SIMATIC

Process Control System PCS 7 Configuring McAfee Application Control

Commissioning Manual

07/2011

A5E03658595-01

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER
indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING
indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION
with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION
without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE
indicates that an unintended result or situation can occur if the relevant information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E03658595-01
Ⓟ 11/2011

Table of contents

Warning concept

This manual contains information that you must observe for the sake of your own safety and to avoid damage to assets. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol. Notices referring only to equipment damage have no safety alert symbol. Warnings are shown in descending order according to the degree of danger as follows.

⚠ DANGER
Indicates that death or severe personal injury will result if proper precautions are not taken.

⚠ WARNING
Indicates that death or severe personal injury may result if proper precautions are not taken.

⚠ CAUTION
With a safety alert symbol indicates that minor personal injury can result if proper precautions are not taken.

CAUTION
Without a safety alert symbol indicates that damage to property may result if proper precautions are not taken.

NOTICE
Indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

In the event of a number of levels of danger prevailing simultaneously, the warning corresponding to the highest level of danger is always used. A warning with a warning triangle indicating possible injury to personnel may also include a warning relating to property damage.

Qualified personnel

The product/system described in this documentation may only be operated only by personnel qualified for the specific task in accordance with the relevant documentation for the specific task, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be adhered to. The information in the relevant documentation must be observed.

Trademarks

All names shown with the trademark symbol ® are registered trademarks of Siemens AG. Third parties using for their own purposes any other names in this document which refer to trademarks might infringe upon the rights of the trademark owners.

Disclaimer of liability

We have reviewed the content of this manual for agreement with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Preface 1

Purpose of the documentation

This documentation describes the use of McAfee Application Control in the SIMATIC PCS 7 and WinCC environment, including its installation and recommended adjustments after installation.

Knowledge required

This documentation is aimed at persons involved in the engineering, commissioning, and operation of automated systems based on SIMATIC PCS 7 or WinCC. Knowledge of administration and IT techniques for Microsoft Windows operating systems is assumed.

Scope of the documentation

The documentation applies to process control systems equipped with the respective product version of SIMATIC PCS 7, or WinCC.

NOTICE
Note that McAfee Integrity Control has released Whitelisting functionality (McAfee Application Control) only for specific product versions. Additional information is available in the Internet at the following address: http://support.automation.siemens.com/WW/view/en/10154608

Whitelisting 2

2.1 Introduction

Effective use of Whitelisting technologies in a process control system is only given as part of a comprehensive security concept. Whitelisting technologies alone cannot protect a process control system against hostile attacks.

It is therefore always advisable to take the
Security concept PCS 7 / WinCC into consideration, which is available on the Internet at:

http://support.automation.siemens.com

In conjunction with the security concept mentioned above, Whitelisting is to be considered an additional layer of defense as an appropriate further means of counteracting the rising risk of malicious attacks.

Whitelisting takes the approach that all applications are not trusted, except for those which have been rated trustworthy after verification, which means that a positive list (Whitelist) is being maintained. This positive list contains all applications that have been rated trustworthy for execution on the computer system.

This renders the principle of Whitelisting the exact opposite of Blacklisting that is based on a list or definition of "non-trustworthy" applications (negative list, i.e. blacklist). An example of blacklisting is a standard virus scanner that operates based on a blacklist, namely the virus pattern. This blacklist must be updated continuously under the aspect of a continuously rising number of "non-trustworthy" applications. This means that an updated black (virus pattern) always has to made available for the virus scanner. The virus scanner is only able to detect "malware" if corresponding "applications" and attack patterns have been entered in this blacklist.

Whitelisting by contrast is based on a positive list and does not require continuous updates to combat new malware threats.

2.2 McAfee Application Control

McAfee Application Control can be used to block execution of unauthorized applications on servers and workstations.
This means that once it has been installed and activated on a computer system, McAfee Application Control protects all executable files against manipulation and prevents execution of unknown files (that are not in the Whitelist).
By contrast to simple Whitelisting concepts, McAfee Application Control employs a dynamic trustworthiness model. This approach dispenses of time-consuming manual updates of the list of approved applications. Updates can be installed in different ways:

- By trusted users
- By trustworthy manufacturers (certificate)
- From a trusted directory
- By means of binary file
- By means of Updater (update programs such as WSUS, or virus scanners)

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

CAUTION
McAfee Application Control part of McAfee Integrity Control. McAfee Integrity Control currently includes the McAfee Application Control and McAfee Change Control components. Only the Whitelisting functionality, i.e. McAfee Application Control, is approved for use in the SIMATIC PCS 7 and WinCC environment. For this reason, coverage in this documentation is restricted exclusively to this functionality. SIEMENS customers may order McAfee Application Control as usual as separate software from McAfee or their distributors.

Administration 3

3.1 Administration

McAfee Application Control can be administered in different ways:

- Locally on a computer system (standalone)
- Centrally using McAfee ePolicy Orchestrator (ePO)

Decisions in favor of central or local administration should be made based on the number of systems to be maintained.

You have to use the following procedure that is independent on the type of administration:

Once McAfee Application Control has been installed on the computer, you first need to run the "solidify" function that scans all connected drives for the presence of executable files. The duration of this procedure depends on the data volume and computer performance and may take several hours. With current hardware, WinCC 7.0.2 Server installation and normal projects, this operation takes approx. 20 to 30 minutes.
You need to restart the computer after McAfee Application Control has been activated. All executables (exe, com, dll, bat, etc.) found during the scan are now protected against manipulation (renaming, deletion, etc.). New files cannot be executed.

