FAQ • 02/2014

Application Whitelisting

SINUMERIK PCU 50 mit Windows XP

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

Dieser Beitrag stammt aus dem Siemens Industry Online Support. Es gelten die dort genannten Nutzungsbedingungen (www.siemens.com/nutzungsbedingungen).

Vorsicht

Die in diesem Beitrag beschriebenen Funktionen und Lösungen beschränken sich überwiegend auf die Realisierung der Automatisierungsaufgabe. Bitte beachten Sie darüber hinaus, dass bei Vernetzung Ihrer Anlage mit anderen Anlagenteilen, dem Unternehmensnetz oder dem Internet entsprechende Schutzmaßnahmen im Rahmen von Industrial Security zu ergreifen sind.

Industrial Security

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Inhaltsverzeichnis

1 Vorwort

Zweck der Dokumentation

Diese Dokumentation beschreibt die Verwendung von McAfee Application Control im SINUMERIK PCU 50 Umfeld, die Installation sowie die empfohlenen Anpassungen von McAfee Application Control nach der Installation.

Erforderliche Kenntnisse

Diese Dokumentation wendet sich an Personen, die in den Bereichen Projektierung, Inbetriebnahme und Service von Automatisierungssystemen mit SINUMERIK PCU 50 tätig sind. Administrationskenntnisse und IT-Techniken für Microsoft Windows Betriebssysteme werden vorausgesetzt.

Gültigkeitsbereich der Dokumentation

Die Dokumentation ist gültig für Anlagen, die mit der jeweiligen Produktversion von SINUMERIK PCU 50 realisiert sind.

ACHTUNG	**Beachten Sie, dass bei McAfee Application Control nur die Funktionalität des Whitelisting für bestimmte Produktversionen freigegeben ist. Weitere Informationen hierzu finden Sie im Internet unter folgender Adresse: http://support.automation.siemens.com** **Diese vorliegende Dokumentation beschränkt sich ausschließlich auf die Beschreibung der Funktionalität Whitelisting**

2 Application Whitelisting

2.1 Einleitung

Der Einsatz der Whitelisting-Technologie auf einer SINMERIK PCU mit Microsoft Windows XP ist nur dann effektiv, wenn er Teil eines umfassenden Sicherheitskonzeptes ist. Der alleinige Einsatz der Whitelisting-Technologie kann nicht vor Angriffen schützen.

Wir empfehlen daher den Einsatz eines mehrstufigen Sicherheitskonzeptes. Whitelisting ist im Zusammenhang mit weiteren Maßnahmen als eine zusätzliche Sicherheitsmaßnahme zu sehen und somit ein zusätzliches Mittel, um dem zunehmenden Angriffsrisiko entgegenzuwirken.

Der Ansatz von Whitelisting besteht darin, dass allen Anwendungen (Applikationen) misstraut wird, außer denen, die bei einer Prüfung als vertrauenswürdig eingestuft wurden. D.h. es wird eine Positivliste (weiße Liste, eine sogenannte Whitelist) gepflegt. Diese Positivliste enthält somit die Anwendungen / Applikationen, die sich als unbedenklich eingestuft wurden und somit auf der SINUMERIK PCU ausgeführt werden dürfen.

2.2 McAfee Application Control

Mit McAfee Application Control können nicht autorisierte Anwendungen auf Workstations blockiert werden. D.h. dass nach der Installation und Aktivierung von McAfee Application Control auf einem Computersystem, alle ausführbaren Dateien vor Veränderung geschützt sind und verhindert wird, dass unbekannte (nicht auf der Whitelist vorhandene) ausführbare Dateien gestartet werden können.

Anders als bei einfachen Whitelisting-Konzepten verwendet McAfee Application Control ein dynamisches Vertrauenswürdigkeitsmodell. Damit sind langwierige manuelle Aktualisierungen von Listen genehmigter Anwendungen hinfällig. Aktualisierungen können auf unterschiedliche Weise eingebracht werden:

- durch vertrauenswürdige Benutzer (Benutzer/User)
- durch vertrauenswürdige Hersteller (Zertifikat)
- von einem vertrauenswürdigen Verzeichnis
- durch eine Binärdatei
- mittels Updater (Aktualisierungsprogramme z.B. WSUS, Virenscanner, …)

Die Software führt vor der Aktivierung einen Scan nach ausführbaren Dateien und Anwendungen z.B. exe, com, bat, dll, Java, Active-X-Steuerelemente, Scripts, usw. auf allen Partitionen und alle lokalen Festplatten durch. Die bei diesem Scan gefundenen Dateien werden von McAfee Application Control für eine spätere Verwendung signiert und autorisiert. Dies beinhaltet auch den Schutz vor nachträglicher Änderung wie z.B. Löschen oder Umbenennen.

