-shelf applications that use non-standard mechanisms for resolving a function name to its corresponding address, e.g., manually walking the program data structures, or jumping to some hard-coded addresses where they believe the function resides, primarily to make reverse engineering difficult. This proves to be an unfortunate choice because similar techniques are also used by malicious code with the intent of exploiting vulnerabilities in legitimate applications. The Solidifier categorically prevents applications that use such non-standard means from executing because it does not heuristically distinguish between "good" and "bad". This behavior manifests itself as an application that fails to run after the Solidifier is enabled. Finetune and the Solidifier are designed to recommend configuration changes for several applications.
In the event that you encounter an application that fails to run and discover the log entry of the following form:

**McAfee Solidifier detected an attempt to exploit process** `<process-name>` **from address** `<return-addr>`.

In order to permit applications that you know are legitimate to execute, you can bypass these validation checks and permit such applications to run by suggesting the following configuration change using the **diag** command:

```
S3> sadmin attr add -b applicationname
```

Some of the Solidifier's memory protection mechanisms do not always generate log messages because they trap such exploit code and instantaneously stop the further execution of any instructions. So, while the mechanisms are deterministic, sometimes, the trade-off is that there is no log output. In a situation where a legitimate application does not work with the Solidifier enabled AND there is no log record to show why the Solidifier prevented its execution, we recommend one other test. The test involves disabling the Solidifier's memory protection and ensuring that the legitimate application works as expected. In this case, the user can bypass validation checks and permit the application to run by performing the following configuration change:

```
S3> sadmin attr add -b applicationname
```
Solidification and Initial Configuration (UNIX)

Solidifier is installed using the McAfee® Solidifier installation package. You interact with the Solidifier using the Solidifier’s command interpreter `sadmin`, which provides the Command Line Interface (CLI) for administering a solidified system.

Solidifying a system

All local drives on a system are solidified using the command:

```
# sadmin solidify
```

or in its abbreviated form, simply,

```
# sadmin so
```

The duration for the solidification process can range between a few minutes to an hour, depending upon the nature of the system – its CPU speed, RAM, installed applications, etc. When solidification is complete, the following message is displayed.

```
Solidifying volume /  
00:04:11: Total files scanned 12265, solidified 6342
```

Solidification also generates an Application log entry as shown below:

```
Local Administrator executed command 'sadmin so' at Wed Apr 23 2008 17:40:21  
(Return status: 0).
```

**Note:** To view the Event Log entry, go to the following location: `/var/log/messages`.

You can view the list of solidified files using the following command:

```
# sadmin list-solidified
```

Or in its abbreviated form, simply,

```
# sadmin ls
```

You can view the list of unsolidified files using the following command:

```
# sadmin list-unsolidified
```

Or in its abbreviated form, simply,

```
# sadmin lu
```

**Note:** Since the `sadmin lu` command prints out a list of unsolidified files, you may find it convenient to redirect its output to a file that can be viewed after the command completes.
The Solidification Process is designed to ensure that a system in daily production use continues to function as before after it has been solidified.

**Enabling the Solidifier**

The Solidifier is enabled using the following command.

```
# sadmin enable
```

The execution of this command causes the following message to be displayed.

**McAfee Solidifier will be enabled on next reboot.**

The log entry is also generated as follows:

```
Local Administrator executed command 'sadmin enable' at Wed Apr 23 2008 17:43:14 (Return status: 0).
```

**Rebooting the system**

After the system is rebooted, the Solidifier Service is started; the system (OS plus applications) is solidified and has the following properties:

- Only solidified code can run. Any code that is created or modified at run-time, after the solidification step completes is considered unauthorized and not allowed to run.
- Authorized code cannot be tampered with. Any OS or application code cannot be deleted, renamed or otherwise updated in any fashion.

**Note:** On UNIX, you can also enable the Solidifier without reboot by enabling and restarting the Solidifier service. Issue the following commands:

```
# sadmin enable
# <ss-path>/scripts/scsrvc restart
```

Here, `<ss-path>` is `<ss-install-path>/mcafee/solidcore` directory. However, reporting/filtering/protection based on path names or process names may not work as expected.

**Entering the Update Mode**

The Update Mode allows a user to bracket all update actions including addition, removal or modification of software on the system. It provides a mechanism to automatically update the Solidifier Inventory and ensure that only those executables that are added or modified during the Update Mode are solidified after its completion. This enables the new or modified software to execute when the system returns to normal operation after the execution of `sadmin end-update` command.

```
# sadmin begin-update
```

Or in its abbreviated form, simply,

```
# sadmin bu
```
Executing the normal workload

The purpose of executing the normal workload is to exercise all applications and let them perform their normal tasks. During the Update Mode, all the updates performed by them are tracked and when the Update Mode ends, are recorded in a log file.

Ending the Update Mode

Upon ending the Update Mode, the Solidifier automatically records all the changes in a private log file.

# sadmin end-update
Tamper-Proofing Configuration

This chapter introduces you to the capabilities that enforce control over changes to files and directories under the purview of the Solidifier.

Tamper-proofing OS, Application Configuration and Log Files

Critical files, directories and volumes can be write-protected using the *deny-write* feature. The write-protection rules applied on the specified files renders them as read only thereby protecting your valuable data. You can control the following operations on a write-protected file:

- Deletion
- Renaming
- Creation of hard links
- Modifying contents
- Appending
- Truncating
- Changing owner
- Creation of Alternate Data Stream (ADS) (Windows only)

When a directory or volume is specified for write-protection, all files in that directory or volume are scanned and added to write protected list. The rules are inherited by sub-directories as well. Hence, all file operations mentioned above cannot be performed on a file if it resides in a write-protected directory or volume. Creation of new files is also denied. You are not allowed to rename, move or delete the parent directory if any file or directory resident in it is write-protected.

All operations mentioned above on a write-protected file, directory or volume are considered unauthorized and are reported by Solidifier. Any unauthorized attempt is stopped and an event is generated in the Event log.

**Note:** Please restrain yourself from using this feature on the Solidifier internal files such as Solidcore.log, s3diag.log, etc.

The deny-write feature is enabled by default. For this feature to work, the Solidifier should be running in Enabled mode. You can view the operational mode of the Solidifier using ‘sadmin status’ command.

Once deny-write feature is enabled, writing data to protected files by updaters and signed binaries is allowed through one of the following mechanisms:

- The Solidifier is in Update mode
- The file has been marked as an updater
- The file has been marked as a signed binary
Enforcing write-protection

You can enforce write-protection rules on to a file, directory or volume in order to protect them from unauthorized access. You should only write protect files that are not routinely being updated by programs, e.g., log files, etc.

**Note:** The write-protected files, directories and volumes can be neither compressed nor encrypted.

The following command can be used to make non-code files, such as configuration files, log files, documents, etc. read-only by making them write protected:

```bash
> sadmin write-protect -i pathname
```

Or

```bash
> sadmin wp -i pathname
```

The pathname signifies the complete path of the file, directory or volume to be write-protected.

For instance,

```bash
S3> sadmin write-protect -i "C:\test.txt"

# sadmin write-protect -i /test.sh
```

**Note:** You can also use the wildcard ‘*’ character in the pathname which represents one complete path component, “C:\test\myfile.txt” or “/test/\test.sh”. However, the wild card * character should not be used as the last component of the rule.

The following Event Log entry is generated:

**Local Administrator executed command 'sadmin write-protect -i "C:\test.txt"' at Thu Nov 15 2007 20:30:05 (Return status: 0).**

**Local Administrator executed command 'sadmin write-protect -i /test.sh' at Fri Apr 25 2008 20:30:05 (Return status: 0).**

**Note:** The hard link to a write-protected file should also be write-protected so that it does not modify the original file.

For Windows

For enforcing write-protection rules over mounted network file systems, the network path should be specified in the sadmin wp command in any one of the following forms:

- \server-name\share-name
- \server-ip\share-name
- mapped-drive-letter:\
For instance, a server named `ftpserver` with IP as `192.168.0.1` exporting a share named `documents` and having been mapped to `W:\` on the client machine be included as shown below to prevent any writes to the share from this client machine.

- `\ftpserver\documents` or
- `\192.168.0.1\documents` or
- `W:\`

**For UNIX**

For enforcing write-protection rules over mounted network file systems, the network path should be specified in the `sadmin wp` command in the following form:

```bash
# sadmin write-protect -i /mount-point
```

For instance, you can write-protect file/directories located on a mount point.

**Excluding write-protection**

Exclusion means that the rule does not apply to the specified path used for excluding. You can exclude a particular file, directory or volume from write-protection using the following command:

```bash
> sadmin write-protect -e pathname
```

Or

```bash
> sadmin wp -e pathname
```

For instance,

```bash
S3> sadmin write-protect -e "C:\test.txt"
```

```bash
# sadmin write-protect -e /test.sh
```

The following Event Log entry is generated:

```bash
Local Administrator executed command 'sadmin write-protect -e "C:\test.txt"' at Thu Nov 15 2007 20:30:05 (Return status: 0).
Local Administrator executed command 'sadmin write-protect -e /test.sh' at Fri Apr 25 2008 20:30:05 (Return status: 0).
```

Exclusion finds special significance in scenarios where the whole directory is write-protected and you may choose to unprotect selective files in that protected directory. The applicability and usage of write-protection rules vary depending upon your specific need and requirement.

**Removing write-protection rule**

The write-protection rules applied to a file, directory or volume can be removed using the following command:

```bash
> sadmin write-protect -r pathname
```
Or

> sadmin wp -r pathname

For instance,

S3> sadmin write-protect -r "C:\test.txt"

# sadmin write-protect -r /test.sh

The following Event Log entry is generated:

Local Administrator executed command 'sadmin write-protect -r "C:\test.txt"' at Thu Nov 15 2007 20:30:05 (Return status: 0).
Local Administrator executed command 'sadmin write-protect -r /test.sh' at Fri Apr 25 2008 20:30:05 (Return status: 0).

Listing write-protected files

You can obtain a complete list of files, directories and volumes that have been write protected using the following command:

> sadmin write-protect -l

Or

> sadmin wp -l

The following Event Log entry is generated on successful execution of this command:

Local Administrator executed command 'sadmin write-protect -l' at Thu Nov 15 2007 20:30:05 (Return status: 0).

Removing all write-protection rules

All write-protection rules on files, directories and volumes are removed (flushed) using the following command:

> sadmin write-protect -f

Or

> sadmin wp -f

The following Event Log entry is generated on successful execution of this command:

Local Administrator executed command 'sadmin write-protect -f'' at Thu Nov 15 2007 20:30:05 (Return status: 0).

Issue the following command to confirm:

> sadmin wp -l

The list is empty and does not show any rules.
Tamper-proofing Critical Files against Read Access

You can read-protect critical files, directories and volumes using the *deny-read* feature. The deny-read feature enforces read-protection on specified files, directories and volumes and also denies the execution of script files. However, the execution of binaries and solidified files is outside the purview of this feature and are allowed to execute. In a nutshell, the following operations are denied:

- Reading data
- Execution of script files
- Execution of binaries

When a directory or a volume is specified for read protection, all files in that directory or volume are scanned and added to the read protected list. The rules are inherited by sub-directories as well.

**Note:** You can move a read-protected file/directory within the same drive (Windows) or same filesystem (UNIX) only.

Any unauthorized attempt made to read data from a read-protected file is stopped and an event is generated in the Event log.

The deny-read feature is disabled by default and can be enabled using the following command:

```
> sadmin features enable deny-read
```

**Note:** No reboot is required after enabling or disabling this feature.

For this feature to work, the Solidifier should be running in Enabled mode. You can view the operational mode of the Solidifier using the `sadmin status` command.

**Note:** Please restrain yourself from using this feature on the Solidifier internal files such as Solidcore.log, s3diag.log, etc.

Once deny-read feature is enabled, reading data from a read-protected file is not permitted except through one of the following mechanisms:

- The Solidifier is in Update mode.
- The file has been marked as an updater.
- The file has been marked as a signed binary. (Windows only)

**Note:** In order to provide extra protection to a read-protected file in every possible way so that its contents are not allowed to be viewed either by renaming, copying, or moving that file, you must ensure that the file is write-protected also using the deny-write feature. A file that is only read-protected (and not write-protected also) becomes readable if it is renamed or copied/moved to another location.

Enforcing read-protection

You can enforce read-protection rules on to a file, directory or volume in order to protect them from unauthorized reading attempts.
**Note:** The read-protected files, directories and volumes can be neither compressed nor encrypted.

You should issue the following command to read protect a local file;

```
> sadmin read-protect -i pathname
```

The pathname signifies the complete path of the file, directory or volume to be read-protected.

**Note:** You can also use the wildcard `*` character in the pathname which represents one complete path component, “C:\test\myfile.txt” or “/test\test.sh”. However, the wildcard * character should not be used as the last component of the rule.

For instance, to read protect a file, issue the following command:

```
S3> sadmin read-protect -i "C:\test.txt"
```

```
# sadmin read-protect -i /test.sh
```

The following Event Log entry is generated:

```
Local Administrator executed command 'read write-protect -i "C:\test.txt"' at Thu Nov 15 2007 20:30:05 (Return status: 0).
Local Administrator executed command 'sadmin read-protect -i /test.sh' at Fri Apr 25 2008 20:30:05 (Return status: 0).
```

**For Windows**

The enforcement of write-protection rules over mounted network file systems for deny read feature remain same as that of deny write. The network path should be specified in the `sadmin rp` command in any one of the following forms:

- `\Server\share`
- `\192.168.2.1\share`
- `W:\`

**For UNIX**

The enforcement of write-protection rules over mounted network file systems for deny read feature remain same as that of deny write. The network path should be specified in the `sadmin rp` command in the following form:

```
# sadmin read-protect -i /mount-point
```

For instance, you can read-protect file/directories located on a mount point.

**Excluding read protection**

Exclusion means that the rule does not apply to the specified path used for excluding. You can exclude a particular file, directory or volume from read-protection using the following command:

```
> sadmin read-protect -e pathname
```

Or
Exclusion finds special significance in scenarios where the whole directory is read-protected and you may choose to unprotect selective files in that protected directory. The applicability and usage of this rule varies depending upon your specific need and requirement.

For instance, to read unprotect a file, issue the following command:

```
S3> sadmin read-protect -e "C:\test.txt"
```

```
# sadmin read-protect -e /test.sh
```

The following Event Log entry is generated:

```
Local Administrator executed command 'read write-protect -e "C:\test.txt"' at Thu Nov 15 2007 20:30:05 (Return status: 0).
Local Administrator executed command 'sadmin read-protect -e /test.sh' at Fri Apr 25 2008 20:30:05 (Return status: 0).
```

**Restoring read access**

You can restore read access to the specified path by removing that file, directory or volume from the read-protected list using the following command:

```
> sadmin read-protect -r pathname
```

Or

```
> sadmin rp -r pathname
```

For instance, to restore read access to a file, issue the following command:

```
S3> sadmin read-protect -r "C:\test.txt"
```

```
# sadmin read-protect -r /test.sh
```

The following Event Log entry is generated:

```
Local Administrator executed command 'read write-protect -r "C:\test.txt"' at Thu Nov 15 2007 20:30:05 (Return status: 0).
Local Administrator executed command 'sadmin read-protect -r /test.sh' at Fri Apr 25 2008 20:30:05 (Return status: 0).
```

**Listing read-protected files**

You can view the list of files, directories and volumes included for read protection using the following command:

```
> sadmin read-protect -l
```

Or

```
> sadmin rp -l
```
After the successful execution of this command, the following message appears on the screen:

+ 'C:\test.txt'
+ '/test.sh'

The following Event Log entry is generated on successful execution of this command:

Local Administrator executed command 'sadmin read-protect -l'' at Thu Nov 15 2007 20:30:05 (Return status: 0).
Local Administrator executed command 'sadmin read-protect -l' at Fri Apr 25 2008 20:30:05 (Return status: 0).