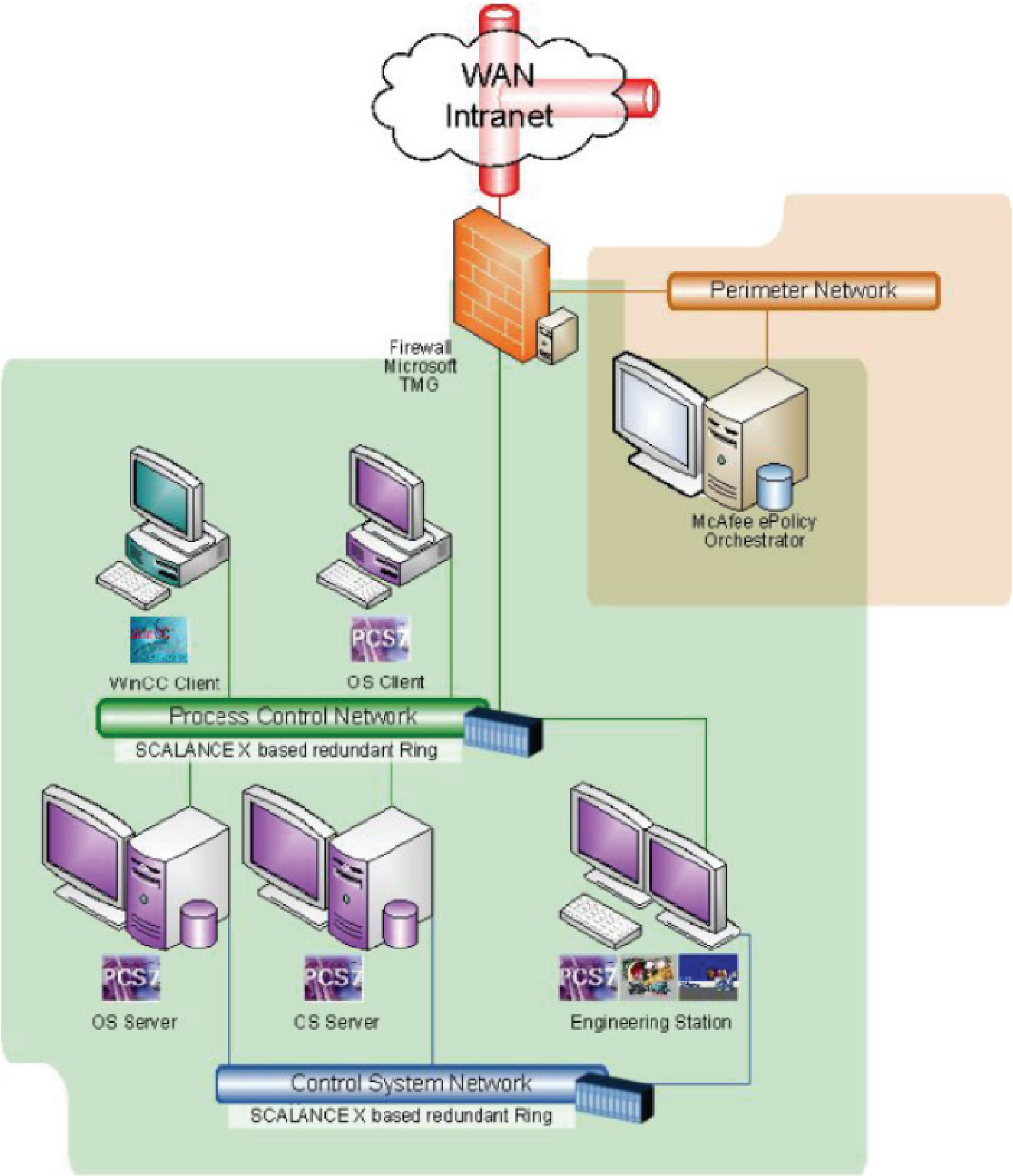
3.2 Local administration of McAfee Application Control

Local administration is handled exclusively by means of command line input. The commands are intelligible and self-explanatory and McAfee provides excellent reference material. McAfee Application Control can be handled conveniently using batch files or scripts.

3.3 Central administration by means of McAfee ePO

Architecture

McAfee ePO should be installed on a separate computer that contains the latest hardware. McAfee ePO may also be installed on an infrastructure computer (e.g. WSUS, virus scan server) that is already available in the system.
McAfee ePO may not be installed on an automation device or Domain Controller.



Central administration, meaning installation, configuration, and monitoring is handled by means of McAfee ePO (McAfee ePolicy Orchestrator), which is a management tool that is not only capable of managing all McAfee products, but also offers an extensive portfolio of network management and monitoring functionalities that are partially free of charge.

Similar to an Active Directory Domain, a central administration should be used in domains consisting of approx 10 or more managed systems.

All local commands and options of McAfee Application Control are also available remotely via ePO. This is partially based on predefined tasks, while remaining functions are being handled by means of remote command line options. By comparison to local administration, ePO offers superior monitoring functions and a clearly arranged event management.

Using McAfee Application Control with PCS 7 and WinCC

4

The following sections explain the notices and special features associated with the use of McAfee Application Control in the SIMATIC PCS 7 & WinCC environment.

This information has been based on McAfee ePolicy Orchestrator (ePO) 4.5 (ePO Agent 4.0), and McAfee Application Control 5.1.

4.1 Preparing for installation

Once McAfee Application Control has been installed and activated on a device, it is not possible to execute new programs or manipulate (update) existing programs.
You should follow the instructions below during integration of McAfee Application Control, or prior to its installation:

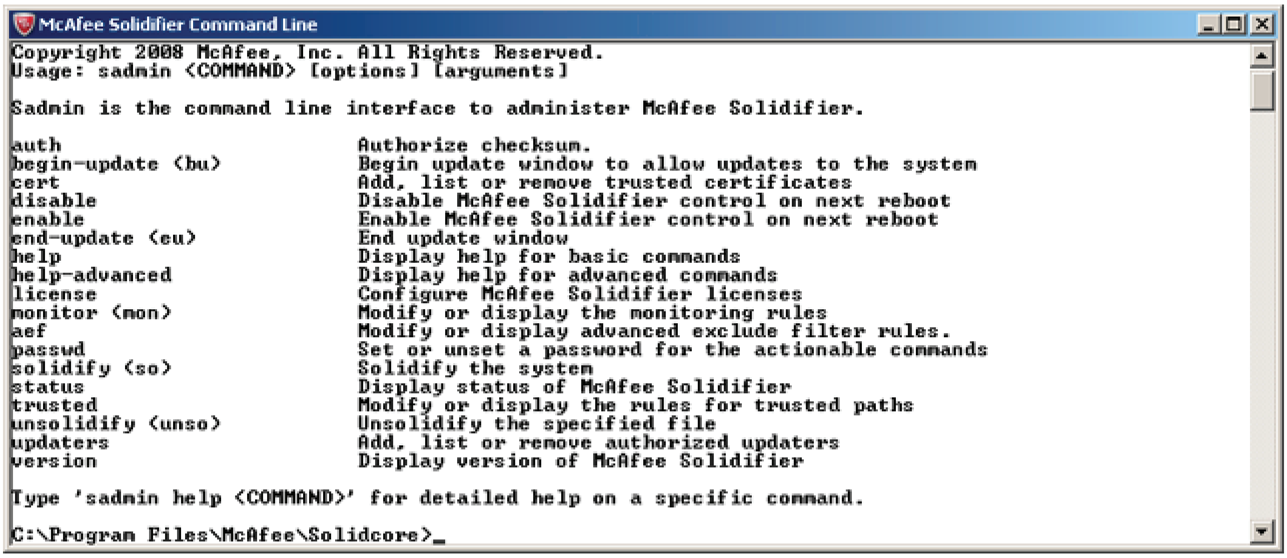
1. The system architecture should be set up in accordance with recommendations based on the Security Concept PCS 7 & WinCC in order to keep malware risks to the possible minimum prior and during integration of McAfee Application Control.
2. Install and configure the operating system.
3. Install all necessary programs and components.
4. Install all security updates that are available for the operating system and programs.
5. Install a virus scanner and update it with the latest virus signature files.
6. You should disconnect the device from external / third-party networks (e.g. at the front-end Firewall).
7. Run a complete virus scan on the device.
8. Install McAfee Application Control locally, or by means of ePO (see the following description).
9. "Solidify" all local hard disks and partitions, i.e. the computer system is scanned for executable programs; only the programs found can be executed in the future. (See the following description).
10. Activate McAfee Application Control and restart the device.