Des Weiteren bringt McAfee Application Control eine Funktion mit, die den Speicher überwacht, einen Schutz vor Buffer Overflow hat und Dateien schützt, die im Speicher laufen.

3 Verwendung und Administration

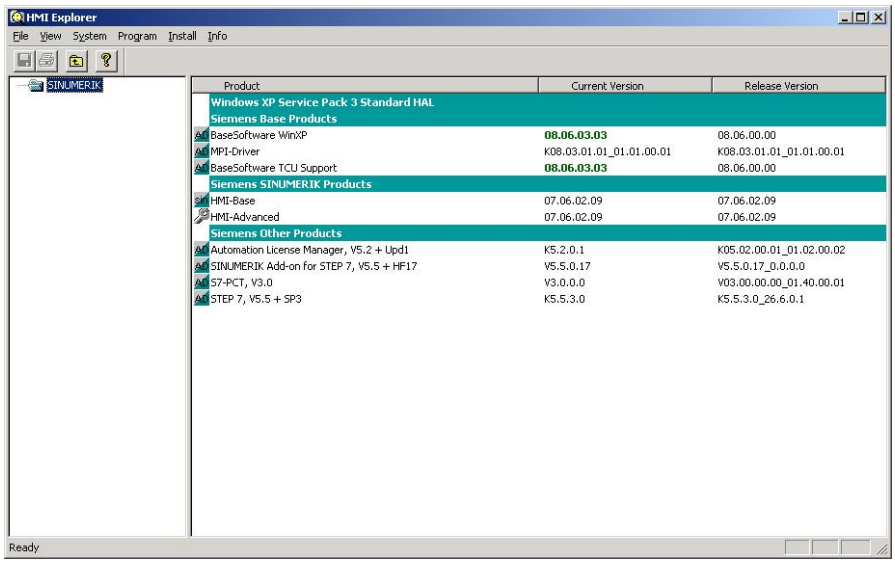
3.1 Version / Device under Test

Eingesetzte Hardware

Es wurde folgende SINUMERIK Software / Hardware auf Verträglichkeit getestet:

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



Eingesetzte Whitelisting-Software

McAfee® Application Control v6.0

- Stand-alone Deployment (Solidifier)

Am Beispiel der Software McAfee Application Control wird beschrieben, wie eine „Härtung“ der SINUMERIK PCU 50 mit Windows XP erfolgen kann. Die lizenzpflichtige Software kann mit der PCU 50 als Stand-alone Variante (Solidifier/Solidcore) benutzt werden.

Der Bezug der Whitelisting-Software erfolgt direkt vom Hersteller.

Hinweis

Bitte beachten Sie die Angaben des Herstellers zu den Systemvoraussetzungen.

Die Funktionsfähigkeit von McAfee Application Control muss auf den anlagenspezifischen Konfigurationen durch Tests abgesichert werden. Der Verträglichkeitstest bei Siemens bildet nicht die genaue Softwareumgebung auf der Anlage nach.

Weiterführende Informationen

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

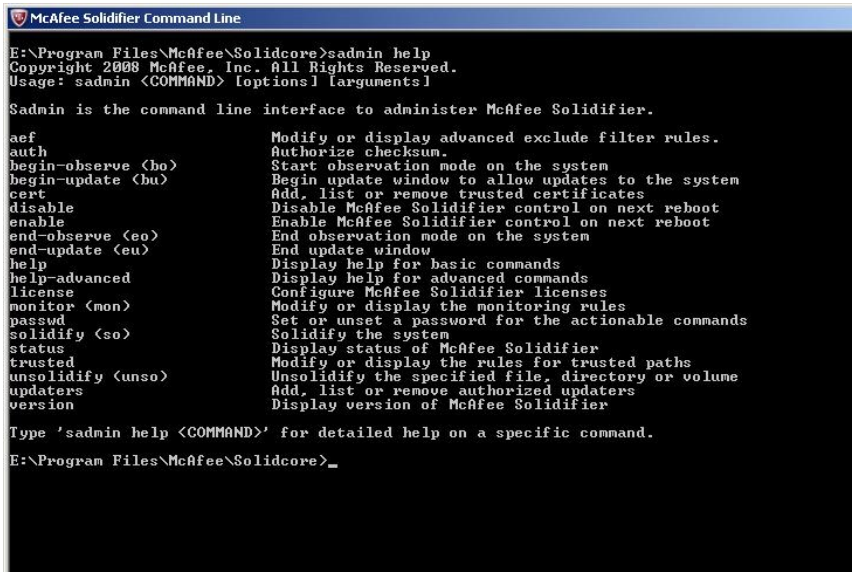
Installieren Sie entsprechend Ihres Betriebssystems die passende Version von McAfee Solidcore. Nach erfolgter Installation erscheint auf dem Desktop das Icon für die McAfee Solidifer Command Line.