Removing read-protection rules

All read-protection rules on files, directories and volumes are removed (flushed) using the following command:

> sadmin read-protect -f

Or

> sadmin rp -f

The following Event Log entry is generated on successful execution of this command:

Local Administrator executed command 'sadmin read-protect -f'' at Thu Nov 15 2007 20:30:05 (Return status: 0).

Issue the following command to confirm:

> sadmin rp -l

The list is empty and does not show any rules.

Tamper-proofing Critical Registry Keys (Windows only)

Critical registry keys can be protected against change using the *deny-write* feature. All enforcement rules to control modifications to registry keys can be applied using this feature. The write-protect-registry (wpr) command takes the registry path name as a parameter value.

Enforcing protection on registry

You should issue the following command to protect a registry file;

S3> sadmin write-protect-reg -i registryname

Or

S3> sadmin wpr -i registryname

For instance,
S3> sadmin wpr -i HKEY_LOCAL_MACHINE\Software\Yahoo\Essentials

**Note:** A wildcard character (*) is supported in pathnames with the exception that it can only represent one complete path component. For example, HKEY_LOCAL_MACHINE\*\Microsoft is allowed while HKEY_LOCAL_MACHINE\* or HKEY_LOCAL_MACHINE\*\* is not supported. The wildcard should not be used in the last path component otherwise the filter will not be effective.

This will protect the registry key from modification attempts and the following Event Log entry will be generated when a change is attempted.

**McAfee Solidifier prevented an attempt to modify Registry key 'HKEY_LOCAL_MACHINE\SOFTWARE\Yahoo\Essentials' by process C:\WINDOWS\regedit.exe (Process Id: 2240, User: MYDOMAIN\Administrator).**

An error message also appears saying that value contents cannot be edited/deleted/modified.

**Note:** New keys can be added in the registry but modification to a key is not allowed.

**Restricted Behavior**

Registry Protection is supported only for the HKEY_LOCAL_MACHINE registry key hive. For every other hive, irrespective of whether it is a top level hive or just a symbolic link, registry protection behavior is undefined.

**Warning:** The registry named HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services should not be protected.

**Excluding protection on a registry**

You can use the command given below to exclude a registry from protection rules:

S3> sadmin write-protect-reg -e registryname

Or

S3> sadmin wpr -e registryname

The Protection rules will be applied based on the longest prefix match. If you include HKEY_LOCAL_MACHINE\Software for protection but exclude HKEY_LOCAL_MACHINE\Software\Microsoft, then if any attempt is made to delete keys or values under HKEY_LOCAL_MACHINE\Software\Microsoft (e.g. HKEY_LOCAL_MACHINE\Software\Microsoft\Office), the modification will succeed.

**Removing a registry from protected list**

Remove a registry file from the protected list using the following command:

S3> sadmin write-protect-reg -r registryname

Or
S3> sadmin wpr -r registryname

Listing protected registries

You can view the list of registries included for protection using the following command:

S3> sadmin write-protect-reg -l

Or

S3> sadmin wpr -l

After the successful execution of this command, the following message appears on the screen:

+ 'HKEY_LOCAL_MACHINE\Software\Yahoo\Essentials'

Removing all registry protection rules

Remove all (Flush) the registries from the registry enforcement rules using the following command:

S3> sadmin wpr -f

Tamper-proofing Solidifier Software and Configuration

There are a class of Solidifier implementations where there are

- Very stringent security requirements, such as those for meeting audit compliance standards or Federal Defense Agencies, or,
- There is the business requirement to ensure that the Solidifier software is not overwritten to gain control over the system, such as for ATM machines and devices that flow through a multi-stage OEM channel.

The Solidifier supports the Product Integrity for tamper-proofing its software and registry key entries. When enabled, it permits the Solidifier code to run even when its components are not in the inventory. This is to ensure that the product does not become unusable from accidental or malicious un-solidification of Solidifier’s software components.

**Note:** The integrity feature fails to protect internal files when the deny-write feature is disabled.

For Windows

Product Integrity maintains the integrity of the following files:

<table>
<thead>
<tr>
<th>File</th>
<th>Control Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;installation path&gt;\Certificates</td>
<td>Tamper-proofing enabled</td>
</tr>
<tr>
<td>&lt;installation path&gt;\scinject.dll</td>
<td>Tamper-proofing enabled</td>
</tr>
<tr>
<td>&lt;installation path&gt;\scpkginj.dll</td>
<td>Tamper-proofing enabled</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>&lt;installation path&gt;\passwd</td>
<td>Tamper-proofing enabled</td>
</tr>
<tr>
<td>The passwd file stores the encrypted password using SHA-1, which is a significantly strong encryption technique. The file is protected by product integrity.</td>
<td></td>
</tr>
<tr>
<td>&lt;System32 folder&gt;\drivers\swin.sys</td>
<td>Authorized to execute unconditionally</td>
</tr>
<tr>
<td>Tamper-proofing enabled</td>
<td></td>
</tr>
<tr>
<td>All files in &lt;root volume&gt;\solidcore</td>
<td>Tamper-proofing enabled for existing files. Files added afterwards can only be modified by the Solidifier.</td>
</tr>
<tr>
<td>Note: You should also not modify any file existing in the &lt;root volume&gt;\Program Files\McAfee\Solidcore folder.</td>
<td></td>
</tr>
</tbody>
</table>

The authority to execute unconditionally implies that there is no validation check for file’s existence in the inventory. To facilitate Solidifier upgrades, product integrity is disabled in update mode even if the feature is shown as enabled.

Only the Solidifier is permitted to change the values for the following registry keys:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\swin
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\scsrvc
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application\System Solidifier

Modifications through the keys HKEY_LOCAL_MACHINE\System\ControlSetXXX are also prevented, since they are links to the HKEY_LOCAL_MACHINE\System\CurrentControlSet registry keys.

However the following, sub keys are not protected because their presence is not essential for the Solidifier’s correct functioning.

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\swin\Enum
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\scsrvc\Enum

**Note:** The authorized updaters have been provided with the capability to override Product Integrity. With Product Integrity enabled, the modifications to Solidifier-protected files and registries can be done through the updaters command and the changes are also tracked by logging events in the Event log.

**For UNIX**

Product Integrity maintains the integrity of the following files:
### Controlling Installation and Uninstallation of Software (Windows only)

The capability to control installation and uninstallation of software is called Package Control. The Package Control feature prevents installation and uninstallation of all types of installers including the ones based on MSI, Non-MSI, INF and Non-INF. The Package Control feature also enforces the following scenarios:

- All Windows optional components are blocked from installation/uninstallation.
- All INF files when right clicked give install option. Installation is blocked by this option.
- There are some INF files which can also be installed using certain exported functions from setupapi.dll or advpack.dll. These installations are also blocked.

Any unauthorized attempt to install/uninstall a package is stopped and an event is generated in the Event log.

The Solidifier currently applies multiple heuristics to detect installers. One of the techniques used among others is that the Solidifier finds the keywords like ‘install’, ‘setup’ or ‘update’ in either of following fields of the PE executable file:

- File name
- Internal file name
- Attributes and Version information of the file
- Manifest

The Package Control feature is disabled by default and can be enabled using the following command:

```
S3> sadmin features enable pkg-ctrl
```
Note: You must reboot the system after enabling or disabling this feature.

For this feature to work, the Solidifier should be running in Enabled mode. You can view the operational mode of the Solidifier using the `sadmin status` command.

Once Package Control is enabled, software cannot be installed using standard commercial installers except through one of the following mechanisms:

- The installer has been marked as an updater using the `sadmin updaters` command.
- The installation/uninstallation of the application can also be carried out in the update mode.
- The installer is marked as a signed binary.

Note: The installation/uninstallation of Windows optional components and INF based installers can be carried out only in update mode.

Exceptions

This section enumerates exceptional behaviors caused by interactions with Windows that are documented here for the reader’s benefit.

1. The following behavior is specific to some Windows optional components, particularly games. When an administrator attempts to uninstall a Windows optional component while the Package Control is in effect, the uninstallation seems to succeed. The Add or Remove Programs screen shows that the component is no longer installed. However, the component remains installed and is executable.

2. When the 'Next' or 'Cancel' button is clicked on the Windows Components Wizard window, even without making any changes to the selected components, the following error message appears:

   "McAfee Solidifier Prevented package modification by 'windows optional component manager' by user: <user_name>.

3. Some utilities like WinDriver tools (wdreg.exe) can bypass this mechanism and install/uninstall INF files.

4. Some optional Windows components can be installed using standard Windows tool like secedit and gpupdate. By default, installation/uninstallation from these tools is not prevented.

5. After installing the Fax Services from Add/Remove Programs > Add/Remove Windows Components, Fax Services gets installed but several deny write errors related to Spoolsv.exe are observed in the Event viewer. However, the Fax service works fine even with these errors. This specific case appears when rundll32.exe has been added as an updater candidate.

6. Some application executables like VNC server and client may not be able to execute when this feature is enabled. On running these applications, the following event is generated in the Event log:

   McAfee Solidifier prevented package modification by '<executable-name>' by user: <username>.

   In order to execute such applications, issue the following command:
S3> sadmin attr -i <executable-name>

This command will override this feature’s implementation on the executable.
Advanced Configuration

This section introduces advanced configuration topics:

Configuring Solidifier features

This section provides information about configuring the Solidifier features. You can choose to enable or disable a particular feature. Some of these features may require a reboot for completion.

Enabling a feature

To enable a feature, execute the following command:

> sadmin features enable featurename

The following Event Log entry is generated in the operating system logs:

Local Administrator executed command 'sadmin features enable featurename' at Thu Nov 08 2007 11:52:05 (Return status: 0).

Disabling a feature

To disable a feature, execute the following command:

> sadmin features disable featurename

The following Event Log entry is generated in the operating system logs:

Local Administrator executed command 'sadmin features disable featurename' at Thu Nov 08 2007 11:52:05 (Return status: 0).

Listing features

To view the complete listing of features along with their configured state, execute the following command:

> sadmin features list

The following Event Log entry is generated in the operating system logs:

Local Administrator executed command 'sadmin features list' at Thu Nov 08 2007 11:52:05 (Return status: 0).

Please refer Appendix C to see the complete feature list.

Configuring a Standard Event Delivery Destination

Solidifier tracks changes on the system and records events in the operating system log. Each event records the occurrence of change. The events can be logged at one or more locations called event sinks. Solidifier supports the following types of event sinks:
1. Operating system log (oslog)
2. System Controller (sc)
3. Debugging output (debuglog)
4. Popup (Windows only)

**Assigning an event to a standard destination**

To log all the events onto the System Controller, issue the following command:

```bash
> sadmin event sink -a ALL sc
```

The following Event Log entry is generated:

```
Local Administrator executed command 'sadmin event sink -a ALL sc' at Thu Nov 15 2007 14:59:35 (Return status: 0).
```

**Removing an event from a standard destination**

The following command ensures that none of the events are logged onto the System Controller.

```bash
> sadmin event sink -r ALL sc
```

The following Event Log entry is generated:

```
Local Administrator executed command 'sadmin event sink -r ALL sc' at Thu Nov 15 2007 15:01:42 (Return status: 0).
```

**Viewing event assignments to standard destinations**

To view the list of events along with their sink configuration, execute the following command:

```bash
> sadmin event sink
```

The following Event Log entry is generated:

```
Local Administrator executed command 'sadmin event sink' at Thu Nov 15 2007 15:03:11 (Return status: 0).
```

**Configuring the Event Cache Size**

The change events are buffered on the Solidifier to deal with network outrage, etc. The default event buffer size on the Solidifier is 2MB. When the buffer limits are about to be reached, then an event is logged in the system log stating that the cache is about to overflow. When the buffer limits are exceeded, then the new events are dropped until the number of events in the buffer falls below its high watermark. You can set the upper watermark level that defines the upper limit when an alert is raised that signifies that the cache is about to overflow. Likewise, setting the lower watermark level signifies that the cache has recovered from overflow.

The upper and lower watermark levels are configurable through the EventCacheWMHigh and EventCacheWMLow parameters respectively. The input value of the parameter EventCacheWMHigh should range between 50 to 100 and the input value of the parameter
EventCacheWMLow should be configured above 20 and should be less than the EventCacheWMHigh.

While configuring these parameters, ensure that the value of the lower watermark level should always be less than the value of the upper watermark level.

**Modifying the Event Cache size**

To set the event cache size to the specified value, execute the following command:

```bash
> sadmin config set EventCacheSize=<no>
```

The following Event Log entry is also generated in the operating system logs:

*Local Administrator executed command 'sadmin config set EventCacheSize=<no>' at Thu Nov 15 2007 10:41:50 (Return status: 0).*

**Setting the high watermark**

To set the upper watermark level, execute the following command:

```bash
> sadmin config set EventCacheWMHigh=<no>
```

The following Event Log entry is also generated in the operating system logs:

*Local Administrator executed command 'sadmin config set EventCacheWMHigh=<no>' at Thu Nov 15 2007 10:46:50 (Return status: 0).*

**Setting the low watermark**

To set the lower watermark level, execute the following command:

```bash
> sadmin config set EventCacheWMLow=<no>
```

The following Event Log entry is also generated in the operating system logs:

*Local Administrator executed command 'sadmin config set EventCacheWMLow=<no>' at Thu Nov 15 2007 10:50:43 (Return status: 0).*

**Configuring Log File Location Path (Windows)**

At install time, the Solidifier installer creates a log file named solidcore.log in the `<install-dir>/Logs` folder (for example, the `C:\Program Files\McAfee\Solidcore\Logs` folder). You can configure this path so that the log file gets installed at a different location other than the default one by modifying the value of the following registry key:

```plaintext
\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\swin\Parameters\LogFilePath
```

You should note that:

1. Changing this registry key to an incorrect value can adversely impact the functioning of the Solidifier.
2. The specified path must only be for the system volume.

3. The specified path should not be relocated to network shares or mapped drives.

4. The full path including the drive letter must be specified in this registry key value.

5. The Solidifier service must be restarted for the change to be applicable.

6. The GatherInfo tool collects logs from the current logfile path (mentioned in registry) as well as from the default installation location (C:\Program Files\McAfee\Solidcore\Logs).

### Configuring Log File Location Path (UNIX)

At install time, the Solidifier installer creates a log file named solidcore.log in the /var/log/mcafee/solidcore directory. You can configure this path so that the log file gets installed at a different location other than the default one by modifying the value of the parameter LogFilePath in /etc/mcafee/solidcore/solidcore.conf file.

**Note:** The solidcore.conf file cannot be modified when Solidifier is in Enabled mode and the integrity feature is enabled. To modify this file, either disable the integrity feature, or move Solidifier to Update mode, or use an authorized updater to make the required change.