4.2 Local administration

4.2.1 AC Administrator

AC Administrator

McAfee Application Control can be protected by means of password so that even a local administrator is prevented from shutting down McAfee Application Control. This means that the "AC Administrator" can be set up independently from the local Windows Administrator.



```
Copyright 2008 McAfee, Inc. All Rights Reserved.
Usage: sadmin <COMMAND> [options] [arguments]

Sadmin is the command line interface to administer McAfee Solidifier.

auth                           Authorize checksum.
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-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
aef                            Modify or display advanced exclude filter 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
updaters                       Add, list or remove authorized updaters
version                        Display version of McAfee Solidifier

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

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

4.2.2 Installation and configuration

Installation and configuration

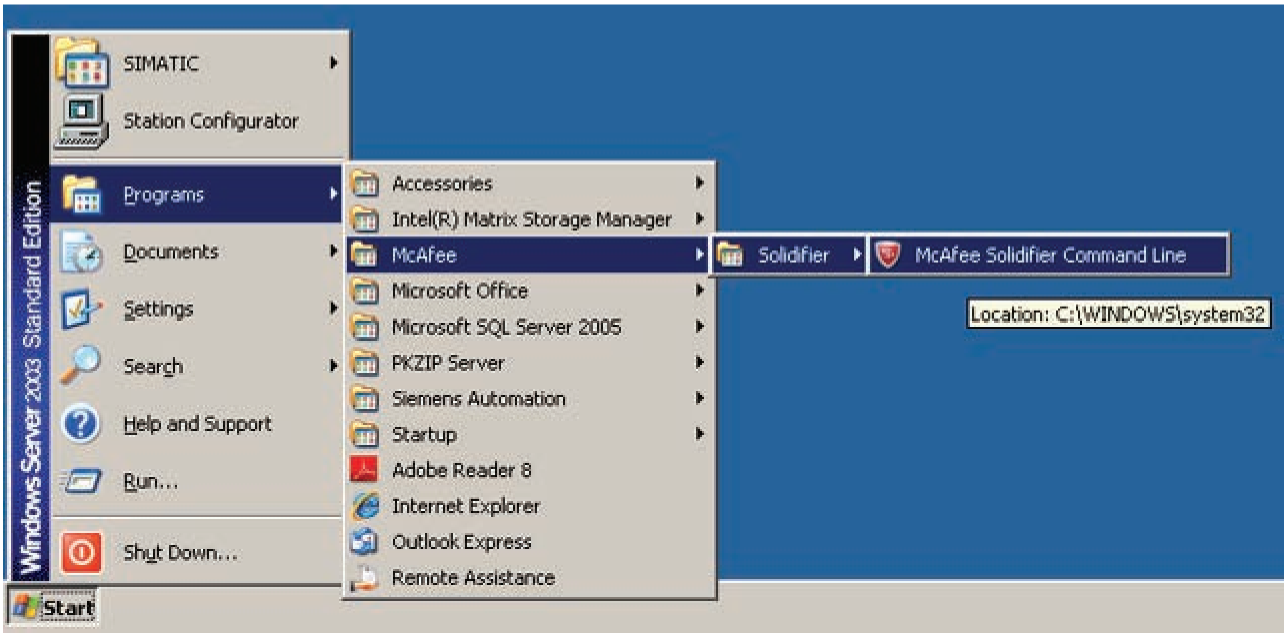
Follow these steps to install McAfee Application Control locally on a computer system:

- Run the Setup for McAfee Application Control and follow the instructions in the dialogs. You can accept all default settings without modifications.

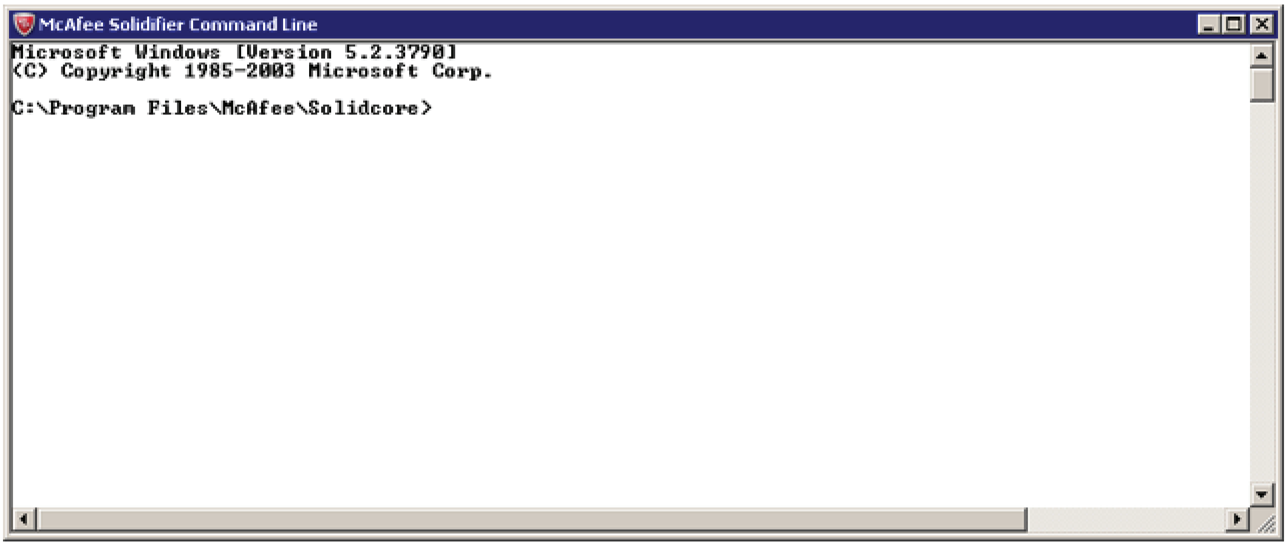
You should then run the "solidify" function for all hard disks and partitions.

Follow these steps:

- After completing the installation, open the McAfee Application Control command line with Start > Programs > McAfee > Solidifier > McAfee Solidifier Command Line

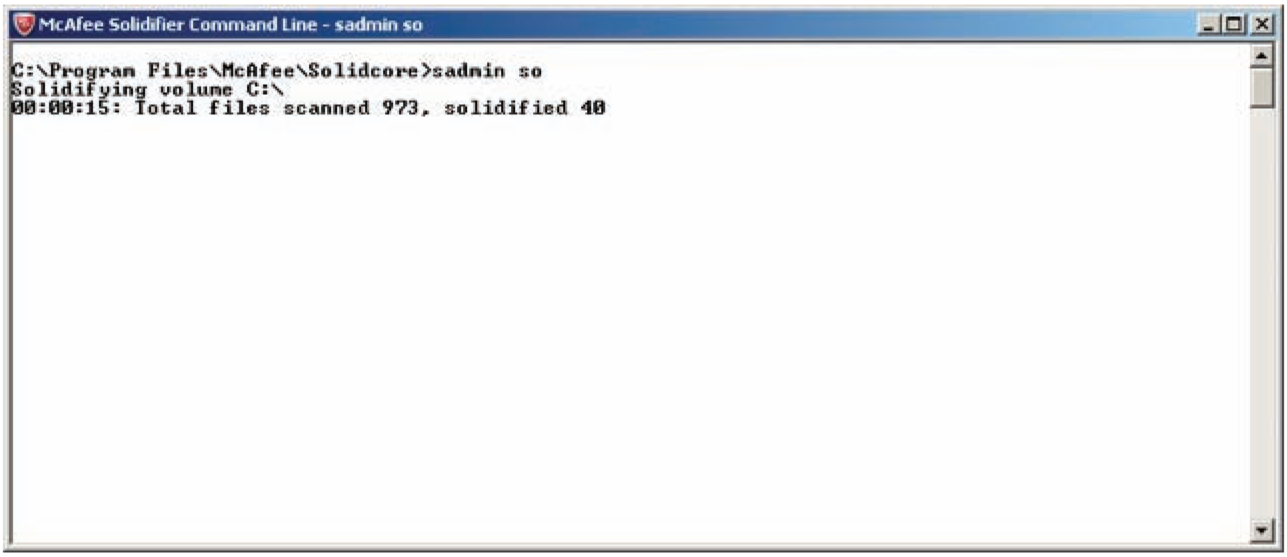


This opens Solidifier command line input:



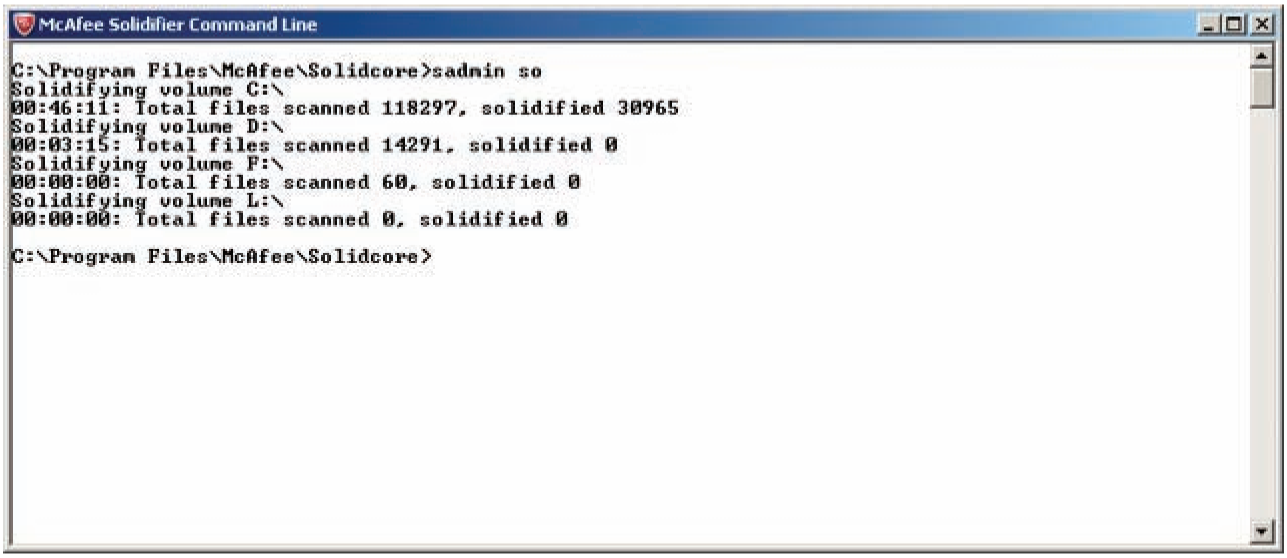
```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

