SIEMENS

http://support.automation.siemens.com/WW/view/en/89027076

# 1 Preface

### Purpose of the documentation

This documentation describes the use of McAfee Application Control in the SINUMERIK PCU 50 environment, the installation as well as the recommended adaptations to the McAfee Application Control after installation.

### Knowledge required

This documentation is intended for persons involved in the configuration, commissioning and servicing of automation systems with SINUMERIK PCU 50. It is assumed that users have the appropriate administration know-how and IT knowledge for Microsoft Windows operating systems.

### Validity of the documentation

The documentation is valid for systems that have been implemented with the particular SINUMERIK PCU 50 product version.

| NOTICE | **Please note, that for McAfee Application Control, the functionality of the whitelisting has only been released for certain product versions. More information on this can be found on the Internet at the following address: http://support.automation.siemens.com**<br>**This documentation only provides a description of the whitelisting functionality** |
|---|---|

# 2 Whitelisting application

## 2.1 Introduction

The use of whitelisting technology on a SINUMERIK PCU with Microsoft Windows XP is only effective if it is part of a comprehensive security concept. Just using whitelisting technology alone cannot protect against hacking attacks.

As a consequence, we recommend that a multi-stage security concept is employed.
In conjunction with additional measures, whitelisting can be seen as an additional security measure, and therefore an additional resource to counteract the increasing risk of attacks.

The basic philosophy of whitelisting is that all applications are mistrusted, unless they have been classified as trustworthy after an appropriate check. This means that a whitelist is maintained in the system. This whitelist therefore contains all applications that have been classified as trustworthy and therefore can be run on the SINUMERIK PCU.

## 2.2 McAfee Application Control

Using McAfee Application Control, unauthorized applications can be blocked on workstations. This means that after installing and activating McAfee Application Control on a computer system, all files that can be executed are protected against changes – and this prevents unknown (i.e. they are not in the whitelist) executable files from being started.

Contrary to basic whitelisting concepts, McAfee Application Control employs a dynamic trustworthiness model. This means that the tedious process of manually updating lists of authorized applications is no longer required. Updates can be incorporated in different ways:

- By trustworthy users
- By trustworthy manufacturers (certificate)
- By a trustworthy directory
- By a binary file
- Using an updater (update program, e.g. WSUS, virus scanners, …)

Before activation, the software scans for executable files and applications, e.g. exe, com, bat, dll, Java, Active-X control elements, scripts etc., on all partitions and all local hard disks. Files found during this scan are signed and authorized by McAfee Application Control for subsequent use. This also includes protection against subsequent changes and modifications, for example, deleting or renaming.

Further, McAfee Application Control has a function that monitors the memory, provides protection against buffer overflow and protects files that run in the memory.

# 3 Use and administration

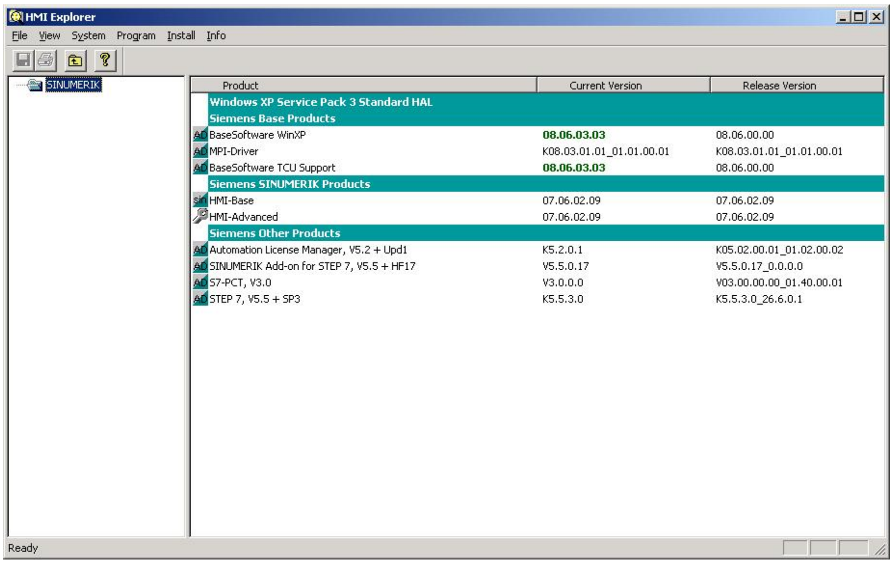
## 3.1 Version / device under test

### Hardware used

The following SINUMERIK software / hardware was subject to a compatibility test:

**PCU 50 V3 1.5GHz Intel Celeron M, 512MB RAM**

- PCU Base 08.06.03.03
- HMI Advanced 07.06.02.09
- Step7 V5.5



| Product | Current Version | Release Version |
|---|---|---|
| **Windows XP Service Pack 3 Standard HAL** | | |
| **Siemens Base Products** | | |
| BaseSoftware WinXP | **08.06.03.03** | 08.06.00.00 |
| MPI-Driver | K08.03.01.01_01.01.00.01 | K08.03.01.01_01.01.00.01 |
| BaseSoftware TCU Support | **08.06.03.03** | 08.06.00.00 |
| **Siemens SINUMERIK Products** | | |
| HMI-Base | 07.06.02.09 | 07.06.02.09 |
| HMI-Advanced | 07.06.02.09 | 07.06.02.09 |
| **Siemens Other Products** | | |
| Automation License Manager, V5.2 + Upd1 | K5.2.0.1 | K05.02.00.01_01.02.00.02 |
| SINUMERIK Add-on for STEP 7, V5.5 + HF17 | V5.5.0.17 | V5.5.0.17_0.0.0.0 |
| S7-PCT, V3.0 | V3.0.0.0 | V03.00.00.00_01.40.00.01 |
| STEP 7, V5.5 + SP3 | K5.5.3.0 | K5.5.3.0_26.6.0.1 |

### Whitelisting software used:

McAfee® Application Control v6.0

- Standalone deployment (Solidifier)

Using the McAfee Application Control Software as example, a description as to how SINUMERIK PCU 50 with Windows XP can be "hardened" is provided. The licensed software can be used with the PCU 50 as a standalone version (Solidifier/Solidcore).

The whitelisting software is directly purchased from the manufacturer.

**Note**

Please observe the manufacturer's information regarding system requirements.

The functionality of the McAfee Application Control must be ensured for the system-specific configurations by carrying out the appropriate tests. The compatibility tests carried out by Siemens does not reflect the exact software environment on the system.

### Additional information

McAfee® Application Control
http://www.mcafee.com/de/resources/data-sheets/ds-application-control.pdf

McAfee® Solidifier Command Line Reference Guide (for Application Control)
https://kb.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23360/en_US/MFE_SO_ALL_RG_CLI_AC_5_1_0.pdf

McAfee® support
https://mysupport.mcafee.com

## 3.2 Installation

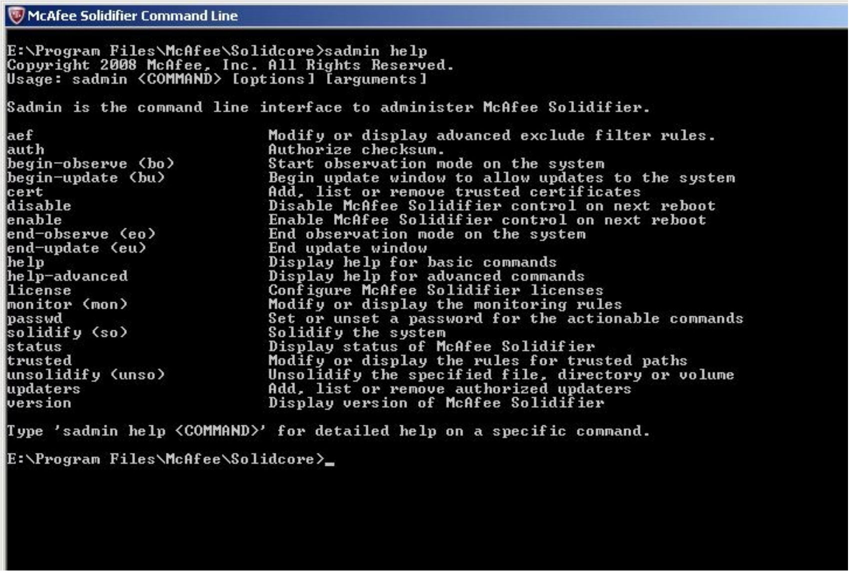
Install the version of McAfee Solidcore that is suitable for your particular operating system. After installation, the icon for the McAfee Solidifier Command Line is displayed on your desktop.