You should note that:

1. The Solidifier service must be restarted for the change to be applicable.

2. The GatherInfo tool collects logs from the current logfile path (mentioned in solidcore.conf file) as well as from the default installation location (/var/log/mcafee/solidcore directory).

### Configuring Size of Log File

You can configure the size of the solidcore.log log file created by Solidifier using the LogFileSize parameter. The default size of this file is 2048 KB. When this parameter is set to 0, then the default value is applicable. Issue the command given below to configure their size:

```
> sadmin config set LogFileSize=<size>
```

**Note:** The LogFileSize parameter takes value in Kilobytes only.

The following Event Log entry is also generated in the operating system logs:

*Local Administrator executed command 'sadmin config set LogFileSize=<size>' at Mon Jan 07 2008 15:51:19 (Return status: 0).*

### Configuring Number of Log Files

You can configure the number of log files (applicable only for solidcore.log) to be created through the LogFileNum parameter. The default value of this parameter is 4 which means that at most five log files will be created starting from solidcore.log file upto solidcore.log.4. When this
parameter is set to 0, then the default value is applicable. Issue the command given below to configure the number of log files to be created:

> sadmin config set LogFileNum=<no>

The following Event Log entry is also generated in the operating system logs:

Local Administrator executed command 'sadmin config set LogFileNum=<no>' at Mon Jan 07 2008 15:51:19 (Return status: 0).

Note: The LogFileNum parameter when configured sets the number of files to be created only for the solidcore.log file.

**Configuring System Controller Heartbeat Timeout**

When the Solidifier is connected to the System Controller, a constant message exchange keeps happening between them to identify any loss in the network connectivity. The System Controller waits at most for the period specified with the HeartbeatTimeout configuration parameter before declaring a connection failure.

The default value of this parameter is 120 seconds. You can configure a value between 0 to 600 seconds. Issue the following command to configure this parameter:

> sadmin config set HeartbeatTimeout=<no>

The following Event Log entry is also generated in the operating system logs:

Local Administrator executed command 'sadmin config set HeartbeatTimeout=<no>' at Wed Jan 09 2008 11:04:00 (Return status: 0).

**Configuring Message Exchange Interval Time**

The interval for exchanging messages between System Controller and solidified hosts can be configured using the HeartbeatInterval parameter. The default value of this parameter is 2 seconds and its value can range anywhere between 0 to 600 seconds but should be less than the value set for the parameter HeartbeatTimeout. You can issue the sadmin config show command to view the value configured for the HeartbeatTimeout parameter. Issue the following command to configure the is parameter:

> sadmin config set HeartbeatInterval=<no>

The following Event Log entry is also generated in the operating system logs:

Local Administrator executed command 'sadmin config set HeartbeatInterval=<no>' at Wed Jan 09 2008 10:43:40 (Return status: 0).

**Configuring Execution Control for Additional Scripts (Windows)**

The Solidifier supports the standard script interpreters that are bundled with the Windows OS, namely, the batch files (.bat), the command interpreter (.cmd), Visual Basic (.vbs), System files (.sys) and Command files (.com) by default. However, customers may wish to explicitly enable Execution Control for other interpreters on a selective basis. The Solidifier
permits custom associations to be defined between file-extensions and the interpreters that interpret the content of such files.

\texttt{S3> sadmin scripts add extension interpreter1 [ interpreter2 ] ...}

Once this association is established, these files become supported file types and are required to be solidified. All files having that extension can only be executed by those interpreters and by none others. For example,

\texttt{S3> sadmin scripts add .vbs wscript.exe cscript.exe}

will cause the Solidifier to enforce that only \texttt{wscript.exe} and \texttt{cscript.exe} can execute any \texttt{.vbs} script. Execution control is enabled and effective immediately for all new interpreter instances that are initiated after the completion of this command. Another interpreter can be added later on to augment this list as shown below:

\texttt{S3> sadmin scripts add .vbs zscript.exe}

If a user attempts to add an interpreter that already exists on this list, then the attempt will be ignored.

There is special legacy support for 16-bit binaries. The Solidifier supports a special tag '16Bit' as a synthetic extension for such programs.

\texttt{S3> sadmin scripts add 16Bit wowexec.exe}
\texttt{S3> sadmin scripts add 16Bit ntvdm.exe}

The user can list all the interpreters for which Execution Control is enabled and in effect as shown below:

\texttt{S3> sadmin scripts list}

This command will list down the extension and the associated interpreter list.

\begin{verbatim}
.bat       "cmd.exe"
.cmd       "cmd.exe"
.sys       "ntvdm.exe"
.vbe       "cscript.exe" "wscript.exe"
16Bit      "ntvdm.exe" "wowexec.exe"
.vbs       "cscript.exe" "wscript.exe"
.com       "ntvdm.exe" "wowexec.exe"
\end{verbatim}

You may remove specific interpreters or the entire list for the extension using the following command:

\texttt{S3> sadmin scripts remove extension [ interpreter1 [ interpreter2 ] ] ...}

If an interpreter does not exist in the current list for the extension, it will be ignored. If no interpreter list is provided, the whole list for that extension shall be removed. The files having the
extension for which the rule has just been removed will stay solidified until the check command is specifically run on them.

<table>
<thead>
<tr>
<th>File extension</th>
<th>Default Interpreter/extension list</th>
</tr>
</thead>
<tbody>
<tr>
<td>.vbs</td>
<td>&quot;wscript.exe&quot; &quot;cscript.exe&quot;</td>
</tr>
<tr>
<td>.vbe</td>
<td>&quot;wscript.exe&quot; &quot;cscript.exe&quot;</td>
</tr>
<tr>
<td>.cmd</td>
<td>&quot;cmd.exe&quot;</td>
</tr>
<tr>
<td>.bat</td>
<td>&quot;cmd.exe&quot;</td>
</tr>
<tr>
<td>16Bit</td>
<td>&quot;wowexec.exe&quot; &quot;ntvdm.exe&quot;</td>
</tr>
<tr>
<td>.com</td>
<td>&quot;ntvdm.exe&quot; &quot;wowexec.exe&quot;</td>
</tr>
<tr>
<td>.sys</td>
<td>&quot;ntvdm.exe&quot;</td>
</tr>
</tbody>
</table>

**Executing Unsolidified Files on Local Shares**

You can execute an unsolidified file in local share only if its parent folder has been granted as trusted status using the `sadmin trusted` command.

**For Windows**

For example, you want to execute the unsolidified file `C:\auth\auth.exe`. Run the following commands:

```
S3> sadmin trusted -i C:\auth
```

Run the `sadmin trusted` command with `-l` argument to confirm the addition:

```
S3> sadmin trusted -l
```

The following message is generated listing the trusted rule:

```
+  C:\auth
```

Now, you execute the file as follows:

```
> C:\auth\auth.exe
```

**For UNIX**

For example, you want to execute the unsolidified file `/TEST/test.sh`. Run the following commands:

```
# sadmin trusted -i /TEST
```
Run the `sadmin trusted` command with `-l` argument to confirm the addition:

```
# sadmin trusted -l
```

The following message is generated listing the trusted rule:

```
+ /TEST
```

Now, you execute the file as follows:

```
# /TEST/test.sh
```

### Executing Files on the Remote Shares (Windows)

You can execute a file located on the network share only if the share has been granted as the trusted status. The network shares cannot be solidified but they should be trusted in order to execute files present on them. Thus, the Solidified Server A can run a remote file, for instance, `\serverB\Lotus-Startup\init.exe` located on Server B only if it has been added as a trusted share on Server A.

To execute any file on the remote share, establish the network share as a trusted share using the following command:

```
S3> sadmin trusted -i \\ServerB\Lotus-Startup\
```

Execute any file located on the remote location.

**Note:** The commands related to Network share may not run from the System Controller since the Solidifier service runs with the privileges of Local System account.

**Note:** Execution of scripts and binaries on network shares is controlled by the `network-tracking` feature. If you disable this feature,
- (32-bit): Scripts execution from network shares will still be allowed. Binaries from network shares can still be executed if the share is included in trusted volume rules.
- (64-bit): Execution of scripts and binaries from network shares will be allowed, irrespective of trusted/sa rules.

### Executing Files on the Remote Shares (UNIX)

Network shares cannot be solidified. However, they can be marked with trusted status in order to execute files present on them. Thus, Solidified Server A can run a remote file, for instance, `/mnt/ps` located on Server B only if it has been added as a trusted share on Server A.

To execute any file on the remote share, establish the network share as a trusted share using the following command:

```
# sadmin trusted -i /mnt
```

Execute any file located on the remote location.
Note: The commands related to Network share may not run from System Controller since the Solidifier service runs with the privileges of Local System account.

Executing files on unsupported volumes (UNIX)

To allow a file located on an unsupported volume (for example, a CDROM) to be executed, you need to declare the parent volume/parent directory/file as trusted (on Linux platform) and declare the parent volume as trusted (on Solaris platform).

For example, to allow the /cdrom/dir1/dir2/file file to be executed, you need to declare as follows:

On Linux platform:

```
# sadmin trusted -i /cdrom
```

(Allows any file under the /cdrom volume [including the /cdrom/dir1/dir2/file file] to be executed)

Or

```
# sadmin trusted -i /cdrom/dir1
```

(Allows any file under the /cdrom/dir1 directory [including the /cdrom/dir1/dir2/file file] to be executed)

Or

```
# sadmin trusted -i /cdrom/dir1/dir2
```

(Allows any file under the /cdrom/dir1/dir2 directory [including the /cdrom/dir1/dir2/file file] to be executed)

Or

```
# sadmin trusted -i /cdrom/dir1/dir2/file
```

(Allows the /cdrom/dir1/dir2/file file to be executed)

On Solaris platform:

```
# sadmin trusted -i /cdrom
```

(Allows any file under the /cdrom volume [including the /cdrom/dir1/dir2/file file] to be executed)

Note: Selective execution privileges for a file (as on Linux platform) are not available on Solaris platform.
Configuring Password Protection for the CLI

The password protection feature of the Solidifier restricts the usage of critical `sadmin` commands by individuals only to the `sadmin` administrator. Once the password has been set, password protection is enabled, all critical commands are password protected and can be accessed only after supplying the password.

Setting a password

Password protection is set using the following command:

```
> sadmin passwd
```

This command is used to set the password. It prompts for the old password (if password is set) and then for the confirmation of the new password twice.

Deleting a password

An existing password can be deleted using the following command:

```
> sadmin passwd -d
```

Managing Mass Deployments and System Upgrades

The Configuration Migration feature of the Solidifier provides a way to extract and store all identified configuration items in an exportable format. This exported configuration can then be imported to any other installation or to permit an upgrade of the OS, or the Solidifier software, on the same system, or on other systems where there is no variation in images.

The user can add, delete or modify the contents of an exported file and import the modified configuration file to affect new parameters. For some parameters, module specific rules are displayed. Hence, modifying such lists is not straightforward and is not recommended. Such parameters include Monitoring Rules List, Capability Rules List, Bypass List, Updaters List etc.

Exporting Configuration Settings

Export the configuration to a file using the following command:

```
> sadmin config export filename
```

Here, `filename` is the name of the file, where configuration is to be exported.

The log entry is also generated as shown:

```
Local Administrator executed command 'sadmin config export filename' at Thu Nov 15 2007 17:51:36 (Return status: 0).
```
Importing Configuration Settings

This command is usable only when the Solidifier is either in the Disabled or Update Mode. Before importing the configuration settings, check the current status of the Solidifier using the following command:

> sadmin status

If the status is not as shown below,

McAfee Solidifier: Disabled
McAfee Solidifier on reboot: Disabled

Then, disable Solidifier and reboot the system. Import the Solidifier configuration from a file that contains a previously exported configuration using the following command:

S3> sadmin config import filename

The log entry is also generated as shown:

Local Administrator executed command 'sadmin config import filename' at Thu Nov 15 2007 17:52:28 (Return status: 0).

Enable Solidifier and reboot to re-use the imported configuration.

> sadmin enable

Configuring Proxy Address for System Controller communications (Windows)

When a host is connected to System Controller, the communication with System Controller is using the default proxy settings. You can control the proxy setting using the Proxy configuration parameter. By default, the Proxy configuration parameter is set to blank.

To set your own proxy settings, use the following command:

S3> sadmin config set Proxy=<address>:<port>

Here, <address> is the IP Address of the Proxy Server and <port> is the proxy service port.

To initialize the Proxy configuration parameter, use the following command:

S3> sadmin config set Proxy=
Routine Maintenance of a Solidified System (Windows)

This chapter contains the following topics:

- **Automated Updates**
- **Manual Updates**

**Automated Updates**

The Solidifier prevents the modification of solidified executable files and also controls the unauthorized installation/uninstallation of MSI based installers without entering the update mode. The Solidifier provides the updaters command to unconditionally authorize legitimate programs to update software on a solidified system.

**Note:** A reboot is not required after adding MSI files to the updaters list.

**Adding Authorized Updaters**

Any executable file can be added to the updaters list by using the following command:

```
S3> sadmin updaters add WindowsInstaller-KB893803-v2-x86.exe
```

The above example unconditionally authorizes the Windows Installer for a HotFix, KB893803, to perform updates on protected files or registry keys.

The following log entry is also generated:

```
Local Administrator executed command 'sadmin updaters add WindowsInstaller-KB893803-v2-x86.exe' at Thu Nov 15 2007 17:53:52 (Return status: 0).
```

Any MSI file can be added to the updaters list by using the following command:

```
S3> sadmin updaters add Ica32Pkg.msi
```

The above example unconditionally authorizes the Windows Installer for an MSI file, Ica32Pkg.msi, to perform changes on protected files or registry keys. The new files are placed on the system and solidified.

The following log entry is also generated:

```
Local Administrator executed command 'sadmin updaters add "C:\Documents and Settings\Administrator\Desktop\Ica32Pkg.msi" at Thu Nov 15 2007 15:36:19 (Return status: 0).
```

The following command sets *iexplore.exe* as an authorized updater only when it is launched by *svchost.exe* as its parent

```
S3> sadmin updaters add -p svchost.exe iexplore.exe
```
The following command sets `svchost.exe` as an authorized updater only when its loads the library `system32\wuauserv.dll`

S3> `sadmin updaters add -l system32\wuauserv.dll svchost.exe`

The following example illustrates the addition of Windows Updaters using a scheduled update. The `-t` option causes the associated tag, e.g., `Win_up_schedule1` to be written to the log for all files that are solidified or unsolidified due to this update rule.

S3> `sadmin updaters add -t Win_up_schedule1 -l system32\wuauserv.dll svchost.exe`

S3> `sadmin updaters add -t Win_up_schedule2 -l system32\wuaueng.dll svchost.exe`

S3> `sadmin updaters add -t Win_up_schedule3 -p svchost.exe iexplore.exe`

S3> `sadmin updaters add -t Win_up_schedule4 -p svchost.exe wuauclt.exe`

S3> `sadmin updaters add -t Win_up_schedule5 -p svchost.exe update.exe`

S3> `sadmin updaters add -t Win_up_schedule6 -p svchost.exe WindowsInstaller-KB893803-v2-x86.exe`

S3> `sadmin updaters add -t Win_up_schedule7 -p svchost.exe bitinst.exe`

S3> `sadmin updaters add -d -t Win_up_schedule8 winlogon.exe`

---

**Note:** It recommended to re-start the system after adding authorized updaters

### Deleting Authorized Updaters

Any protected file can be deleted from the updaters list by using the following command:

S3> `sadmin updaters remove pathname`

where `pathname` provides the path for the protected program that needs to be deleted from the authorized updaters list.