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

- Start solidification by entering the "sadmin solidify" or "sadmin so" command



```
C:\Program Files\McAfee\Solidcore>sadmin so
Solidifying volume C:\
00:00:15: Total files scanned 973, solidified 40
```

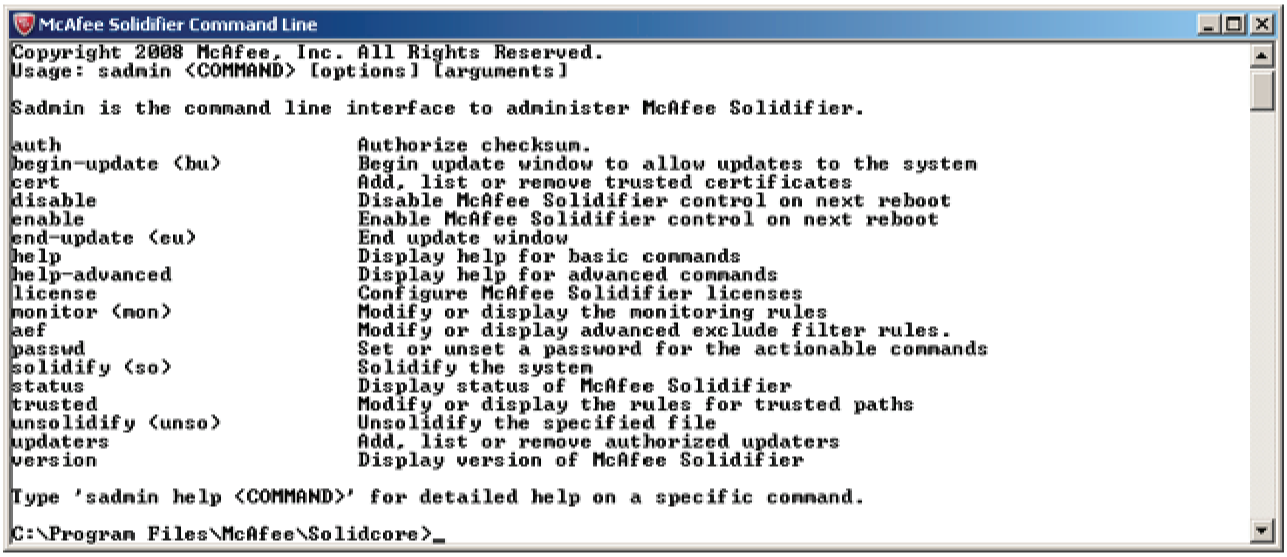
All partitions and local hard disks of the computer system are now scanned for the presence of executable files (applications), e.g. exe, com, bat, dll, as well as Java, Active-X control elements, and scripts. McAfee Application Control then signs and authorizes all files found during the scan for future use. It also protects the files against manipulation such as deletion, or renaming.



```
C:\Program Files\McAfee\Solidcore>sadmin so
Solidifying volume C:\
00:46:11: Total files scanned 118297, solidified 30965
Solidifying volume D:\
00:03:15: Total files scanned 14291, solidified 0
Solidifying volume F:\
00:00:00: Total files scanned 60, solidified 0
Solidifying volume L:\
00:00:00: Total files scanned 0, solidified 0

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

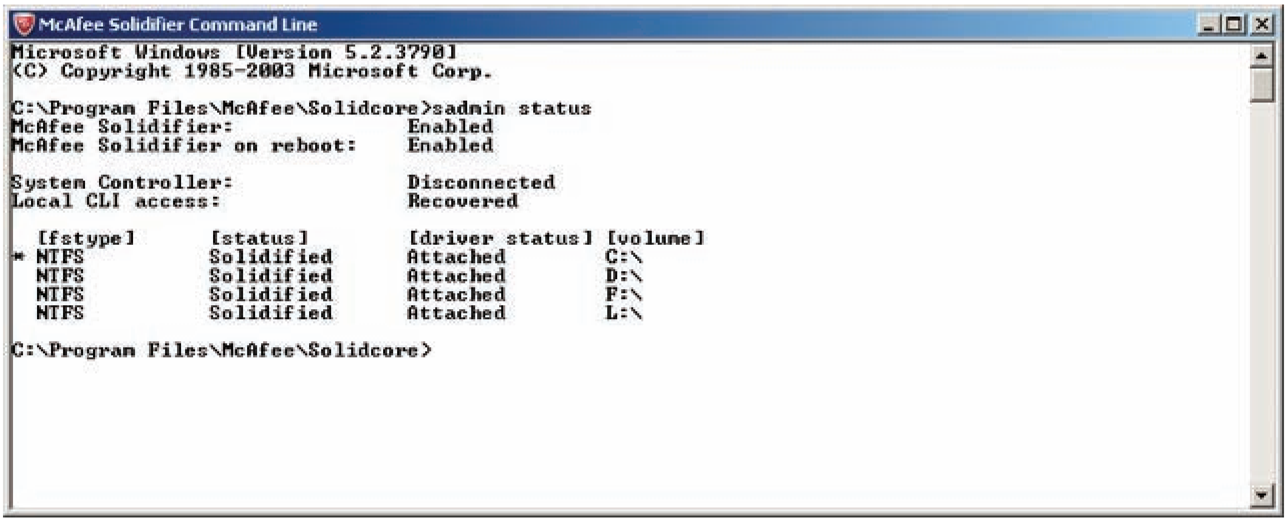
On successful completion of "solidification", the Solidifier command line reports the number of files scanned per partition or hard disk, including the number of files that have been authorized.

You need to activate McAfee Application Control on completion of "solidification". Enter the corresponding "sadmin enable" command at the Solidifier command line. The McAfee Solidifier Control will be activated at the next restart.