Härten und Aktivieren

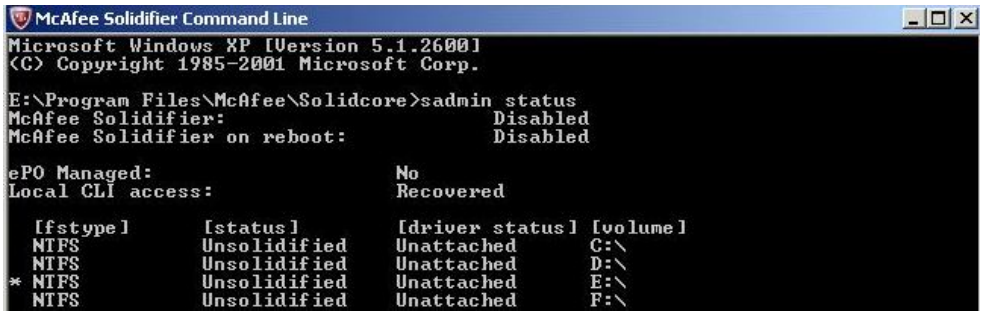
Nach Doppelklick des Icons startet die McAfee Solidifier Command Line, die nun über entsprechende Befehle bedient werden kann. Eine detaillierte Liste der Befehle und Funktionen entnehmen Sie bitte der Softwaredokumentation des eingesetzten Sicherheits-Produktes z.B. McAfee Solidifier Command Line Reference Guide (for Application Control).

Grundbefehle: SADMIN / SADMIN HELP

Über HELP erhalten Sie entsprechende Hilfestellungen zu den Befehlen und optionalen Parametern.

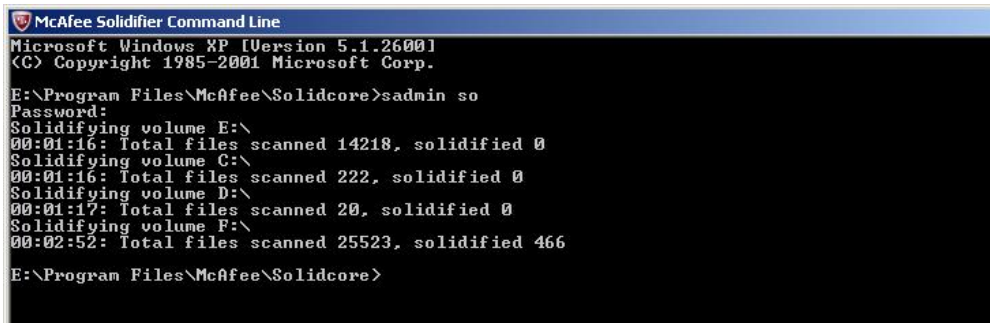


Abfrage des aktuellen Status des Whitelistings: **SADMIN STATUS**



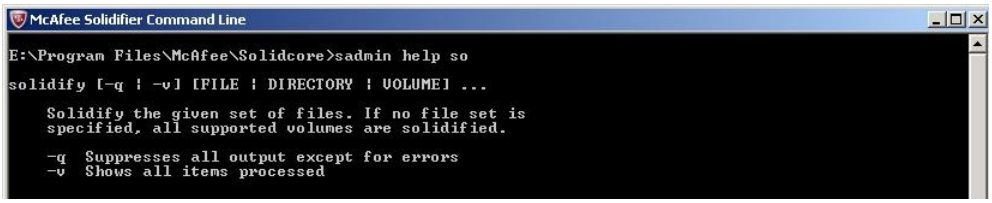
Hier ist zu sehen, dass die Festplatten noch nicht gehärtet/geschützt sind (Unsolidified) und die Funktion generell noch deaktiviert (Disabled) ist.

Über den Befehl **SADMIN SO** kann die komplette Festplatte nach den Standard-einstellungen gehärtet werden. Je nach Hardwareausbau kann dies einige Minuten in Anspruch nehmen. Nach dem Beenden des "Solidifizieren" können Sie in der Commandozeile sehen, wie viel Dateien pro Partition bzw. Festplatte insgesamt gescannt wurden und wie viele Dateien dabei autorisiert/gehärtet wurden.