The following log entry is generated:

```
Local Administrator executed command 'sadmin updaters remove pathname' at Thu Nov 15 2007 17:55:34 (Return status: 0).
```

The following example illustrates the removal of Windows Updaters for scheduled update:

S3> `sadmin updaters remove -l system32\wuauserv.dll svchost.exe`

S3> `sadmin updaters remove -l system32\wuaueng.dll svchost.exe`

S3> `sadmin updaters remove -p svchost.exe iexplore.exe`
S3> sadmin updaters remove -p svchost.exe wuaclt.exe
S3> sadmin updaters remove -p svchost.exe update.exe
S3> sadmin updaters remove -p svchost.exe WindowsInstaller-KB893803-v2-x86.exe
S3> sadmin updaters remove -p svchost.exe bitinst.exe
S3> sadmin updaters remove winlogon.exe

Listing Authorized Updaters

The protected files can be listed using the following command:

S3> sadmin updaters list

After execution of this command, the following message appears on the screen:

-t Auto_2 luall.exe

The following log entry is generated:

Local Administrator executed command 'sadmin updaters list' at Thu Nov 15 2007 17:56:42 (Return status: 0).

Note: A running application should be restarted after adding it as an authorized updater.

Removing All (Flushing) Authorized Updaters

To remove all (flush) the complete list of authorized updaters, enter:

S3> sadmin updaters flush

Manual Updates

Through an Update Window

To perform manual software update in the Update Mode, perform the following steps:

Check the current status of the Solidifier using the following command:

S3> sadmin status

After execution of this command, the following message appears on the screen:

McAfee Solidifier: Enabled
McAfee Solidifier on reboot: Enabled

Begin the Update Mode using the following command:

S3> sadmin bu
After execution of this command, the following message appears on the screen:

**McAfee Solidifier is in update mode.**

The following log entry is generated:

*Local Administrator executed command 'sadmin bu' at Thu Nov 15 2007 10:15:44 (Return status: 0).*

The Solidifier status during Update Mode is viewed using the following command:

```
S3> sadmin status
```

After execution of this command, the following message appears on the screen:

**McAfee Solidifier: Update**  
**McAfee Solidifier on reboot: Update**

Now, you can perform software update actions: Add/delete/modify software on the computer. Double-click some program, for example, Windows2000-KB822831-x86-enu.exe to install it on the computer. Follow the application installation procedures as presented through the setup wizard. It may include restarting the computer.

End the Update Mode using the following command:

```
S3> sadmin eu
```

After execution of this command, the following log entry is generated:

*Local Administrator executed command 'sadmin eu' at Thu Nov 15 2007 10:20:06 (Return status: 0).*

Check the current status of the Solidifier using the following command:

```
S3> sadmin status
```

After execution of this command, the following message appears on the screen:

**McAfee Solidifier: Enabled**  
**McAfee Solidifier on reboot: Enabled**

---

**Note:** Windows2000-KB822831-x86-enu.exe is the Update for Windows Server 2000. This is an example only and the same procedure applies to other installations and software updates.

### Precedence of tag reporting

The event tags are reported to the System Controller in the following precedence:

- Changes done in Update mode
- Changes made by authorized updater
- Changes made via Secure Signed updates
Through Incremental Solidification

Solidifying a File

To solidify a specific file, for example, Hello.exe, use the following command:

S3> sadmin so c:\Hello.exe

After execution of this command, the following message appears on the screen:
00:00:00: Total files scanned 1, solidified 1

The following log entry is generated:

Solidifying a Folder

To solidify a specific folder, for example, C:\Program Files, use the following command:

S3> sadmin so "C:\Program Files"

After execution of this command, the following message appears on the screen:
00:00:02: Total files scanned 71, solidified 29

The following log entry is generated:
Local Administrator executed command 'sadmin so "C:\Program Files"' at Thu Nov 15 2007 10:27:07 (Return status: 0).

Solidifying a Volume

To solidify a specific volume, for example, the C: drive, use the following command:

S3> sadmin so C:

After execution of this command, the following message appears on the screen:
Solidifying volume C:\
00:00:31: Total files scanned 1733, solidified 978

The following log entry is generated:
Local Administrator executed command 'sadmin so C:\' at Thu Nov 15 2007 10:28:36 (Return status: 0).

Listing Solidified Files

The following command displays a list of files that have been solidified/write-protected on the system:

S3> sadmin list-solidified
Listing Unsolidified Files

The following command displays a list of files that have not been solidified on the system:

```
S3> sadmin list-unsolidified
```

This command may take a few minutes to complete and displays the files that have not been solidified.

Best Practice: Check Modification Attempts on Solidified Files

The check command is particularly useful for detecting and reporting modifications to a solidified file in the Disabled Mode. The user should execute the check command each time a system is solidified or updated but before rebooting. If the update procedure is successfully performed, the check command should not display modified files.

```
S3> sadmin check
```

This command displays the files that are solidified and have been modified by the user. The output is displayed as follows:

```
Checking volume C:\ ...
Checking volume E:\ ...
Checksum and Filetype mismatch for file 'E:\Documents and Settings\Administrator\Desktop\Hello.exe'
```

The check command does not work inside the Update Mode.

Solidifier administration by field personnel

Solidifier user model has been enhanced to add updaters and configuration attribute updates to an existing set of password-protected updaters/updates without needing to enter the password again. Thus, vendors selling servers with password-protected Solidifier installed can update the Solidifier configuration without needing to inform their users the original password. Also, vendors selling servers with Solidifier installed to other vendors can update the Solidifier configuration even when their customers have in turn sold the servers with password protection added to Solidifier.

To handle this situation, Solidifier provides the following solutions:

- Allow authentication through signatures instead of passwords
- Signed updaters can issue sadmin commands on the CLI without requiring any password

The steps to add a signed updater are given below:

1. Create an executable binary that contains sadmin commands.
2. Sign this executable binary and then execute it.

However, the following scenarios are not applicable:
Signed binaries/updater executables are not allowed to execute when the local CLI is locked down.

The updater executable will prompt for password for the execution of sadmin commands when the system is in Disabled mode.

Script files cannot work as an updater. Hence the above scenario works fine only for executable binaries only.

### Users as Updaters

Starting with version 4.9.0, Solidifier allows you to specify users as updaters so that the file changes made by these users are treated as authorized changes. Thus, all files modified by users declared as updater users are automatically re-solidified, all files added by these users are automatically solidified, and all files deleted by these users are considered unsolidified.

To declare a user as an updater user, use the following syntax:

```
S3> sadmin updaters add -u USERNAME
```

Here, USERNAME can be a simple name (for example, john_smith), user’s domain name (john_smith@mycompany.com), or user’s hierarchical domain name (MYDOMAIN\john_smith). If you specify user’s simple name, users with this name in ALL domains are marked as updater users.

For example:

```
S3> sadmin updaters add -u jane.smith@mycompany.com
```

To declare a user as an updater user and also specify a tag name, use the following syntax:

```
S3> sadmin updaters add -t TAG -u USERNAME
```

Here, TAG is the tag name (for example, “McAfee001”) and USERNAME is as described above.

To unmark a user as an updater user, use the following syntax:

```
S3> sadmin updaters remove -u USERNAME
```

Here, USERNAME is as described above. Please ensure that you specify USERNAME in the same format as that used while declaring this user as an updater user.

**Note:** Other `updaters` command arguments like `-l`, `-p`, `-d`, and `-n` are not applicable when you specify the `-u` argument.

### Scripts as Updaters

Starting with version 4.9.0, you can also declare scripts as updaters so that the file changes made by these scripts are treated as authorized changes.
Note: The Scripts as Updaters functionality is available on all Windows platforms except Windows Vista (64-bit), Windows Server 2008 (64-bit), and Windows Server 2003 (IA64).

To declare a script as updater, use the following syntax:

\texttt{S3> sadmin updaters add SCRIPT}

Here, \texttt{SCRIPT} is the full path name of the script. For example:

\texttt{S3> sadmin updaters add C:\myscripts\myscript12.bat}

To unmark a script that was earlier declared as updater, use the following syntax:

\texttt{S3> sadmin updaters remove SCRIPT}

Here, \texttt{SCRIPT} is the full path name of the script. For example:

\texttt{S3> sadmin updaters remove C:\myscripts\myscript42.bat}

Note: Other \texttt{updaters} command arguments like \texttt{-l}, \texttt{-p}, are not applicable when you are specifying a script as updater.

Applications in a Trusted Path as Updaters

Starting with version 4.9.0, you can also declare all binaries/scripts located in a trusted folder as updaters so that the file changes made by these binaries/scripts are treated as authorized changes.

Note: Only those binaries/scripts with extensions .exe, .cmd, .sys, .com, .vbe, .vbs, or .bat are supported.

To include all binaries/scripts located in a volume as updaters, use the following syntax:

\texttt{S3> sadmin trusted -i -u VOLUMESETNAME}

The above command includes volume \texttt{VOLUMESETNAME} as a trusted volume and includes all binaries/scripts (hierarchically) under this volume as updaters.

The volume names \texttt{VOLUMESETNAME} can be specified on the Windows platform in any of the following ways:

- \texttt{\servername\sharename} – specific share \texttt{sharename} exported by the server \texttt{servername}
- \texttt{\servername} - all shares exported by server \texttt{servername}
- \texttt{\*} - all shares exported by all servers

To include all binaries/scripts located in a folder as updaters, use the following syntax:

\texttt{S3> sadmin trusted -i -u PATHNAME}
The above command includes folder *PATHNAME* as a trusted folder and includes all binaries/scripts (hierarchically) under this folder as updaters. You can use wildcard characters in path name as long as the wildcard character is not the last specification in the name. Thus, `C:\Windows\*\drivers` is allowed but `C:\Windows\*\dr*` is not.

You can also exclude a folder under a trusted volume or a trusted folder, so that this folder is no longer included as a trusted folder and all binaries/scripts (hierarchically) under this folder are no longer included as updaters. Use the following syntax:

```
S3> sadmin trusted -e PATHNAME
```

Here, PATHNAME is as described above.

To remove the trusted specification of a volume or a folder so that it is no longer included in the trusted list (specified earlier using `-i` argument) or excluded from the trusted list (specified earlier using `-e` argument), use the following syntax:

```
S3> sadmin trusted -r VOLUMESETNAME | PATHNAME
```

Here, VOLUMESETNAME and PATHNAME are as described above.

### Updating Applications in Enabled Mode

Starting with version 4.9.0, Solidifier allows you to upgrade applications in Enabled mode. This support is available by enabling the `INV_DEFERRED_UPDATE` feature.

To update an application in Enabled mode, perform these steps:

1. Ascertain the names and checksums of all binary files included in the upgrade package for the application.

2. Register each binary file as follows:

   ```
   S3> sadmin so -c CHECKSUM [-t TYPE] FILE
   ```

   Here, FILE is the full pathname of the binary file, CHECKSUM is the SHA1 checksum of the binary file, and TYPE is the type of the binary file.

   TYPE can be '32bit-exe', '32bit-dll', '32bit-driver', '64bit-exe', '64bit-dll', '64bit-driver', or script.

3. Now, install the application in the usual manner – manually or through your Software Management System.

After the application has been installed, all specified binary files will also be solidified.

To unregister binary files, use the following syntax:

```
S3> sadmin unso -c FILE
```
Here, FILE is as described above.
Routine Maintenance of a Solidified System (UNIX)

This chapter contains the following topics:

- “Automated Updates”
- “Manual Updates”

Automated Updates

The Solidifier prevents the modification of solidified executable files without entering the update mode. The Solidifier provides the updaters command to unconditionally authorize legitimate programs to update software on a solidified system.

Adding Authorized Updaters

Any executable file (ELF binary or #! script) can be added to the updaters list by using the following command:

```bash
# sadmin updaters add <pathname>
```

Where `<pathname>` provides the path for the solidified program, which is being unconditionally authorized to perform updates, i.e., modifications to self, or other solidified files, or the addition or installation of new programs, or uninstallation of existing programs on the solidified system.

The following log entry is also generated:

```
Local Administrator executed command 'sadmin updaters add <filename>' at Wed Apr 23 2008 17:53:52 (Return status: 0).
```

The following command sets child.sh as an authorized updater only when it is launched by parent.sh as its parent:

```bash
# sadmin updaters add -p parent.sh child.sh
```

The following example illustrates the addition of updaters using a scheduled update. The `-t` option causes the associated tag, e.g., `tag1` to be written to the log for all files that are solidified or unsolidified due to this update rule.

```bash
# sadmin updaters add -t tag1 test.sh
# sadmin updaters add -t tag2 -p parent.sh child.sh
# sadmin updaters add -d -t tag3 parent.sh
```

Deleting Authorized Updaters

Any protected file can be deleted from the updaters list by using the following command:
# sadmin updaters remove *pathname*

where *pathname* provides the path for the protected program that needs to be deleted from the authorized updaters list.

The following log entry is generated:

**Local Administrator executed command 'sadmin updaters remove *pathname*' at Wed Apr 23 2008 17:55:34 (Return status: 0).**

The following example illustrates the removal of updaters:

```
# sadmin updaters remove -p parent.sh child.sh
# sadmin updaters remove test.sh
```

### Listing Authorized Updaters

The protected files can be listed using the following command:

```
# sadmin updaters list
```

After execution of this command, the following message appears on the screen:

```
-t tag3 parent.sh
```

The following log entry is generated:

**Local Administrator executed command 'sadmin updaters list' at Wed Apr 23 2008 17:56:42 (Return status: 0).**

**Note:** A running application should be restarted after adding it as an authorized updater.

### Removing All (Flushing) Authorized Updaters

To remove all (flush) the complete list of authorized updaters, enter:

```
# sadmin updaters flush
```

### Manual Updates

#### Through an Update Window

To perform manual software update in the Update Mode, perform the following steps:

Check the current status of the Solidifier using the following command:

```
# sadmin status
```

After execution of this command, the following message appears on the screen:

**McAfee Solidifier: Enabled**

**McAfee Solidifier on reboot: Enabled**
Begin the Update Mode using the following command:

```bash
# sadmin bu
```

After execution of this command, the following message appears on the screen:

**McAfee Solidifier is in update mode.**

The following log entry is generated:

```bash
Local Administrator executed command 'sadmin bu' at Wed Apr 23 2008 10:15:44 (Return status: 0).
```

The Solidifier status during Update Mode is viewed using the following command:

```bash
# sadmin status
```

After execution of this command, the following message appears on the screen:

**McAfee Solidifier:** Update
**McAfee Solidifier on reboot:** Update

Now, you can perform software update actions: Add/delete/modify software on the computer.