```
Copyright 2008 McAfee, Inc. All Rights Reserved.
Usage: sadmin <COMMAND> [options] [arguments]

Sadmin is the command line interface to administer McAfee Solidifier.

auth                        Authorize checksum.
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-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
aef                         Modify or display advanced exclude filter 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
updaters                    Add, list or remove authorized updaters
version                     Display version of McAfee Solidifier

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

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

Restart the computer. After the restart has been completed, you can query the status of McAfee Solidifier by entering the "sadmin status" command at the Solidifier command line.



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

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

System Controller:               Disconnected
Local CLI access:                Recovered

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

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

The computer system is now protected, which means that all applications it contains are protected against manipulation such as deletion, or renaming.

For information on how to enable explicit modifications, refer to the section "Update installation (Page 61)".

4.3 Central administration using McAfee ePolicy Orchestrator

4.3.1 Installing and configuring McAfee ePO Server

Installing and configuring McAfee ePO Server

McAfee ePolicy Orchestrator is an extensive software package that you can use to manage a multitude of different programs (including McAfee VirusScan). Moreover, it also provides the functionality of a network management tool. To be able to work with McAfee ePolicy Orchestrator, you actually need in-depth knowledge of the software. If you do not yet have any experience with McAfee ePolicy Orchestrator, you are strongly advised to carefully study the documentation and tutorials offered by McAfee.

The following paragraphs describe procedures for installing and configuring McAfee ePolicy Orchestrator, based on the following order:

- Installation of McAfee ePolicy Orchestrator 4.6
- Installation of the Solidcore Extension Package
- Installation of the license for Solidcore, or McAfee Application Control

Installation of McAfee ePolicy Orchestrator (ePO)

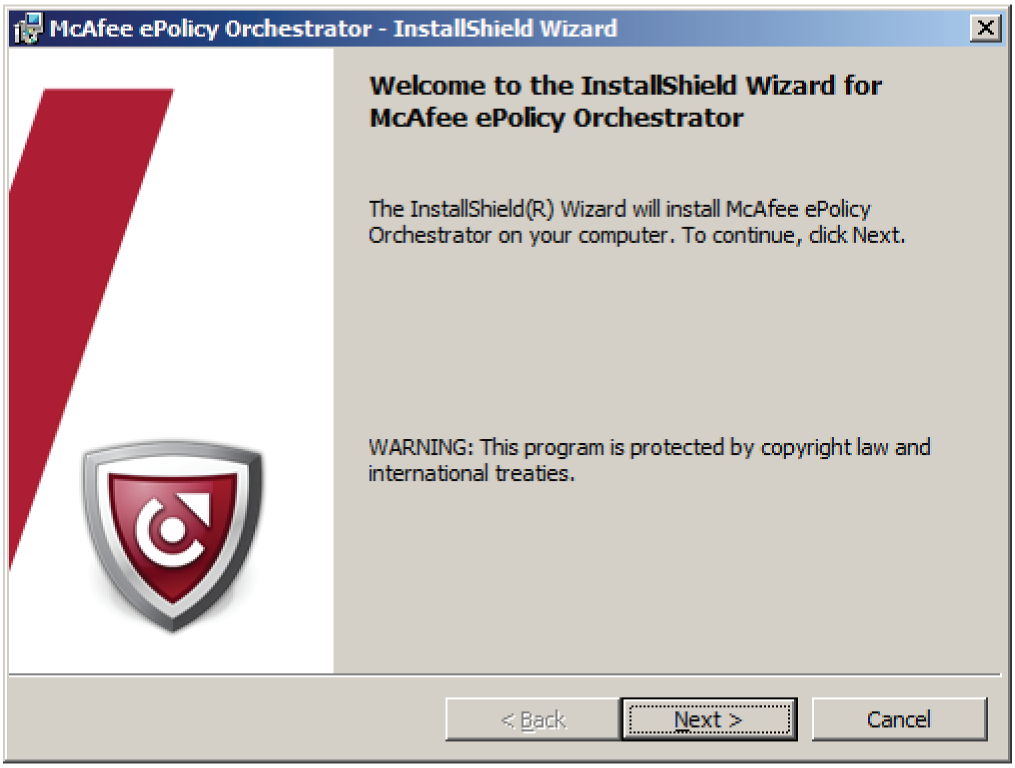
Install McAfee ePO on a separate computer that contains the latest hardware. System requirements are specified in the following listing:

Platform supported

- Server operating system: 32-bit
  - Windows Server 2008 + Service Pack 2 (SP2) Standard, Enterprise, or Datacenter
  - Windows Server 2003 + SP2 Standard, Enterprise, or Datacenter
- Server operating system: 64-bit
  - Windows Server 2008 + SP2 Standard, Enterprise, or Datacenter
  - Windows Server 2008 R2 Standard, Enterprise, or Datacenter
  - Windows Server 2008 for Small Business Premium
  - Windows Server 2003 + SP2 Standard, Enterprise, or Datacenter
- Browser
  - Firefox 3.5
  - Firefox 3.6
  - Internet Explorer 7.0
  - Internet Explorer 8.0

- Network support
  - IPv4
  - IPv6
- Virtual servers
  - VMware ESX 3.5.x update 4
  - VMware ESX 4.0 update 1
  - Citrix Deserver 5.5 update 2
  - Windows Server 2008 R2 Hyper-V
- Database (32-bit and 64-bit)
  - SQL Server 2008 + SP1/SP2/R2 Standard, Enterprise, Workgroup, Express
  - SQL Server 2005 + SP3 Standard, Enterprise, Workgroup, Express
- Additional requirements
  - 1.5 GB of free hard disk space (2 GB is recommended)
  - 1 GB RAM (2 GB to 4 GB is recommended)
  - At least Intel Premium 4 processor, 1.3 GHz or faster
  - Monitor: 1024 x 768 pixels, 256 colors, VGA
  - NIC: 100 Mbps or faster
  - File system: NTFS is recommended
  - It is recommended to set up a separate server for domains containing of more than 250 systems.
  - IP address: McAfee recommends the use of a static IP address

1. Run "setup.exe" to initiate installation of McAfee ePO.
2. Setup requirements are displayed. Follow the instructions in this dialog.