### Hardening and activating

McAfee Solidifier Command Line is started by double-clicking on the icon; it can now be deployed by using the appropriate commands. A detailed list of the commands and functions is provided in the software documentation of the safety product being used, e.g. McAfee Solidifier Command Line Reference Guide (for Application Control).

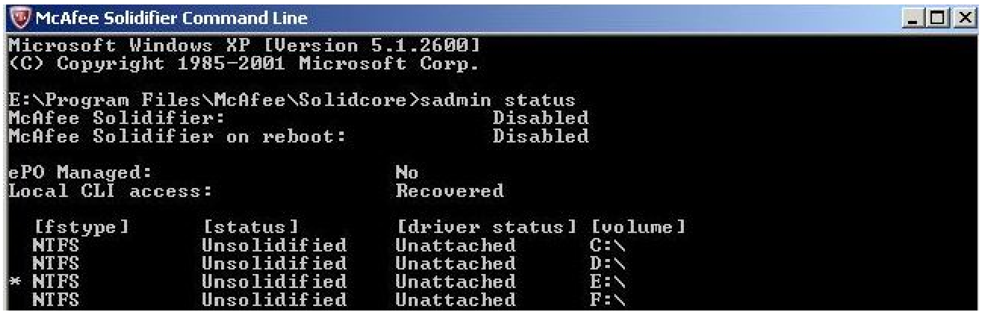
### Basic commands: SADMIN / SADMIN HELP

You can obtain the appropriate help for commands and optional parameters through HELP.



```
E:\Program Files\McAfee\Solidcore>sadmin help
Copyright 2008 McAfee, Inc. All Rights Reserved.
Usage: sadmin <COMMAND> [options] [arguments]

Sadmin is the command line interface to administer McAfee Solidifier.

aef                         Modify or display advanced exclude filter rules.
auth                        Authorize checksum.
begin-observe (bo)          Start observation mode on the system
begin-update (bu)           Begin update window to allow updates to the system
cert                        Add, list or remove trusted certificates
disable                     Disable McAfee Solidifier control on next reboot
enable                      Enable McAfee Solidifier control on next reboot
end-observe (eo)            End observation mode on the system
end-update (eu)             End update window
help                        Display help for basic commands
help-advanced               Display help for advanced commands
license                     Configure McAfee Solidifier licenses
monitor (mon)               Modify or display the monitoring rules
passwd                      Set or unset a password for the actionable commands
solidify (so)               Solidify the system
status                      Display status of McAfee Solidifier
trusted                     Modify or display the rules for trusted paths
unsolidify (unso)           Unsolidify the specified file, directory or volume
updaters                    Add, list or remove authorized updaters
version                     Display version of McAfee Solidifier

Type 'sadmin help <COMMAND>' for detailed help on a specific command.

E:\Program Files\McAfee\Solidcore>_
```

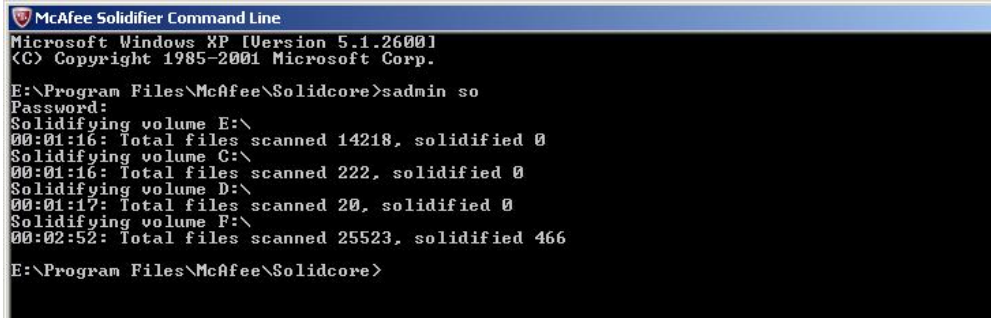
Querying the current status of the whitelisting: **SADMIN STATUS**