End the Update Mode using the following command:

```bash
# sadmin eu
```

After execution of this command, the following message appears on the screen:

**McAfee Solidifier is in update mode.**

The following log entry is generated:

```bash
Local Administrator executed command 'sadmin eu' at Wed Apr 23 2008 10:20:06 (Return status: 0).
```

Check the current status of the Solidifier using the following command:

```bash
# sadmin status
```

After execution of this command, the following message appears on the screen:

**McAfee Solidifier:** Enabled
**McAfee Solidifier on reboot:** Enabled

**Precedence of tag reporting**

The event tags are reported to the System Controller in the following precedence:

- Changes done in Update mode
- Changes made by an authorized updater
Through Incremental Solidification

Solidifying a File

To solidify a specific file, for example, test.sh, use the following command:

```
# sadmin so /test.sh
```

After execution of this command, the following message appears on the screen:
00:00:00: Total files scanned 1, solidified 1

The following log entry is generated:
```
```

Solidifying a Folder

To solidify a specific folder, for example, /mydir, use the following command:

```
# sadmin so /mydir
```

After execution of this command, the following message appears on the screen:
00:00:02: Total files scanned 71, solidified 29

The following log entry is generated:
```
Local Administrator executed command 'sadmin so /mydir' at Fri Apr 25 2008 10:27:07 (Return status: 0).
```

Listing Solidified Files

The following command displays a list of files that have been solidified/write-protected on the system:

```
# sadmin list-solidified
```

Listing Unsolidified Files

The following command displays a list of files that have not been solidified on the system:

```
# sadmin list-unsolidified
```

This command may take a few minutes to complete and displays the files that have not been solidified.

Best Practice: Check Modification Attempts on Solidified Files

The check command is particularly useful for detecting and reporting modifications to a solidified file in the Disabled Mode. The user should execute the `sadmin check` command each time a system is solidified or updated but before rebooting. If the update procedure is successfully performed, the check command should not display modified files.
# sadmin check

This command displays the files that are solidified and have been modified by the user. The output is displayed as follows:

Checking volume / ...
Checking volume /mnt ...
Checksum and filetype mismatch for file `/foo2bar2`.

The check command does not work inside the Update Mode.
Application Control

About Application Control

Note: The Application Control feature is available on Solidifier for Windows only.

Starting with version 4.9.0, Solidifier provides a comprehensive feature called Application Control that allows you to define 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.

The Application Control feature is controlled by the app-control feature and uses the auth command for configuration.

Note: The Application Control feature has the highest precedence over all Solidifier features except the “Users as Updaters” feature that allow/ban applications. Thus, an application once declared to be an allowed or whitelist application will be allowed to run even if it is not solidified or is not declared as an updater. Similarly, an application once declared to be a banned or blacklist application will not be allowed to run even if it is solidified or is declared as an updater.

Using the Application Control Feature

The steps to use the Application Control feature are as follows:

1. Identify allowed applications. Also, identify whether any of these allowed applications need to run as updaters.
2. Identify banned applications.
3. Ascertain the checksum or version details of these applications. You need one of these details for specifying applications with the auth command.

   Use your favorite method for computing the Checksum (SHA1 hash value) of your application file. One of the standard utilities available is Microsoft’s File Checksum Integrity Verifier (FCIV) command-prompt utility.

   Application Version details are available in the Version tab (or Details tab for Windows Server 2008 and Windows Vista) of Properties dialog box. Product name and Product version entries are required for specifying applications with the auth command.

4. Declare the applications as allowed or banned.

Declare Applications as Allowed Applications

To declare an application as an allowed application using Checksum, use the following syntax:
S3> sadmin auth -a -c CHECKSUM

Here, CHECKSUM is the SHA1 hash value of the application file.

For example:

S3> sadmin auth -a -c 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12

To declare an application as an allowed application using Version Details, use the following syntax:

S3> sadmin auth -a -v VERSION

Here, VERSION is the application version details in Product name\Product version format.

Please note the following:

- This method is not applicable for the following cases (use Checksum instead):
  - Product name and Product version entries are not available.
  - Product name and Product version entries contain special characters like ® etc.
  - The application is a self-launching application.
- Only the first two strings (including the separator characters) of Product version need to be specified. For example, if Product Version is 8.0.2.3, you need to specify only 8.0. Similarly, you need to specify only 8, 2 if the Product Version is 8, 2, 5, 7. Only dot, comma, and space characters are supported as separator characters.
- If Product name and/or Product version values have spaces, you need to specify them enclosed in a single pair of double quotes, for example, “A B C\1, 9”.

In case,

For example:

S3> sadmin auth -a -v McAfee\8.5

**Declare Applications as Allowed Updater Applications**

To declare an application as an allowed updater application, use the following syntax that uses an additional -u argument:

S3> sadmin auth -a -u [-c CHECKSUM] | [-v VERSION]

Here, CHECKSUM and VERSION have the same meanings as described above.

**Declare Applications as Banned Applications**

To declare an application as a banned application, use the following syntax:

S3> sadmin auth -b [-c CHECKSUM] | [-v VERSION]
Here, CHECKSUM and VERSION have the same meanings as described above.

**List Allowed/Banned Applications**

To list the Allowed/Banned applications, use the following syntax:

```
S3> sadmin auth -l
```

The list of Allowed/Banned Applications appears as in the following example:

```
cb - "17dfa91a89f0dcad44b3d9c4a99ae8e9bb300756"
cau "36eed05f8b52fedd6f7e477800228dcd56cfe45b"
```

**Unmark Applications**

To unmark an application as Allowed or Banned, use the following syntax:

```
S3> sadmin auth -r CHECKSUM | VERSION
```

Here, CHECKSUM and VERSION have the same meanings as described above. Use CHECKSUM or VERSION just as you had specified while adding the application as an Allowed or Banned application.

Use the following command to unmark all applications declared as Allowed or Banned:

```
S3> sadmin auth -f
```
Troubleshooting

Event Log Messages

The Solidifier events can be viewed in the Application Event Logs: (Start menu → Programs → Administrative Tools → Event Viewer → Application) on Windows platform or from the file /var/log/mcafee/solidcore/solidcore.log on UNIX platforms.

Note: You can view the event sink information using the sadmin event sink command.

The table below lists the events that are generated by the Solidifier and provides their severity and event message:

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Key</th>
<th>Event Log Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALERT_CACHE_OVERFLOW</td>
<td>Error</td>
<td>Event Cache Watermark Overflowed.</td>
</tr>
<tr>
<td>ALERT_CACHE_WM_BREACHED</td>
<td>Warning</td>
<td>Event Cache Watermark Breached. Level = {level} percent of cache size.</td>
</tr>
<tr>
<td>ALERT_CACHE_WM_RECOVERED</td>
<td>Information</td>
<td>Event Cache Watermark Recovered. Level = {level} percent of cache size.</td>
</tr>
<tr>
<td>BEGIN_UPDATE</td>
<td>Information</td>
<td>McAfee Solidifier is starting update mode on the system to allow updates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Workflow Id: {workflow_id}, Comment: {comment}).</td>
</tr>
<tr>
<td>BOOTING_DISABLED</td>
<td>Warning</td>
<td>McAfee Solidifier is currently disabled.</td>
</tr>
<tr>
<td>BOOTING_DISABLEDTERNAL_ERROR (Windows only)</td>
<td>Error</td>
<td>McAfee Solidifier is disabled because of internal error {error}.</td>
</tr>
<tr>
<td>BOOTING_DISABLED_SAFEMODE (Windows only)</td>
<td>Warning</td>
<td>McAfee Solidifier is disabled because system is in safe mode.</td>
</tr>
<tr>
<td>BOOTING_ENABLED</td>
<td>Information</td>
<td>McAfee Solidifier is currently enabled.</td>
</tr>
<tr>
<td>BOOTING_UPDATE_MODE</td>
<td>Information</td>
<td>System is booting in McAfee Solidifier update mode.</td>
</tr>
<tr>
<td>COMMAND_EXECUTED</td>
<td>Information</td>
<td>user_name executed command {command} at {end_time} (Return status: {status}).</td>
</tr>
<tr>
<td>DISABLED_DEFERRED</td>
<td>Warning</td>
<td>McAfee Solidifier will be disabled on next reboot.</td>
</tr>
<tr>
<td>ENABLED_DEFERRED</td>
<td>Information</td>
<td>McAfee Solidifier will be enabled on next reboot.</td>
</tr>
<tr>
<td>END_UPDATE</td>
<td>Information</td>
<td>McAfee Solidifier is ending update mode on the system (Workflow Id: {workflow_id}).</td>
</tr>
<tr>
<td>Event Name</td>
<td>Key</td>
<td>Event Log Entry</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EXECUTION_DENIED</td>
<td>Error</td>
<td>McAfee Solidifier prevented unauthorized execution of <code>filename</code> by process <code>processname</code> (Process Id: PID, User: <code>user_name</code>).</td>
</tr>
<tr>
<td>FILE_RESOLIDIFIED</td>
<td>Information</td>
<td><code>filename</code> was resolidified which was modified by program <code>program_name</code> (User: <code>user_name</code>, Workflow Id: <code>workflow_id</code>).</td>
</tr>
<tr>
<td>FILE_SOLIDIFIED</td>
<td>Information</td>
<td><code>filename</code> was solidified which was created by program <code>program_name</code> (User: <code>user_name</code>, Workflow Id: <code>workflow_id</code>).</td>
</tr>
<tr>
<td>FILE_UNSOLIDIFIED</td>
<td>Information</td>
<td><code>filename</code> was unsolidified which was deleted by program <code>program_name</code> (User: <code>user_name</code>, Workflow Id: <code>workflow_id</code>).</td>
</tr>
<tr>
<td>INVENTORY_CORRUPT</td>
<td>Error</td>
<td>McAfee Solidifier detected that its internal inventory for the volume <code>volumename</code> is corrupt. To rectify, please delete the inventory and solidify the volume again.</td>
</tr>
<tr>
<td>PKG_MODIFICATION_ALLOWED_UPDATE</td>
<td>Information</td>
<td>McAfee Solidifier allowed package modification by <code>filename</code> by user <code>user_name</code>. (Workflow Id: <code>workflow_id</code>)</td>
</tr>
<tr>
<td>PKG_MODIFICATION_PREVENTED</td>
<td>Error</td>
<td>McAfee Solidifier prevented package modification by <code>filename</code> by user <code>user_name</code>.</td>
</tr>
<tr>
<td>PKG_MODIFICATION_PREVENTED_2</td>
<td>Error</td>
<td>McAfee Solidifier prevented package modification by <code>filename</code> by user <code>user_name</code>.</td>
</tr>
<tr>
<td>PROCESS_HIJACKED</td>
<td>Error</td>
<td>McAfee Solidifier detected an attempt to exploit process <code>processname</code> from address <code>faulting_address</code>.</td>
</tr>
<tr>
<td>PROCESS_TERMINATED_UNAUTH_API</td>
<td>Error</td>
<td>McAfee Solidifier prevented process <code>processname</code>, being run by <code>user_name</code>, from making unauthorized access to API <code>api_name</code> (return address <code>return_address</code>). The process was terminated.</td>
</tr>
<tr>
<td>PROCESS_TERMINATED_UNAUTH_SYSCALL</td>
<td>Error</td>
<td>McAfee Solidifier prevented process <code>processname</code>, being run by <code>user_name</code>, from making unauthorized syscall <code>syscall_number</code> (return address <code>return_address</code>). The process was terminated.</td>
</tr>
<tr>
<td>READ_DENIED</td>
<td>Error</td>
<td>McAfee Solidifier prevented an attempt to read file <code>filename</code> by process <code>processname</code> (Process Id: PID, User: <code>user_name</code>).</td>
</tr>
<tr>
<td>REG_KEY_WRITE_DENIED</td>
<td>Error</td>
<td>McAfee Solidifier prevented an attempt to modify Registry key <code>registry_keyname</code> by process.</td>
</tr>
</tbody>
</table>
## Event Name
### Key
### Event Log Entry

(Windows only)
- **processname** (Process Id: PID, User: user_name).
- **REG_VALUE_WRITE_DENIED** (Windows only) Error
  - McAfee Solidifier prevented an attempt to modify Registry key registry_keyname with value value by process processname (Process Id: PID, User: user_name).
- **SC_CONNECTED** Information
  - Connected to McAfee System Controller hostname.
- **SC_DISCONNECTED** Information
  - Disconnected from McAfee System Controller hostname.
- **TRIAL_EXPIRED** (Windows only) Error
  - McAfee Solidifier will disable on next reboot as its trial period has expired.
- **UPDATE_MODE_DEFERRED** Information
  - McAfee Solidifier will be in update mode on next reboot (Workflow Id: %s, Comment: %s).
- **WRITE_DENIED** Error
  - McAfee Solidifier prevented an attempt to modify file filename by process processname (Process Id: PID, User: user_name).

### Troubleshooting Microsoft Windows related issues

#### OS limitation: Filter Driver Interactions

The Windows NT file system imposes fundamental restrictions on the amount of memory that file system filter drivers can consume in the kernel. When a system has multiple filter drivers loaded, e.g., anti virus agents, backup agents, access control agents, system monitoring agents, security software agents, interactions between them can cause application or system hangs. Such a situation requires customers to decide which agents are absolute operational necessities and consider uninstalling the inessential ones. (Note that the uninstallation will require a reboot, since the inessential filter drivers must be unloaded from the kernel.)

#### Boot failures due to self-modifying drivers

There are certain drivers which on being loaded modify their images on disk. If prevented by Solidifier, they return errors which might lead to a blue screen. Such drivers cannot be unsolidified, because then they can't be loaded, for example, clkdrv.sys, the crypt key driver. We recommend that such drivers should be solidified and always authorized to execute using the command

```
S3> sadmin attr add -a filename
```

#### Booting in Safe Mode

To use a Safe Boot option, follow these steps:
1. Restart your computer and start pressing the F8 key on your keyboard. On a computer that is configured for booting to multiple operating systems, you can press the F8 key when the Boot Menu appears.

2. Select an option when the Windows Advanced Options menu appears, and then press ENTER.

3. When the Boot menu appears again, and the word "Safe Mode" appear in blue at the bottom, select the installation that you want to start, and then press ENTER.

Detailed instructions are available at [http://support.microsoft.com/kb/315222](http://support.microsoft.com/kb/315222)

**Note:** The Solidifier is disabled in safe mode (Windows 2000, Windows XP, and Windows 2003), Directory services restore mode and VGA mode (Windows NT4) by default.

### Troubleshooting system crashes (Windows)

In the rare event that you encounter a system crash when the Solidifier is enabled, you can follow the steps outlined below for recovering from the crash and getting the system operational once again.

<table>
<thead>
<tr>
<th>System crash (<strong>Blue Screen</strong>) when Solidifier is enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Symptom</strong></td>
</tr>
<tr>
<td>The system will show a blue screen with a bug check number.</td>
</tr>
<tr>
<td>The Field Engineer should check that the automatic reboot on BSOD option is disabled, while trying to reproduce the Bug check. Otherwise, the system will reboot automatically without showing any bug check number, when the bug check actually happens.</td>
</tr>
<tr>
<td><strong>What should you note down and report?</strong></td>
</tr>
<tr>
<td>• The bug check number and all the parameters it shows on screen.</td>
</tr>
<tr>
<td>• The complete memory dump, <code>memory.dmp</code>, which resides in the Windows folder.</td>
</tr>
<tr>
<td><strong>What is the recovery procedure?</strong></td>
</tr>
<tr>
<td>• Boot the system in safe mode</td>
</tr>
<tr>
<td>o Press F8 as the system is booting up</td>
</tr>
<tr>
<td>o Select <em>Boot in safe mode</em>.</td>
</tr>
<tr>
<td>In Windows 2000, XP and 2003, press &quot;F8&quot; as the system is booting up. From the menu that appears, select the &quot;Safe mode with networking&quot; option.</td>
</tr>
<tr>
<td>In Windows NT, by default the boot menu will show &quot;VGA boot&quot; and/or &quot;Safe boot&quot; options. Select any one of the two options.</td>
</tr>
<tr>
<td>• Disable Solidifier</td>
</tr>
</tbody>
</table>
- Issue the `scsrvc -d` at the Solidifier command line interface.
- Issue the `sadmin disable` command.
- Gather diagnostics: Run `GatherInfo`
  
The crash dump, if it was enabled before the occurrence of the BSOD, will be found in the configured path. This is very useful for debugging.
- Reboot the system.