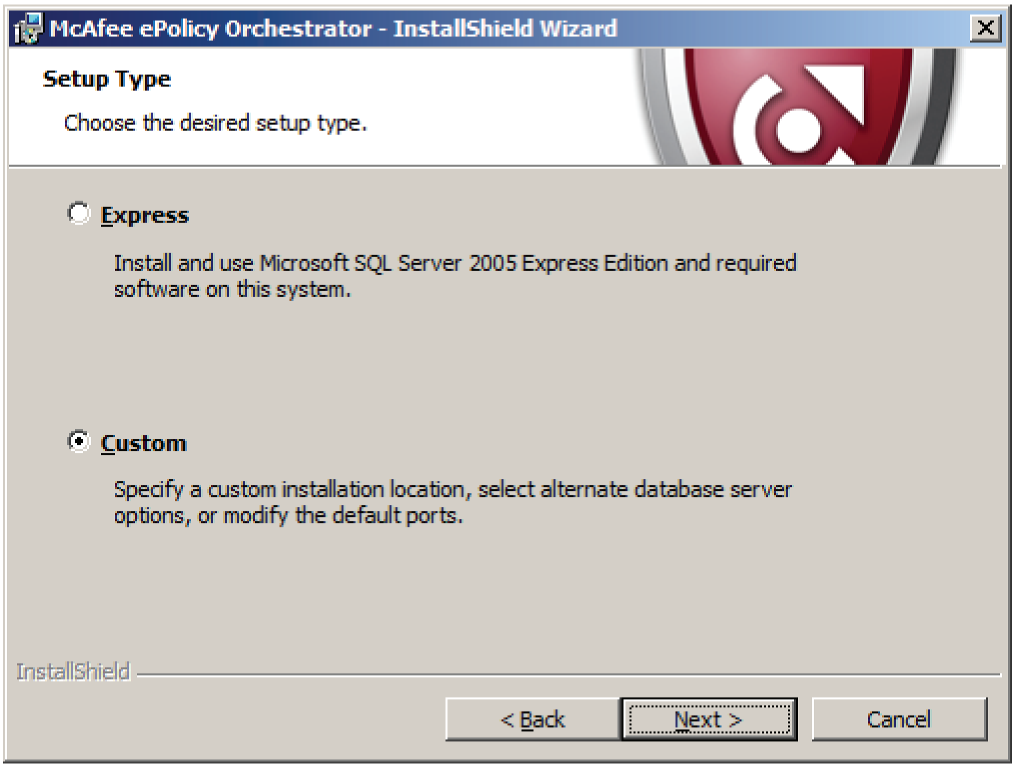
Welcome to the InstallShield Wizard for McAfee ePolicy Orchestrator

The InstallShield(R) Wizard will install McAfee ePolicy Orchestrator on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3. Click "Next" to launch the InstallShield Wizard for McAfee ePO.

4. Select the required setup type for the SQL Server.



McAfee ePolicy Orchestrator - InstallShield Wizard

Setup Type

Choose the desired setup type.

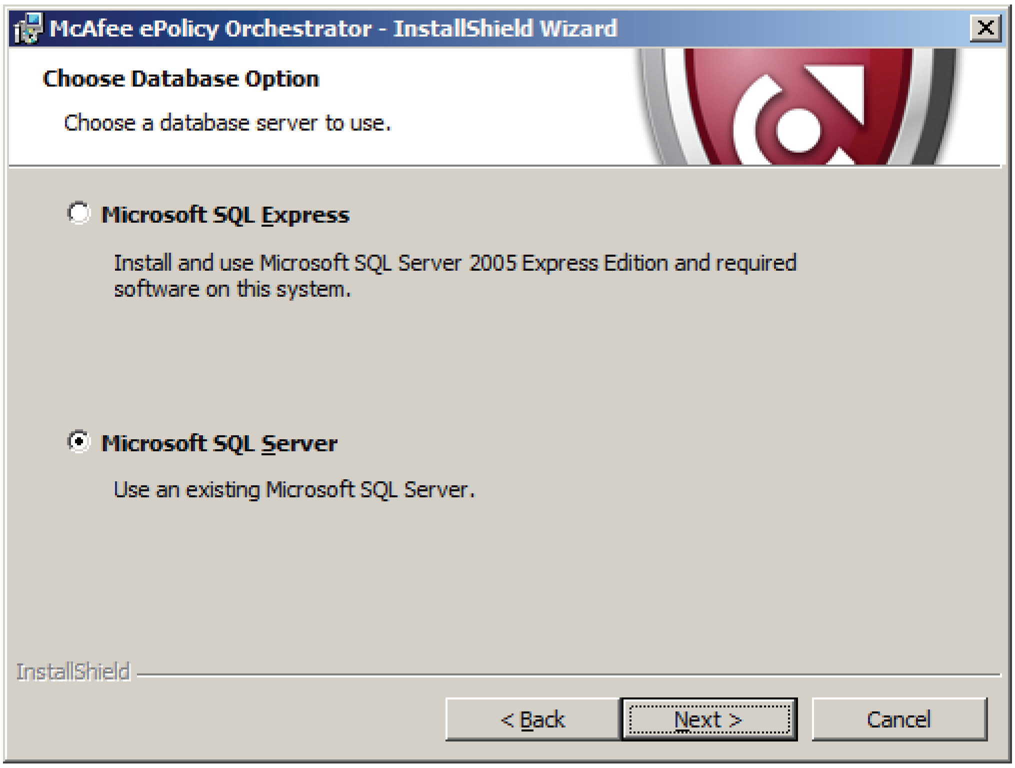
○ **Express**

Install and use Microsoft SQL Server 2005 Express Edition and required software on this system.

● **Custom**

Specify a custom installation location, select alternate database server options, or modify the default ports.

5. Select which database server is to be used.



McAfee ePolicy Orchestrator - InstallShield Wizard

Choose Database Option

Choose a database server to use.