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Program Files\McAfee\Solidcore>sadmin status
McAfee Solidifier:                      Disabled
McAfee Solidifier on reboot:            Disabled

ePO Managed:                    No
Local CLI access:               Recovered

  [fstype]      [status]        [driver status] [volume]
  NTFS          Unsolidified    Unattached      C:\
  NTFS          Unsolidified    Unattached      D:\
* NTFS          Unsolidified    Unattached      E:\
  NTFS          Unsolidified    Unattached      F:\
```

Here, it can be seen that the hard disks have still not been hardened (unsolidified) and the function is still disabled.

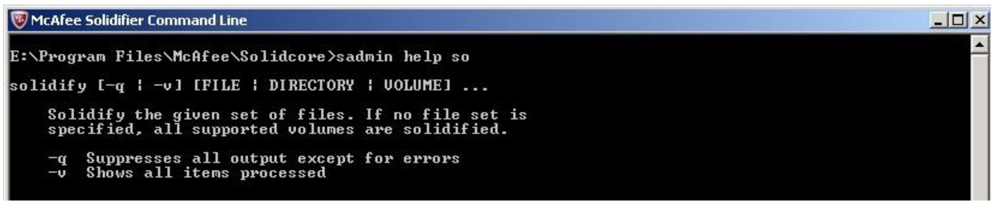
The complete hard disk can be hardened according to standard settings using the **SADMIN SO** command. Depending on the hardware expansion, this may take several minutes. After "solidification" has been completed, in the command line you can see how many files were scanned for each partition or hard disk and how many files were authorized/hardened.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Program Files\McAfee\Solidcore>sadmin so
Password:
Solidifying volume E:\
00:01:16: Total files scanned 14218, solidified 0
Solidifying volume C:\
00:01:16: Total files scanned 222, solidified 0
Solidifying volume D:\
00:01:17: Total files scanned 20, solidified 0
Solidifying volume F:\
00:02:52: Total files scanned 25523, solidified 466

E:\Program Files\McAfee\Solidcore>
```

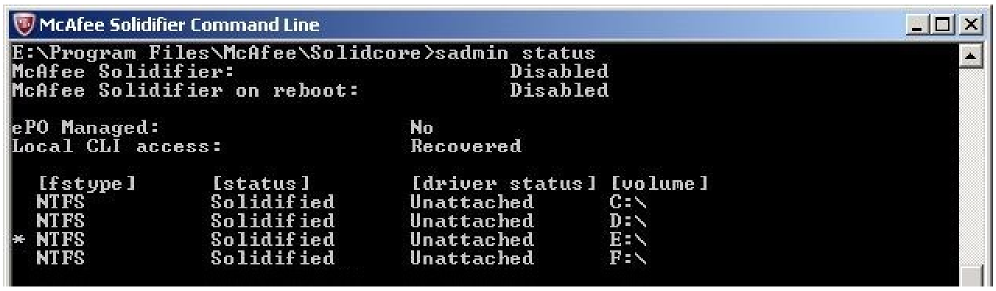
Use command **SADMIN HELP SO** for further options or to harden just individual partitions

You can obtain detailed information about the command here.



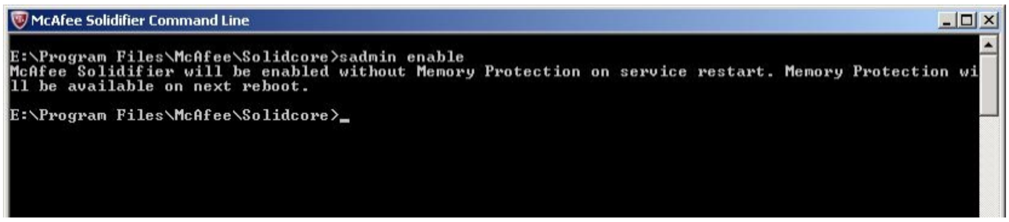
```
E:\Program Files\McAfee\Solidcore>sadmin help so

solidify [-q | -v] [FILE | DIRECTORY | VOLUME] ...

    Solidify the given set of files. If no file set is
    specified, all supported volumes are solidified.

    -q  Suppresses all output except for errors
    -v  Shows all items processed
```

The status can again be queried after hardening has been completed. Here, it can be seen that although the partitions have been hardened, the function is still disabled.