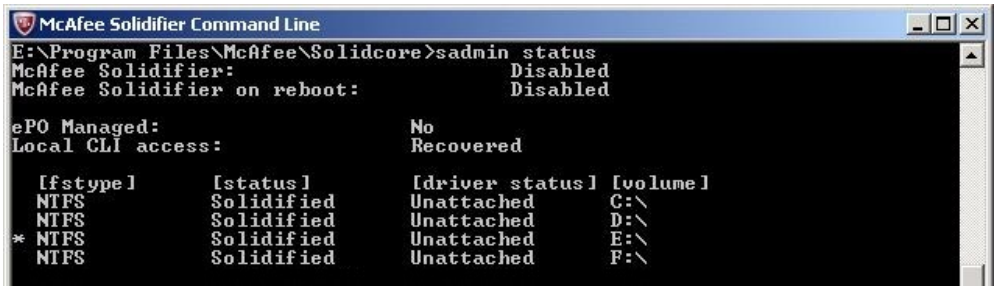


Um weitere Optionen bzw. nur einzelne Partitionen zu härten, benutzen Sie den Befehl **SADMIN HELP SO**

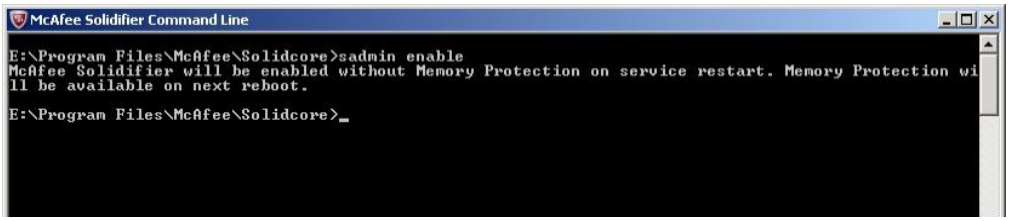
Hier erhalten Sie detaillierte Informationen zu dem Befehl.



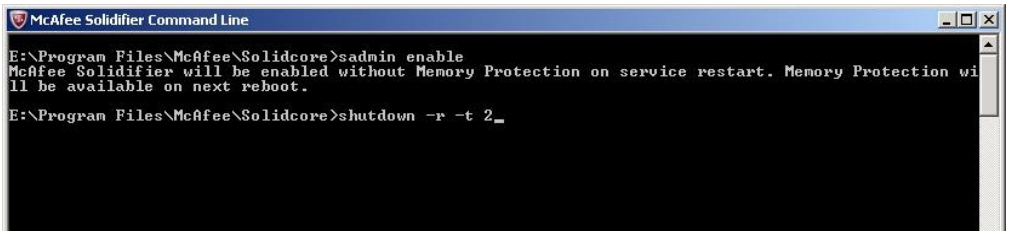
Nach erfolgter Härtung kann der Status erneut abgefragt werden. Es ist zu sehen, dass die Partitionen zwar gehärtet sind, die Funktion aber generell noch deaktiviert (Disabled) ist.



Um die McAfee Application Control nun zu aktivieren, muss die Funktionalität noch aktiviert werden. Der Befehl dazu lautet: **SADMIN ENABLE**



Im Anschluss daran muss die SINUMERIK PCU neu gestartet werden. Dies kann entweder über den Desktop erfolgen oder über den Command-Befehl forciert werden. In hier gezeigten Beispiel wird nach 2 Sekunden das System heruntergefahren und neu gestartet.



Nach erfolgtem Reboot kann über die Solidcore Command Line der Status erneut abgefragt werden.

Das Computersystem und die darauf befindlichen Anwendungen und ausführbaren Dateien sind vor bewussten, aber auch ungewollten Änderungen wie z.B. löschen oder umbenennen geschützt.

3.3 Weiteres Vorgehen

Sie können nun wie gewohnt Ihre SINUMERIK PCU benutzen. Bei rechenintensiven und zeitkritischen Programmen wird empfohlen, den Arbeitsspeicher der SINUMERIK PCU 50 V3 auf 4GB RAM hochzurüsten.

Whitelisting deaktivieren

Um künftig Änderungen an Programmen und dem System z.B. SW-Updates durchzuführen, muss McAfee Application Control wieder deaktiviert werden. Dies erfolgt über den Befehl **SADMIN DISABLE** und hat, wie schon beim Aktivieren, einen Reboot zur Folge.

Passwortschutz

Um unautorisiertes Deaktivieren von McAfee Application Control zu unterbinden, empfehlen wir die Solidifier Kommandozeile mittel Passwort zu schützen. Dies erfolgt über den Befehl **SADMIN PASSWD**. Die detaillierte Beschreibung entnehmen Sie bitte dem McAfee Solidifier Command Line Reference Guide for Application Control.

Hinweis

Bitte beachten Sie die Angaben des Herstellers zu den Systemvoraussetzungen.

Die Funktionsfähigkeit von McAfee Application Control muss auf den anlagenspezifischen Konfigurationen durch Tests abgesichert werden. Der Verträglichkeitstest bei Siemens bildet nicht die genaue Softwareumgebung auf der Anlage nach.