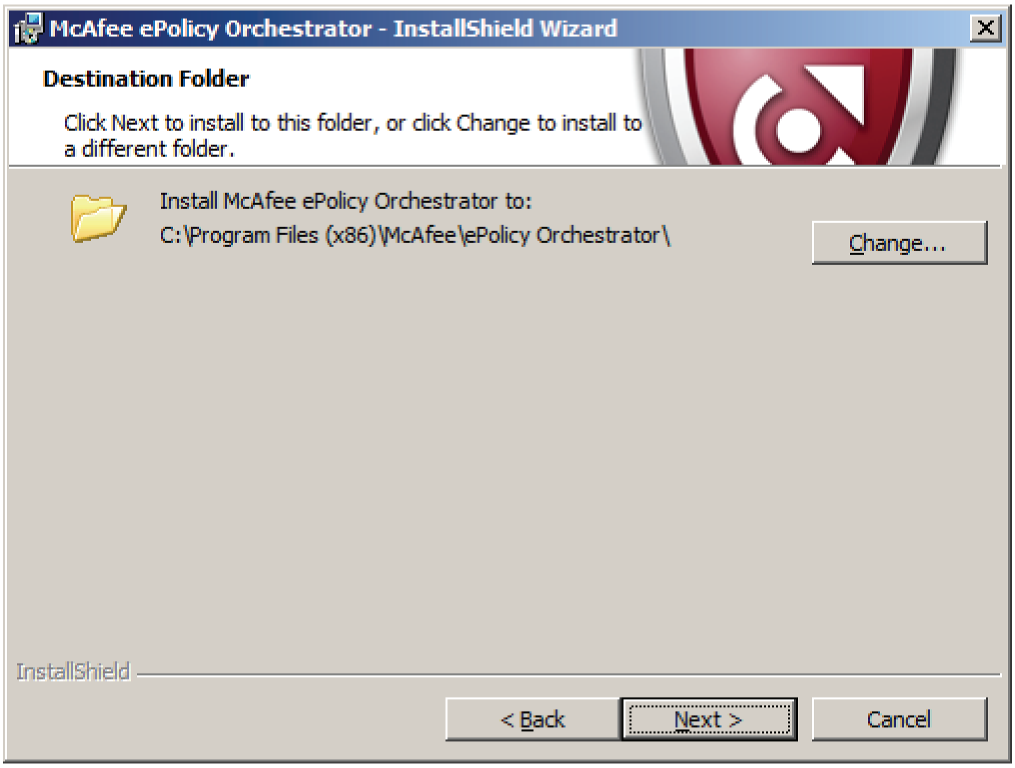
○ **Microsoft SQL Express**

Install and use Microsoft SQL Server 2005 Express Edition and required software on this system.

● **Microsoft SQL Server**

Use an existing Microsoft SQL Server.

6. The next dialog "Target folder" proposes a target folder for installation. To change this folder, click on "Change…".



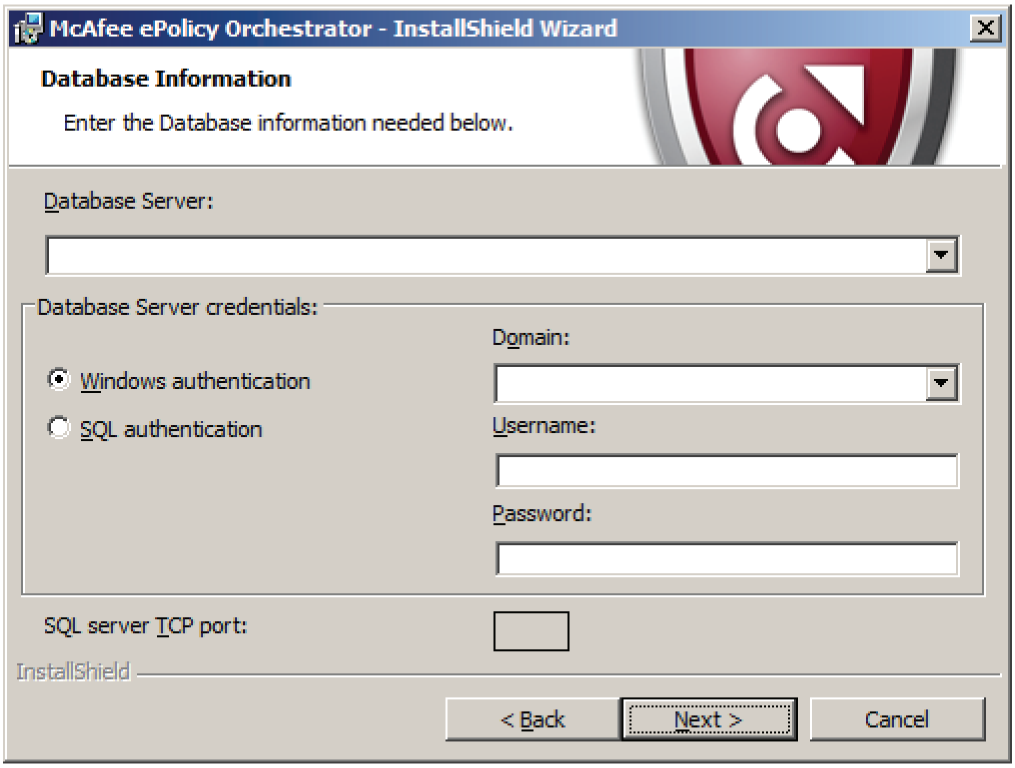
McAfee ePolicy Orchestrator - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install McAfee ePolicy Orchestrator to:
C:\Program Files (x86)\McAfee\ePolicy Orchestrator\

7. In the "Database information" dialog, specify the data that ePO uses to access the database, e.g. the database server and authentication details. In the "Domain" field, enter the domain name, or the computer name if the computer is not a domain member.



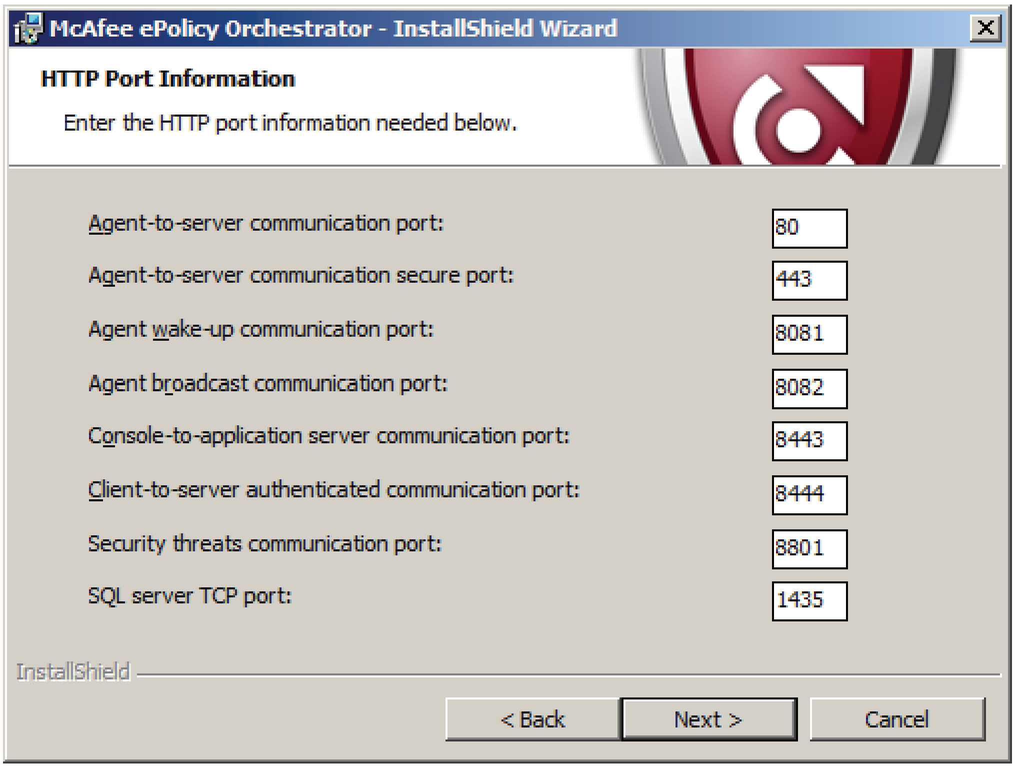
McAfee ePolicy Orchestrator - InstallShield Wizard

Database Information

Enter the Database information needed below.