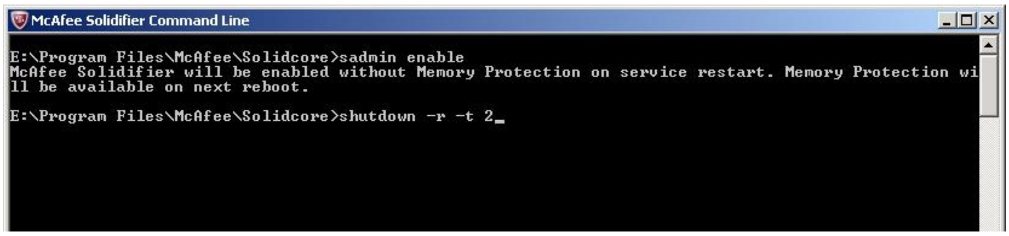
```
E:\Program Files\McAfee\Solidcore>sadmin status
McAfee Solidifier:                          Disabled
McAfee Solidifier on reboot:                Disabled

ePO Managed:                         No
Local CLI access:                    Recovered

  [fstype]      [status]        [driver status] [volume]
  NTFS          Solidified      Unattached      C:\
  NTFS          Solidified      Unattached      D:\
* NTFS          Solidified      Unattached      E:\
  NTFS          Solidified      Unattached      F:\
```

The functionality still has to be activated in order to now activate McAfee Application Control. The command is called: **SADMIN ENABLE**



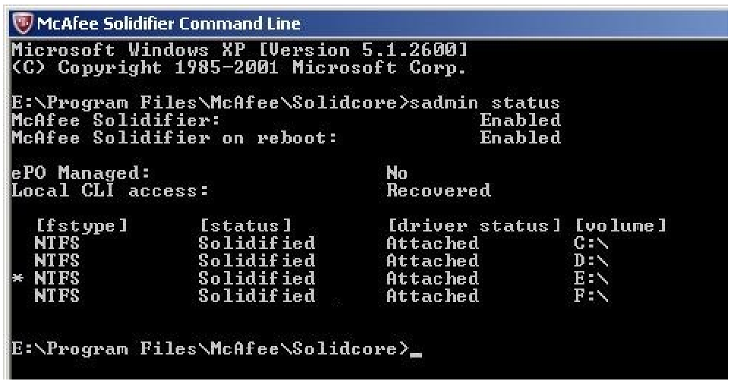
```
E:\Program Files\McAfee\Solidcore>sadmin enable
McAfee Solidifier will be enabled without Memory Protection on service restart. Memory Protection wi
ll be available on next reboot.

E:\Program Files\McAfee\Solidcore>_
```

SINUMERIK PCU must be restarted at the end. This can either be done from the desktop, or forced using Command. In the example shown here, after 2 seconds, the system is run down and restarted.



```
E:\Program Files\McAfee\Solidcore>sadmin enable
McAfee Solidifier will be enabled without Memory Protection on service restart. Memory Protection wi
ll be available on next reboot.

E:\Program Files\McAfee\Solidcore>shutdown -r -t 2_
```

After the system has rebooted, the status can be queried again using the Solidcore Command Line.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Program Files\McAfee\Solidcore>sadmin status
McAfee Solidifier:                          Enabled
McAfee Solidifier on reboot:                Enabled

ePO Managed:                        No
Local CLI access:                   Recovered

  [fstype]      [status]        [driver status] [volume]
  NTFS          Solidified      Attached        C:\
  NTFS          Solidified      Attached        D:\
* NTFS          Solidified      Attached        E:\
  NTFS          Solidified      Attached        F:\

E:\Program Files\McAfee\Solidcore>_
```

The computer system – and the applications and executable files on it – are protected against conscious but also unintentional changes, for example deleting or renaming.

## 3.3 Next steps

You can now use your SINUMERIK PCU as usual. We recommend that you increase the size of the work memory of the SINUMERIK PCU 50 V3 to 4GB RAM for time-critical programs and those requiring a high level of processing performance.

### Deactivating whitelisting

McAfee Application Control must be deactivated to make changes to programs and the system, for example, software updates.
This is done using the **SADMIN DISABLE** command, and just the same as when activating, results in a reboot.

### Password protection

In order to prevent unauthorized deactivation of McAfee Application Control, we recommend that the Solidifier command line is password-protected. This is realized using the **SADMIN PASSWD** command. For a detailed description, please refer to the McAfee Solidifier Command Line Reference Guide for Application Control.

**Note**

Please observe the manufacturer's information regarding system requirements.

The functionality of the McAfee Application Control must be ensured for the system-specific configurations by carrying out the appropriate tests. The compatibility tests carried out by Siemens does not reflect the exact software environment on the system.