### No Error Message is displayed while trying to enable Solidifier when inventory is corrupted

<table>
<thead>
<tr>
<th>Symptom</th>
</tr>
</thead>
<tbody>
<tr>
<td>The system will show a blue screen with the following error check:</td>
</tr>
<tr>
<td><code>0xE0100010(0x00000010,0x00000000,0x00000000,0x00000000)</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What should you note down and report?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot the system manually and execute the following command:</td>
</tr>
<tr>
<td><code>S3&gt; sadmin status</code></td>
</tr>
<tr>
<td>The corrupted volume will show the status as ‘Corrupt’ as seen in the following output:</td>
</tr>
</tbody>
</table>

```
McAfee Solidifier: Disabled
McAfee Solidifier on reboot: Disabled
System Controller: 192.168.82.193:51848
Local CLI access: Recovered

[fstype] [status] [driver status] [volume]
* NTFS Corrupt Unattached C:\
  FAT32 Solidified Unattached E:\
```

On issuing the "sadmin enable" command, the system should show proper error message and enable should not be allowed. If the inventory is corrupt, no error message is displayed rather the following informative message is displayed:

**Solidify the system volume first.**
What is the recovery procedure?

You should follow the steps given below to recover a volume’s inventory:

1. Delete inventory for that volume by issuing the following command:
   
   S3> del <volume-name>

2. Restart Solidifier service using the following commands:
   
   S3> net stop scsrvc
   S3> net start scsrvc

3. Solidify the volume again using the following command:
   
   S3> sadmin so <volume name>

Troubleshooting system crashes (UNIX)

In the rare event that you encounter a system crash when the Solidifier is enabled, you can follow the steps outlined below for recovering from the crash and getting the system operational once again.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>The system may hang and stop responding to any command.</th>
</tr>
</thead>
</table>
| What is the recovery procedure? | - Boot the system in single mode  
- Open the Solidifier configuration file viz. /etc/mcafee/solidcore/solidcore.conf and change the value of parameter RTEModeOnReboot to be 0x0.  
- Now, run the Solidifier service manually (/<install-dir>/mcafee/solidcore/scripts/scsrvc -d). This will start the Solidifier in Disabled mode.  
- Remove the Solidifier package, if required  
- Gather diagnostics: Run GatherInfo  
- Reboot the system |

The Field Engineer who observes the symptom first hand, or the Support Engineer who is responding to a field issue, must ensure that the following information is collected before contacting McAfee support:
### Information to be collected for debugging

<table>
<thead>
<tr>
<th>Problem description</th>
<th>Provided by person reporting the problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnostics</td>
<td>Information generated using Solidifier utilities</td>
</tr>
<tr>
<td>Error messages</td>
<td>Observe and record as described below</td>
</tr>
<tr>
<td>Device /Appliance image</td>
<td>To help recreate the problem</td>
</tr>
</tbody>
</table>

### Troubleshooting Active Directory related issues

#### Not able to execute logon scripts from Active Directory (Group Policy)

**Symptom**

The system shows the following error message:

```plaintext
McAfee Solidifier prevented unauthorized execution of '\Device\LanmanRedirector\<Domain Controller host_name>\sysvol\<Domain name>\Policies\{<unique_policy_name>\} \User\Scripts\Logon\<script_name>\' by process \User\\script_name\ (Process Id: PID, User: user_name).
```

**What steps should you follow?**

We recommend that you follow the following practices:

1. Solidify the complete system (Domain Controller) with the `sadmin solidify` command. There is no need to solidify any path related to Sysvol manually, as all Solidifier-supported files will be solidified automatically on the system.

2. Add the `ntfrs.exe` file as an authorized updater to automatically update all Sysvol volumes among all domain controllers in a local domain using the following command:

   ```plaintext
   S3> sadmin updaters add -t AD ntfrs.exe
   ```

3. Trust the Sysvol network path of each domain controller in the local domain in all domain controller (self and peers) using the following command:

   ```plaintext
   S3> sadmin trusted -i \<DC_DNS_NAME>\SYSVOL
   ```

   Here, `<DC_DNS_NAME>` is the DNS name of the Domain Controller machine (for example, `dc1.mycompany.com`).

   **Example:** Assume that `mycompany.com` is the root domain and has
two domain controllers named \textit{dc1.mycompany.com} and \textit{dc2.mycompany.com}. Then, you have to add two rules in both domain controllers (self and peers) for proper functioning of Group Policy of AD as follows:

\begin{verbatim}
S3> sadmin trusted -i \dc1.mycompany.com\SYSVOL
S3> sadmin trusted -i \dc2.mycompany.com\SYSVOL
\end{verbatim}

If a child domain of the root domain is also present in Active Directory Forest, one trusted rule for each domain controller (self and peers) in the child domain needs to be added in each domain controller. For example, assume that \textit{sales.mycompany.com}, a child domain of \textit{mycompany.com}, has its own three domain controllers named cdc1.sales.mycompany.com, cdc2.sales.mycompany.com, and cdc3.sales.mycompany.com respectively. In this case, three trusted rules need to be added in all three domain controllers of the child domain for proper functioning of Group Policy in the child domain as follows:

\begin{verbatim}
S3> sadmin trusted -i \cdc1.sales.mycompany.com\SYSVOL
S3> sadmin trusted -i \cdc2.sales.mycompany.com\SYSVOL
S3> sadmin trusted -i \cdc3.sales.mycompany.com\SYSVOL
\end{verbatim}

\textbf{Note:} You can add and execute any file on the trusted path, independent of the Solidifier status (Enabled or Disabled). You can execute unauthorized (or unsolidified) code only from the trusted network path, and not from the local system path. The existing files which are solidified on local system are still protected and cannot be modified/deleted from the network path.

4. Always run Solidifier commands with actual file paths to list solidified files status. For example:

\begin{verbatim}
S3> sadmin ls C:\WINDOWS\SYSVOL\domain\Policies
\end{verbatim}

The Field Engineer who observes the symptom first hand, or the Support Engineer who is responding to a field issue, must ensure that the following information is collected before contacting McAfee support:

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
\textbf{Information to be collected for debugging} & \\
\hline
Problem description & Provided by person reporting the problem \\
\hline
Diagnostics & Information generated using Solidifier utilities \\
\hline
\end{tabular}
\end{table}
Log File for Debugging (Windows)

A log file named solidcore.log is created in the <install-dir>\Logs folder (Windows) or the /var/log/mcafee/solidcore/ directory (UNIX). The solidcore.log file is rotated as it reaches the threshold size of 2048 MB. There can be at most five such log files present in this directory at any given time. The files are generated with the following names:

- solidcore.log
- solidcore.log.1
- solidcore.log.2
- solidcore.log.3
- solidcore.log.4

The logs are rotated in the chronological order such that the file named "solidcore.log.4" has the oldest logs and "solidcore.log" has the newest logs.

Note: The above information is based on the default settings of the solidcore.log file. However, if you have configured any of the settings viz, path, size or number of this file, then you should take the new configuration into consideration while trouble-shooting.

Error messages

Always ask the person who is reporting an error to record an error message related to the symptom that is visible. The error message may be:

- In a console window, or
- At the Solidifier command line interface, or
- In a popup window from the Operating System or an application (Windows only), or
- In the event viewer
- In the /var/log/messages file (Linux) or /var/adm/messages file (Solaris)

These error messages provide valuable insight to people who investigate the problem further. If there are multiple error messages that look similar but are not identical, the user should record the details of each one as they will be helpful for providing the context surrounding the problem.

Command Line Interface Error Messages

When an invalid filename is provided to a command such as sadmin so, then the following message is displayed on the CLI:

The path 'filename' does not exist or cannot be accessed.
Solution: Provide a valid filename and perform solidification.

When an invalid volume ID is provided to a command such as sadmin so that it accepts volume ID as parameter, then the following message is displayed on the CLI:

*The path [<volume name>:] is on an unsupported volume.*

Solution: Provide correct supported volume id.

When sadmin is run from non-administrative account it fails to connect to the Solidifier Service and the following message is displayed on the CLI:

*Failed to connect to the McAfee Solidifier Service: Insufficient privileges.*

Solution: Re-login using an account that has administrative privileges.

If you try to run the solidify command on a volume with improper volume name such as non-alphabetic characters or colon ‘:’ is missing after the volume name, then the following message is displayed on the CLI:

*The Path ‘C:\Program Files\McAfee\Solidcore\<Volume_Name>’ does not exist.*

Solution: Provide a proper supported volume name and perform solidification.

**Legitimate failures that are not errors**

This section introduces the user to the behavior of the Solidifier through examples. Once the Solidifier is enabled on a solidified system and upholds the following properties:

- Only solidified code can run. Any code that is created or modified at run-time on a solidified system is not allowed to run, unless explicitly authorized to do so
- Vulnerabilities in solidified code cannot be exploited
- Authorized code cannot be tampered with. Any OS or application code cannot be deleted, renamed or otherwise updated in any fashion

**Only Solidified Programs Can Be Executed**

The Solidifier ensures that a program file can be executed only if it was solidified. Every time some code is launched, loaded, or executed from disk, Solidifier checks whether or not the code has been previously solidified. If so, then the code executes normally, otherwise the Solidifier prevents its execution.

**Attempt to execute an unsolidified .exe**

When an attempt is made to execute an unsolidified program *putty.exe* from a supported volume, the operation fails and a pop-up window appears displaying:

*Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.*
If putty.exe is executed from the command prompt, the following message is displayed:

Access is denied.

In both cases, the following log entry is generated:

```
McAfee Solidifier prevented unauthorized execution of 'C:\Documents and Settings\Administrator\Desktop\dbg_x86_6.5.3.8.exe' by process C:\WINDOWS\system32\CMD.EXE (Process Id: 1580, User: MYDOMAIN\Administrator).
```

The Event Log shows that the Solidifier prevented the execution of unauthorized code. An error message is displayed in the Event Viewer. No user action is required.

**Attempt to execute an unsolidified .vbs script**

When a user double clicks an unsolidified (unauthorized) .vbs script, its execution fails and the Windows Script Host displays a pop-up window as in the following message:

```
Loading script "C:\shared\AUTH\AUTH.vbs" failed (Access is denied.).
```

The following log entry is generated:

```
McAfee Solidifier prevented unauthorized execution of 'C:\shared\Auth\Auth.vbs' by process C:\WINDOWS\System32\wscript.exe (Process Id: 928, User: Win2K3-TST-POOJ\Administrator).
```

The Event Log shows that the Solidifier prevented the execution of unauthorized code. An error message is displayed in the Event Viewer. No user action is required.

**Attempt to execute an unsolidified file (ELF binary)**

When an attempt is made to execute an unsolidified file foo2bar2, the operation fails.

If foo2bar2 is executed from the command prompt, the following message is displayed:

Permission denied

The following Event Log entry is generated:

```
McAfee Solidifier prevented unauthorized execution of 'binaryname' by process /bin/bash (Process Id: 1580, User: root).
```

**Attempt to execute an unsolidified #! script**

When a user tries to execute an unsolidified (unauthorized) #! script, its execution fails and the following message is displayed:

```
bad interpreter: Permission denied
```

The following Event Log entry is generated:

```
McAfee Solidifier prevented unauthorized execution of 'scriptname' by process /bin/bash (Process Id: 928, User: root).
```
Only supported programs can be installed/uninstalled

The Solidifier controls the unauthorized installation/uninstallation of installers.

**Attempt to install a MSI based package**

When an attempt is made to install a MSI based package *Ica32Pkg.msi*, the operation fails and a pop-up window is displayed saying:

**The system administrator has set policies to prevent the installation.**

The following log entry is generated:

```
McAfee Solidifier prevented package modification by 'C:\Documents and Settings\Administrator\Desktop\Ica32Pkg.msi' by user: MYDOMAIN\Administrator.
```

The log shows that the Solidifier prevented the execution of unauthorized code. An error message is displayed in the Event Viewer. No user action is required.

*Note:* The event logs will appear if the package control feature is in enabled state.

**Attempt to uninstall a MSI based package**

When an attempt is made to uninstall a MSI based package *Ica32Pkg.msi*, the operation fails and a pop-up window is displayed saying:

**This installation is forbidden by system policy. Contact your system administrator.**

The following log entry is generated:

```
McAfee Solidifier prevented package modification by 'C:\Documents and Settings\Administrator\Desktop\Ica32Pkg.msi' by user: MYDOMAIN\Administrator.
```

The log shows that the Solidifier prevented the execution of unauthorized code. An error message is displayed in the Event Viewer. No user action is required.

**Attempt to install/uninstall Windows optional components**

When an attempt is made to install/uninstall Windows optional components through Add remove programs, the operation fails and the following Event Log entry is generated:

```
McAfee Solidifier Prevented package modification by 'windows optional component manager' by user: <user_name>
```

The Event Log shows that the Solidifier prevented the execution of unauthorized code. An error message is displayed in the Event Viewer. No user action is required.

*Note:* The event logs will appear if the package control feature is in enabled state.

**Attempt to install an INF based package**

When an attempt is made to install an INF *mmdriver.inf* by right clicking on it, the operation fails and the following Event Log entry is generated:
**McAfee Solidifier prevented package modification by mmdriver.inf by user: MYDOMAIN\Administrator.**

The Event Log shows that the Solidifier prevented the execution of unauthorized code. An error message is displayed in the Event Viewer. No user action is required.

**Note:** The event logs will appear if the package control feature is in enabled state.

### Solidified Programs Cannot Be Tampered With (Windows)

The Solidifier ensures the integrity of the software installed on a solidified system. During normal production usage, solidified program files cannot be modified, renamed, or deleted, even with administrative privileges. Any attempt to modify a solidified file is prevented and an access error is generated instead. Also, Solidifier does not allow you to make changes to its registry files. Solidifier protects its Registry files from any changes made to them in the Enabled Mode.

**Attempt to rename a solidified file**

The rename operation fails and a pop-up window is displayed saying:

*Cannot rename rtlrack: Access is denied.*

Make sure the disk is not full or write-protected and that the file is not currently in use.

The following log entry is generated:

**McAfee Solidifier prevented an attempt to modify file 'C:\rtlrack.exe' by process E:\WINNT\explorer.exe (Process Id: 2984, User: MYDOMAIN\Administrator).**

The log shows that the Solidifier prevented the rename operation. An error message is displayed in the Event Viewer. No user action is required.

**Attempt to move a solidified file.**

The move operation fails and a pop-up window is displayed saying:

*Cannot rename rtlrack: Access is denied.*

Make sure the disk is not full or write-protected and that the file is not currently in use.

The following log entry is generated:

**McAfee Solidifier prevented an attempt to modify file 'C:\rtlrack.exe' by process C:\WINNT\explorer.exe (Process Id: 2984, User: MYDOMAIN\Administrator).**

The log shows that the Solidifier prevented the move operation. An error message is displayed in the Event Viewer. No user action is required.

**Attempt to delete a solidified file**

The delete operation fails and a pop-up window is displayed saying:

*Cannot delete putty: Access is denied.*

Make sure the disk is not full or write-protected and that the file is not currently in use.
The following log entry is generated:

**McAfee Solidifier prevented an attempt to modify file 'C:\putty.exe' by process C:\WINNT\explorer.exe (Process Id: 2984, User: MYDOMAIN\Administrator).**

The log shows that the Solidifier prevented the delete operation. An error message is displayed in the Event Viewer. No user action is required.

**Attempt to overwrite a solidified file**

The operation fails and a pop-up window is displayed saying:

**Cannot copy putty: Access is denied.**
*Make sure the disk is not full or write-protected and that the file is not currently in use.*

The following log entry is generated:

**McAfee Solidifier prevented an attempt to modify file 'C:\putty.exe' by process C:\WINNT\explorer.exe (Process Id: 2984, User: MYDOMAIN\Administrator).**

The log shows that the Solidifier prevented the overwrite (copy) operation. An error message is displayed in the Event Viewer. No user action is required.

**Attempt to add alternate stream for a solidified file**

The operation fails and the following message appears on the sadmin CLI:

**Access is denied.**

The following log entry is generated:

**McAfee Solidifier prevented an attempt to modify file 'C:\virus.exe:hello.exe' by process C:\WINNT\system32\CMD.EXE (Process Id: 2984, User: MYDOMAIN\Administrator).**

**Attempt to delete alternate stream for a solidified file.**

The operation fails but no message is displayed, although a log entry is generated in the Event Log.

**Attempt to rename a registry key**

The operation fails and a pop-up is displayed saying:

**The Registry Editor cannot rename mykey. Error while renaming value.**

**Attempt to delete a registry key**

The operation fails and a pop-up is displayed saying:

**Cannot create value: Error writing to the registry.**
Solidified Programs Cannot Be Tampered With (UNIX)

The Solidifier ensures the integrity of the software installed on a solidified system. During normal production usage, solidified program files cannot be modified, renamed, or deleted, even with administrative privileges. Any attempt to modify a solidified file is prevented and an access error is generated instead.

Attempt to move a solidified file

The move operation fails and a message is displayed as shown below:

mv: cannot move ‘filename’ to ‘filename1’: Permission denied

The following Event Log entry is generated:

McAfee Solidifier prevented an attempt to modify file ‘filename’ by process /bin/mv (Process Id: 1472, User: root).

Attempt to delete a solidified file

The delete operation fails and a message is displayed as shown below:

rm: cannot remove ‘filename’: Permission denied

The following Event Log entry is generated:

McAfee Solidifier prevented an attempt to modify file ‘filename’ by process /bin/rm (Process Id: 1472, User: root).

Attempt to overwrite a solidified file

The operation fails and a message is displayed as shown below:

cp: cannot create regular file ‘filename’: Permission denied

The following Event Log entry is generated:

McAfee Solidifier prevented an attempt to modify file ‘filename’ by process /bin/cp (Process Id: 1472, User: root).

Vulnerabilities in Solidified Programs Cannot Be Exploited (Windows)

The Solidifier ensures the integrity of the running processes using a feature called Memory Protection. Once a process starts to execute, there may be cases where a software error, such as lack of bounds checking, creates a vulnerability that can be exploited to inject new code and cause buffer overflow. In an unprotected system, injected code can execute and take complete control of the computer. The Solidifier prevents the injected code from doing so. In cases of code injection, the attempted injection itself (such as overflowing a buffer and rewriting the stack) precludes further execution of the authorized code in the process and a log entry is generated for it. The Solidifier halts the execution of the process before the injected code can damage the
computer, or the damaged code executes in a random and potentially harmful manner. It generates the following log message:

McAfee Solidifier detected an attempt to exploit process `<process-name>` from address `<return-addr>`.

**Note:** Log generation is not guaranteed for all exploits. Event Logs may not be generated for all such hijacking attempts even though all the exploits will be terminated.
Appendix: Command Quick Reference

The sadmin utility enables system administrators to perform initialization, maintenance, and monitoring operations from the Windows command line interface. The usage of the commands is sadmin command [command-arguments]...

This chapter discusses the syntax and usage of the sadmin commands. The sadmin commands are divided into two categories: basic sadmin command and advanced sadmin commands.

All basic commands can be viewed using the help command and all advanced commands can be viewed using the help-advanced command. The sadmin CLI commands are case in-sensitive. The commands can be issued in upper, lower and mixed case.

<table>
<thead>
<tr>
<th>Command</th>
<th>Parameters</th>
<th>Description and usage note</th>
<th>Required server state or mode to execute command</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>begin-update (bu)</td>
<td>sadmin bu [work-flow id [comment]]</td>
<td>This command starts the Update Mode</td>
<td>Enabled Mode and Disabled Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>disable</td>
<td>N/A</td>
<td>This command disables McAfee Solidifier</td>
<td>Enabled Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>enable</td>
<td>N/A</td>
<td>This command enables McAfee Solidifier</td>
<td>Disabled Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>end-update (eu)</td>
<td>sadmin eu</td>
<td>This command ends the Update Mode</td>
<td>Update Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>help</td>
<td></td>
<td>This command displays help for basic commands</td>
<td>Any Mode</td>
<td></td>
</tr>
<tr>
<td>help-advanced</td>
<td></td>
<td>This command displays help for advanced commands</td>
<td>Any Mode</td>
<td></td>
</tr>
<tr>
<td>license</td>
<td>sadmin license add licensekey</td>
<td>This command adds the license and also helps you to view the licenses installed on the system.</td>
<td>Disabled Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>monitor (mon)</td>
<td>sadmin monitor file [-e</td>
<td>-i</td>
<td>-r] [FILE</td>
<td>DIRECTORY</td>
</tr>
</tbody>
</table>

Table 1: McAfee Solidifier Administration Command Reference
<table>
<thead>
<tr>
<th>Command</th>
<th>Parameters</th>
<th>Description and usage note</th>
<th>Required server state or mode to execute command</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sadmin monitor</td>
<td>procexec [ -e</td>
<td>-i</td>
<td>-r] [PROCESS-NAME] ... ]</td>
<td>This command sets new password and enables password protection</td>
</tr>
<tr>
<td></td>
<td>sadmin monitor list</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sadmin monitor flush</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>passwd</td>
<td>sadmin passwd [-d]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>solidify (so)</td>
<td>sadmin solidify [-q</td>
<td>-v] [filename</td>
<td>directoryname</td>
<td>volumename]</td>
</tr>
<tr>
<td></td>
<td>sadmin solidify [-q</td>
<td>-v] [filename</td>
<td>directoryname</td>
<td>volumename]</td>
</tr>
<tr>
<td>status</td>
<td>sadmin status [volume]</td>
<td>This status command displays the current status of the Solidifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>trusted</td>
<td>sadmin trusted [-e</td>
<td>-i</td>
<td>-r] volumemname / pathname ...</td>
<td>This command includes, excludes, removes, lists or flushes trusted volumes or pathnames</td>
</tr>
<tr>
<td></td>
<td>sadmin trusted -l</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sadmin trusted -f</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>unsolidify</td>
<td>sadmin unsolidify [filename ... ]</td>
<td>This command unsolidifies all supported files</td>
<td>Any Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>(unso)</td>
<td>sadmin unsolidify [filename ... ]</td>
<td>This command unsolidifies all supported files</td>
<td>Any Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>updaters</td>
<td>sadmin updaters add [-d] [-n] [-t ruleid] [-l libraryname] exename</td>
<td>This command enables you to add, list or remove authorized updaters</td>
<td>Any Mode</td>
<td>Basic</td>
</tr>
<tr>
<td></td>
<td>sadmin updaters list</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sadmin updaters remove [-l libraryname] exename</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sadmin updaters remove [-p parent-exe-name] exename</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>sadmin updaters flush</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>version</td>
<td>N/A</td>
<td>This command displays the version of the Solidifier</td>
<td>Any Mode</td>
<td>Basic</td>
</tr>
<tr>
<td>attr</td>
<td>sadmin attr add [-a</td>
<td>-b</td>
<td>-c</td>
<td>-d</td>
</tr>
<tr>
<td></td>
<td>sadmin attr remove [-a</td>
<td>-b</td>
<td>-c</td>
<td>-d</td>
</tr>
<tr>
<td></td>
<td>sadmin attr list [-a</td>
<td>-b</td>
<td>-c</td>
<td>-d</td>
</tr>
<tr>
<td></td>
<td>sadmin attr flush [-a</td>
<td>-b</td>
<td>-c</td>
<td>-d</td>
</tr>
<tr>
<td>Command</td>
<td>Parameters</td>
<td>Description and usage note</td>
<td>Required server state or mode to execute command</td>
<td>Type</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>check</td>
<td>sadmin check [-r] [filename</td>
<td>directoryname</td>
<td>volumename]...</td>
<td>This command checks the consistency of the specified file set. If no file set is specified this command checks all volumes. The command will check the file on disk with the stored file checksum, etc in inventory.</td>
</tr>
<tr>
<td>config</td>
<td>sadmin config export filename sadmin config import [-a] filename sadmin config set NAME=VALUE sadmin config show</td>
<td>This command is used to export configuration of the Solidifier installation to a described disk file or import the configuration from the described file.</td>
<td>Any Mode</td>
<td>Advanced</td>
</tr>
</tbody>
</table>
| diag             | sadmin diag fix [-f] | This command determines interoperability configuration for programs on the system.  
fix - Applies the configuration.  
-f Force the 'fix' for restricted programs. | Enabled and Update Mode | Advanced |
<p>| event            | sadmin event sink [eventname] sadmin event sink [-a]-[-i] eventname | ALL sinkname | ALL | This command displays the list of events and their sink configuration. | Any Mode | Advanced |
| features         | sadmin features [enable | disable] featurename sadmin features list | This command allows you to enable, disable or display the list of Solidifier features. | Any Mode | Advanced |
| list-solidified  | sadmin list-solidified [-l] [filename | directoryname | volumename] ... | This command displays the list of solidified files. List of all the directories and volumes can also be displayed using this command. When no file-sets are supplied, this command will list all the solidified items in inventory. | Any Mode | Advanced |
| list-unsolidified| sadmin lu [filename | directoryname | volumename]... | This command displays the list of unsolidified files. | Any Mode | Advanced |
| lockdown         | N/A        | This command disables the Local CLI.                                                                                                                                                                                   | Any Mode | Advanced |
| read-protect     | sadmin read-protect [-e -i -r] pathname ... sadmin read-protect -i sadmin read-protect -f | This command allows you to use the deny-read feature. | Any mode | Advanced |
| recover          | sadmin recover | This command enables a local administrator to recover the Local CLI.                                                                                                                                              | Any Mode | Advanced |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Parameters</th>
<th>Description and usage note</th>
<th>Required server state or mode to execute command</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>write-protect (wp)</td>
<td>`sadmin write-protect [-e</td>
<td>+l</td>
<td>-r ] pathname ...<code>&lt;br&gt;</code>sadmin write-protect -l<code>&lt;br&gt;</code>sadmin write-protect -f`</td>
<td>This command adds the supplied file or directory or a volume to inventory and write-protects it.</td>
</tr>
<tr>
<td>write-protect-reg (wpr)</td>
<td>`sadmin write-protect-reg [-e</td>
<td>+l</td>
<td>-r ] [registry-key] ...<code>&lt;br&gt;</code>sadmin write-protect-reg -l<code>&lt;br&gt;</code>sadmin write-protect-reg -f`</td>
<td>This command allows you to use the deny-write feature.</td>
</tr>
</tbody>
</table>
Appendix: Diagnostic Tools

<table>
<thead>
<tr>
<th>Utility name</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScAnalyzer</td>
<td>Discover the run-time characterization of a system and whether pre-requisites for deploying the Solidifier are met</td>
</tr>
<tr>
<td>GatherInfo</td>
<td>Gather diagnostic data from logs and the Solidifier File Inventory</td>
</tr>
<tr>
<td>Finetune (Windows only)</td>
<td>Update the configuration to permit selected COTS Auto-Updaters to continue to function</td>
</tr>
</tbody>
</table>

ScAnalyzer

ScAnalyzer is a lightweight deployment utility which is used by field engineers, or professional services personnel, for characterizing a host’s run-time environment, and discovering whether the host satisfies the pre-requisites for installing Solidifier. The run-time characterization includes:

- Operating system version
- Service pack level
- Processor and memory configuration
- Installed applications
- Installed Hot fixes
- Installed services
- System devices
- List of running processes
- List of open network ports: It is run once before and once more after Solidifier is installed to discover differences in the run-time characterization and address them if necessary.

When ScAnalyzer is executed, it compares the software installed on the system with an internal, prepackaged check list for creating a file named `scanalysis.bat`, which lists all programs that Auto-Updaters and exceptions for bypassing the stringent API validation checks. This file can be edited by the user for further customization. This file should be used for effecting configuration changes for the Solidifier.

This tool is located in the default installation folder for the Solidifier, `C:\Program Files\McAfee\Solidcore\Tools\ScAnalyzer`. 
Usage and Interpretation (Windows)

To run the tool, issue the following command:

```s3> scanalyzer```

The following parameters can be used with this command:

- `-h` Displays help for using ScAnalyzer
- `-v` Displays version of ScAnalyzer
- `[-c <checklist>]` Detects if any of the application in the checklist is installed on the system
- `-d` Compares difference in running services, processes and open ports in two ScAnalyzer reports
- `-o <output file>` Writes the output to the output file. If no file is specified output is printed on console
- `-s <scan_file>` Detects if any of the application in the checklist is present in the ScAnalyzer report
- `-q` Runs the ScAnalyzer in quiet mode
- `-n` No time stamp is added in output file name

On executing the ScAnalyzer tool, the `data\scan<machine_name>_<date>_<time>.txt` file is generated in the current working directory.

Usage and Interpretation (UNIX)

The ScAnalyzer tool is available in `<install-dir>/mcafee/solidcore/tools/scanalyzer/` folder. Issue the following command to run the tool:

```#/scanalyzer.sh```

The following parameters can be used with this command:

- `-h` or `--help` Displays help for using ScAnalyzer
- `-v` or `--version` Displays version of ScAnalyzer
- `-d <rep1 rep2>` Compare differences in two ScAnalyzer reports
- `-r <install path>` Path for disk space check
- `-o [output file]` Writes the output to the output file. If no file is specified, output is displayed on the screen.
-q Runs ScAnalyzer in quiet mode
-n No time stamp is added in output file name

On executing the ScAnalyzer tool, the data/report=<machine_name>-<date>_<time> file is generated in the current working directory.

**Manual Review of ScAnalyzer Reports (Windows)**

A manual review of the ScAnalyzer report should check the following:

- Check OS Version and Service pack level for supported versions.
- The existence of Hot Fixes that are pre-requisites for the Solidifier should be verified, and applied, when necessary.
- Certain applications such as Anti Virus update their code when they run. The ScAnalyzer output should be checked for these applications so at the system configuration can be changed to register them as Auto-Updaters.

**GatherInfo**

This utility gathers information related to log files, inventory, version, system state, etc. needed by a Technical Support Engineer to troubleshoot field issues. It is shipped as a part of the Solidifier product and is installed in the Solidifier installation directory.

*Note:* The GatherInfo utility collects logs only from the installation directory path as well as from the changed location.

This tool is located in the default installation folder for the Solidifier, "C:\Program Files\McAfee\Solidcore\Tools\GatherInfo."

**Usage and Interpretation (Windows)**

To run the tool, issue the following command:

*S3> gatherinfo*

The following parameters can be used with this command:

- **-h** Displays help for using GatherInfo
- **-v** Displays version of GatherInfo
- **-q** Gathers logs in quiet mode
- **-x** Excludes security logs collection

On executing the GatherInfo tool, the gatherinfo.zip file is generated in the current working directory. These logs can be used to identify the most common support issues.
Usage and Interpretation (UNIX)

The GatherInfo tool is available in <install-dir>/mcafee/solidcore/tools/gatherinfo/ folder. Issue the following command to run the tool:

# ./gatherinfo.sh

The following parameters can be used with this command:

- **-h or --help**  Displays help for using GatherInfo
- **-v or --version**  Displays version of GatherInfo
- **-c <core-file> or --core <core-file>**  Use this core file for getting backtrace
- **-q**  Gathers logs in quiet mode
- **-n**  No time stamp is added in output file name

On executing the GatherInfo tool, the gatherinfo-<machine_name>-<date>_<time>.tar.gz file is generated in the current working directory. These logs can be used to identify the most common support issues.

Finetune

Please see “Configuring Solidifier-certified Auto-Updaters”.
Appendix: Secure Signed Updates Reference

An administrator can install new software, or patches/updates on a solidified system without entering Update Mode provided the installer is a digitally signed file and its certificate is present in Solidifier Certificates store.

If the installation is to be performed by means of an .msi, only the signed .msi files would be allowed to install on a solidified system.

The primary consumers for this method of performing updates are the manufacturers who embed the Solidifier in their system, e.g., ATM manufacturers, storage system manufacturers, Point-Of-Sale systems manufacturers, etc. However, this method for performing updates can also be used within a commercial Enterprise also. Effectively, the administrator can execute an unsolidified program code on a solidified system provided that it is specially signed.

The signing process is made secure using the public-private key cryptographic technique for the validation of signed files. A private key is used for signing an executable file. The public key corresponding to that private key must be present on the solidified system in the Certificates directory under the Solidifier install directory.

Any signed file that has a valid public key certificate installed on the system is allowed to execute. The behavior of the validated signed installer is similar to that of an updater on the system.

By default, the Secure Signed Update Feature is enabled.

Perform the following steps to declare a signed installer to Solidifier:

1. Execute the following command on signed installer file (at the command prompt):

   ```
   > <ss-install-dir>\tools\scgetcerts.exe <sourcefile/sourcedirectory name> <destination-directory-name> -O
   ```

   Here sourcefile/sourcedirectory is the full path name of the source file or directory. If directory is specified, certificates will be extracted from all the files in this path.

   scgetcerts.exe utility can extract certificate from a code file. This utility can run on any machine whether solidified or not.

   The step extracts the certificate for the signed installer file to the destination directory name specified by the user.

   To see detail usage of scgetcerts execute the following command

   ```
   > <ss-install-dir>\tools\scgetcerts.exe
   ```
2. Add the extracted certificate file to Solidifier Certificate store (the <ss-install-dir>/Certificates folder) by executing the following command (at the Solidifier command-line):

   **S3> sadmin cert add CERTFILE**

   Here, the CERTFILE is the extracted certificate.

3. Execute the signed installer file that is now accepted as a signed updater.

   Use the following command to remove a certificate from Solidifier Certificate store:

   **S3> sadmin cert remove CERTFILE**

   Use the following command to list the Certificates available in Solidifier Certificate store:

   **S3> sadmin cert list**
Appendix: Advanced Configuration parameters

Displaying Configuration parameters

You can display a list of the configuration parameters using the following command:

\texttt{> sadmin config show}

After this command completes successfully, the following message is displayed at the command prompt:

**For Windows**

- \texttt{EventCacheSize} 2 (0x2)
- \texttt{EventCacheWMHigh} 90 (0x5a)
- \texttt{EventCacheWMLow} 70 (0x46)
- \texttt{FailSafeConf} 0 (0x0)
- \texttt{* FeaturesEnabled} 8935410997087 (0x8206fff975f)
- \texttt{* FeaturesEnabledOnReboot} 8935410997087 (0x8206fff975f)
- \texttt{* FeaturesInstalled} 9562006683889 (0x8b2540300f1)
- \texttt{FileAttrCTrack} 5042 (0x13b2)
- \texttt{* FileDenyReadOptions} 1024 (0x400)
- \texttt{* FileDenyWriteOptions} 4831 (0x12df)
- \texttt{HeartbeatInterval} 2 (0x2)
- \texttt{HeartbeatTimeout} 120 (0x78)
- \texttt{* LockdownStatus} 0 (0x0)
- \texttt{LogFileNum} 4 (0x4)
- \texttt{* LogFilePath} C:\Program Files\McAfee\Solidcore\Logs
- \texttt{LogFileSize} 2048 (0x800)
- \texttt{MobilityIntervalMax} 30 (0x1e)
- \texttt{MobilityIntervalMin} 5 (0x5)
- \texttt{MobilityResponseTimeout} 10 (0xa)
- \texttt{MobilityState} 0 (0x0)
- \texttt{Proxy} NULL
- \texttt{* RTEMode} 0 (0x0)
- \texttt{* RTEModeOnReboot} 0 (0x0)
- \texttt{SCAddress1} NULL
- \texttt{SCAddress2} NULL
- \texttt{SCPort} 5125 (0x1405)
- \texttt{SCUUID} NULL
- \texttt{SSTag} NULL
- \texttt{* WorkFlowId} None

**For UNIX**

- \texttt{* ChecksumType} 2 (0x2)
- \texttt{HeartbeatTimeout} 120 (0x78)
- \texttt{EventCacheSize} 2 (0x2)
- \texttt{EventCacheWMHigh} 90 (0x5a)
- \texttt{EventCacheWMLow} 70 (0x46)
- \texttt{FailSafeConf} 0 (0x0)
- \texttt{* FeaturesInstalled} 16889258039 (0x1035010037)
* FeaturesEnabled: 16620757031 (0x1025000027)
* FeaturesEnabledOnReboot: 16620757031 (0x1025000027)
* FileDenyWriteOptions: 735 (0x2df)
* FileDenyReadOptions: 735 (0x2df)
* FileAttrCTrack: 4912 (0x1330)
* HeartbeatInterval: 2 (0x2)
* LockdownStatus: 0 (0x0)
* LogFileNum: 4 (0x4)
* LogFilePath: /var/log/mcafee/solidcore
* LogFileSize: 2048 (0x800)
* MobilityState: 0 (0x0)
* MobilityIntervalMin: 5 (0x5)
* MobilityIntervalMax: 30 (0x1e)
* MobilityResponseTimeout: 10 (0xa)
* RTEMode: 0 (0x0)
* RTEModeOnReboot: 0 (0x0)
* SCAddress1: NULL
* SCAddress2: NULL
* SCPort: 5125 (0x1405)
* SCUUID: NULL
* SSTag: NULL
* WorkFlowId: None

**Note:** All the parameter names preceded by * cannot be configured by the administrator. The usage and steps to configure the rest of the parameters have been discussed in the relevant sections of this document.

The following table shows the configurable parameter names, their default values and the values within which it can be configured.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Default value</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HeartbeatTimeout</td>
<td>120 (0x78)</td>
<td>(\geq 0 \text{ and } \leq 600)</td>
</tr>
<tr>
<td>EventCacheSize</td>
<td>2 (0x2)</td>
<td>(&gt; 0 \text{ and } &lt; \text{MAX_INT32})</td>
</tr>
<tr>
<td>EventCacheWMHigh</td>
<td>90 (0x5a)</td>
<td>((&gt; 50 \text{ and } &lt; 100) &amp; (\text{&gt; EventCacheWMLow}))</td>
</tr>
<tr>
<td>EventCacheWMLow</td>
<td>70 (0x46)</td>
<td>((&gt; 20 \text{ and } \text{&lt; EventCacheWMHigh}))</td>
</tr>
<tr>
<td>FailSafeConf</td>
<td>0 (0x0)</td>
<td>0 or 1</td>
</tr>
<tr>
<td>HeartbeatInterval</td>
<td>2 (0x2)</td>
<td>(\geq 0 \text{ and } \leq 600)</td>
</tr>
<tr>
<td>LogFileNum</td>
<td>4 (0x4)</td>
<td>(\geq 0 \text{ and } \leq \text{MAX_INT})</td>
</tr>
<tr>
<td>LogFileSize</td>
<td>2048 (0x800)</td>
<td>(\geq 0 \text{ and } \leq \text{MAX_INT})</td>
</tr>
<tr>
<td>MobilityState</td>
<td>0 (0x0)</td>
<td>0 or 1</td>
</tr>
<tr>
<td>MobilityIntervalMin</td>
<td>0 (0x0)</td>
<td>((&gt; 5 \text{ and } \text{&lt; MobilityIntervalMax}))</td>
</tr>
<tr>
<td>MobilityIntervalMax</td>
<td>0 (0x0)</td>
<td>((&gt; 30 \text{ and } \text{&gt; mobility interval min and } \text{&lt; MAX_INT32}))</td>
</tr>
<tr>
<td>MobilityResponseTimeout</td>
<td>0 (0x0)</td>
<td>((&gt; 10 \text{ and } \text{&lt; MAX_INT32}))</td>
</tr>
</tbody>
</table>
### Parameter Name

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Default value</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCAddress1</td>
<td>NULL</td>
<td>SC IP address</td>
</tr>
<tr>
<td>SCAddress2</td>
<td>NULL</td>
<td>Secondary SC IP address</td>
</tr>
<tr>
<td>SCPort</td>
<td>5125 (0x1405)</td>
<td>(1-65534)</td>
</tr>
<tr>
<td>SCUUID</td>
<td>NULL</td>
<td>Auto generated</td>
</tr>
<tr>
<td>SSTag</td>
<td>NULL</td>
<td>Valid Host name</td>
</tr>
</tbody>
</table>

### Modifying the value of configuration parameters

The value of the configuration parameters can be modified depending upon the requirements. The syntax to modify the value of the configuration parameters is given below:

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

The ‘NAME’ signifies the configuration parameter name. The ‘VALUE’ refers to the new value of the configuration parameter that is going to be applicable after the change.
Appendix: Solidifier feature list

Displaying Solidifier features

You can view the complete list of Solidifier features using the following command:

S3> sadmin features list

After this command completes successfully, the following message is displayed at the command prompt:

For Windows (x86)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>anti-debugging</td>
<td>Disabled</td>
</tr>
<tr>
<td>app-control</td>
<td>Enabled</td>
</tr>
<tr>
<td>app-control-dsr</td>
<td>Enabled</td>
</tr>
<tr>
<td>app-control-installer-detect</td>
<td>Enabled</td>
</tr>
<tr>
<td>checksum</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec-dlls</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec-drivers</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec-exes</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-read</td>
<td>Disabled</td>
</tr>
<tr>
<td>deny-write</td>
<td>Enabled</td>
</tr>
<tr>
<td>discover-updaters</td>
<td>Enabled</td>
</tr>
<tr>
<td>integrity</td>
<td>Enabled</td>
</tr>
<tr>
<td>inv-deferred-update</td>
<td>Enabled</td>
</tr>
<tr>
<td>mon</td>
<td>Disabled</td>
</tr>
<tr>
<td>mon-file</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mon-fattr</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mon-proc-exec</td>
<td>Disabled</td>
</tr>
<tr>
<td>mon-reg</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mon-uat</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mp</td>
<td>Enabled</td>
</tr>
<tr>
<td>mp-casp</td>
<td>Enabled</td>
</tr>
<tr>
<td>mp-mangling</td>
<td>Disabled</td>
</tr>
<tr>
<td>mp-decoy</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mp-decoy-reorder</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mp-syscall-bktrk</td>
<td>Disabled</td>
</tr>
<tr>
<td>mp-vasr</td>
<td>Disabled</td>
</tr>
<tr>
<td>mp-vasr-randomization</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mp-vasr-rebasing</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mp-vasr-relocation</td>
<td>Disabled*</td>
</tr>
<tr>
<td>network-tracking</td>
<td>Enabled</td>
</tr>
<tr>
<td>pkg-ctrl</td>
<td>Disabled</td>
</tr>
<tr>
<td>popups</td>
<td>Enabled</td>
</tr>
<tr>
<td>script-auth</td>
<td>Enabled</td>
</tr>
<tr>
<td>signing</td>
<td>Enabled</td>
</tr>
<tr>
<td>signing-fic</td>
<td>Enabled</td>
</tr>
<tr>
<td>ssl</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
For Windows (x64)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>app-control</td>
<td>Enabled</td>
</tr>
<tr>
<td>app-control-dsr</td>
<td>Enabled</td>
</tr>
<tr>
<td>app-control-installer-detect</td>
<td>Enabled</td>
</tr>
<tr>
<td>checksum</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec-dlls</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec-drivers</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec-exes</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-read</td>
<td>Disabled</td>
</tr>
<tr>
<td>deny-write</td>
<td>Enabled</td>
</tr>
<tr>
<td>discover-updaters</td>
<td>Enabled</td>
</tr>
<tr>
<td>integrity</td>
<td>Enabled</td>
</tr>
<tr>
<td>inv-deferred-update</td>
<td>Enabled</td>
</tr>
<tr>
<td>mon</td>
<td>Disabled</td>
</tr>
<tr>
<td>mon-file</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mon-fattr</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mon-proc-exec</td>
<td>Disabled</td>
</tr>
<tr>
<td>mon-reg</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mon-uat</td>
<td>Disabled*</td>
</tr>
<tr>
<td>mp</td>
<td>Enabled</td>
</tr>
<tr>
<td>mp-nx</td>
<td>Enabled</td>
</tr>
<tr>
<td>network-tracking</td>
<td>Enabled</td>
</tr>
<tr>
<td>pkg-ctrl</td>
<td>Disabled</td>
</tr>
<tr>
<td>popups</td>
<td>Enabled</td>
</tr>
<tr>
<td>script-auth</td>
<td>Enabled</td>
</tr>
<tr>
<td>signing</td>
<td>Enabled</td>
</tr>
<tr>
<td>signing-fic</td>
<td>Enabled</td>
</tr>
<tr>
<td>ssl</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Note:** The pkg-ctrl feature is not available on the IA64 architecture.

For UNIX

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>checksum</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-exec</td>
<td>Enabled</td>
</tr>
<tr>
<td>deny-read</td>
<td>Disabled</td>
</tr>
<tr>
<td>deny-write</td>
<td>Enabled</td>
</tr>
<tr>
<td>integrity</td>
<td>Enabled</td>
</tr>
<tr>
<td>mon</td>
<td>Disabled</td>
</tr>
<tr>
<td>mon-file</td>
<td>Disabled</td>
</tr>
<tr>
<td>mon-proc-exec</td>
<td>Disabled</td>
</tr>
<tr>
<td>script-auth</td>
<td>Enabled</td>
</tr>
<tr>
<td>signing</td>
<td>Enabled</td>
</tr>
<tr>
<td>signing-fic</td>
<td>Enabled</td>
</tr>
<tr>
<td>ssl</td>
<td>Enabled</td>
</tr>
</tbody>
</table>