Database Server credentials: ● Windows authentication ○ SQL authentication

8. In the "HTTP port information" dialog, specify the port numbers that the ePO server uses to communicate with the agents.



McAfee ePolicy Orchestrator - InstallShield Wizard

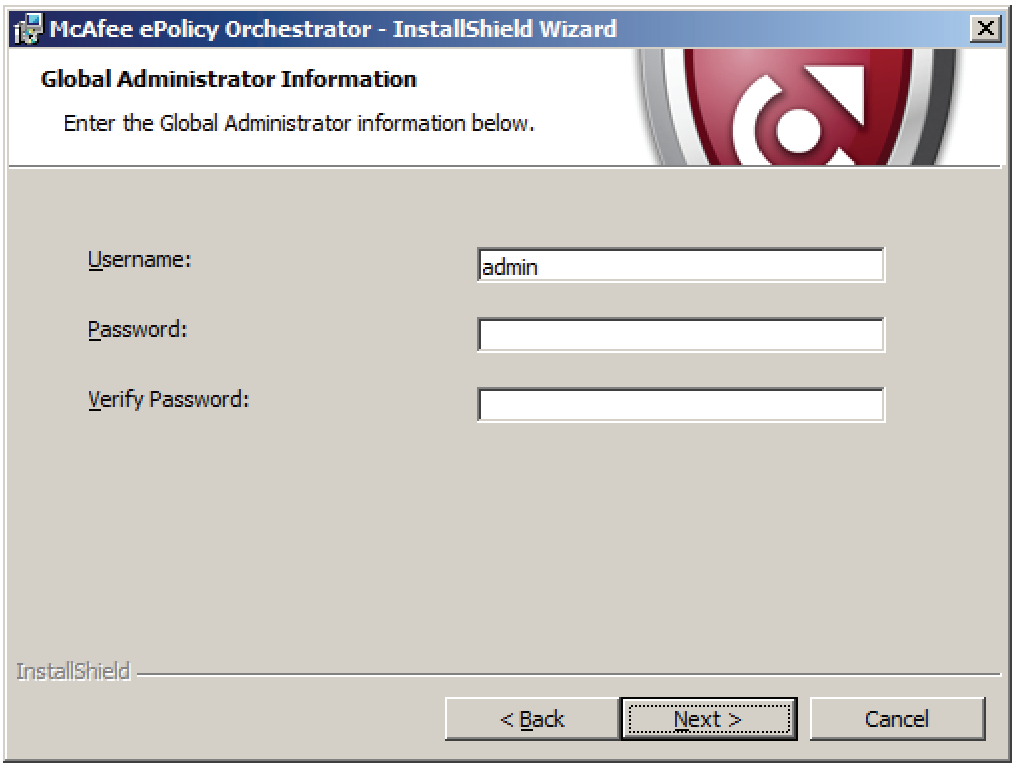
HTTP Port Information

Enter the HTTP port information needed below.

Agent-to-server communication port:	80
Agent-to-server communication secure port:	443
Agent wake-up communication port:	8081
Agent broadcast communication port:	8082
Console-to-application server communication port:	8443
Client-to-server authenticated communication port:	8444
Security threats communication port:	8801
SQL server TCP port:	1435

9. Click "Next" to open a dialog that once again shows you a summary of installation settings you made.

10. Specify the Administrator's user name and password for ePO in the next dialog "Global Administrator information".



McAfee ePolicy Orchestrator - InstallShield Wizard

Global Administrator Information

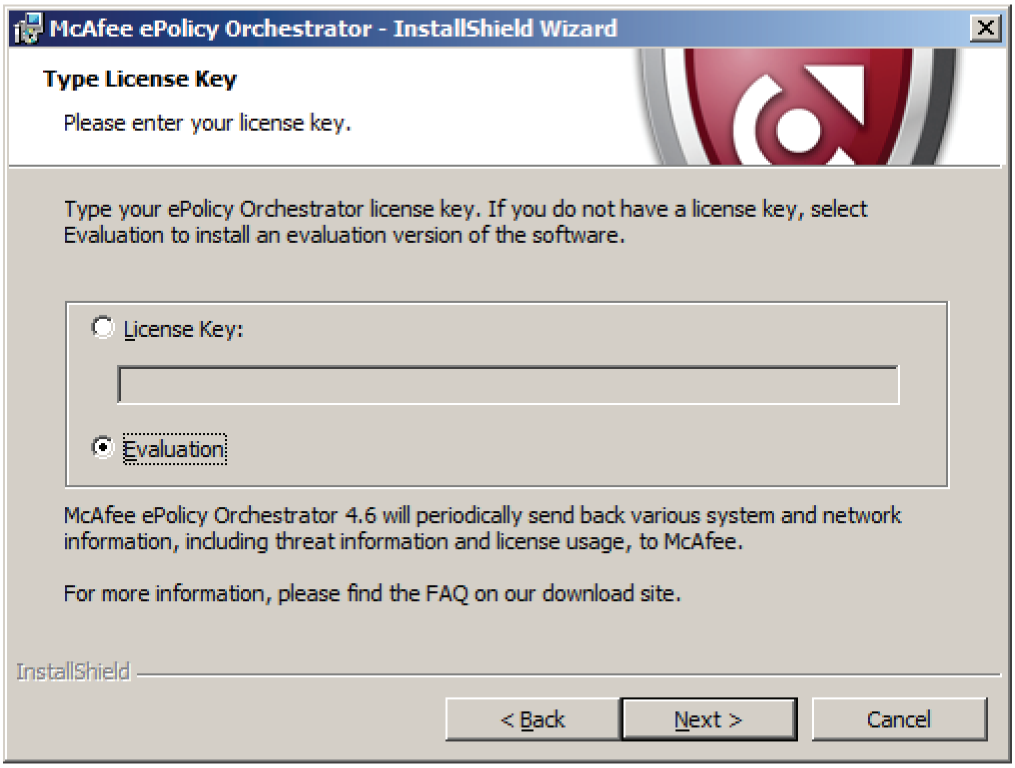
Enter the Global Administrator information below.

Username: admin

Password:

Verify Password:

11. Enter your ePO license key in the "Enter license key" dialog.



McAfee ePolicy Orchestrator - InstallShield Wizard

Type License Key

Please enter your license key.

Type your ePolicy Orchestrator license key. If you do not have a license key, select Evaluation to install an evaluation version of the software.

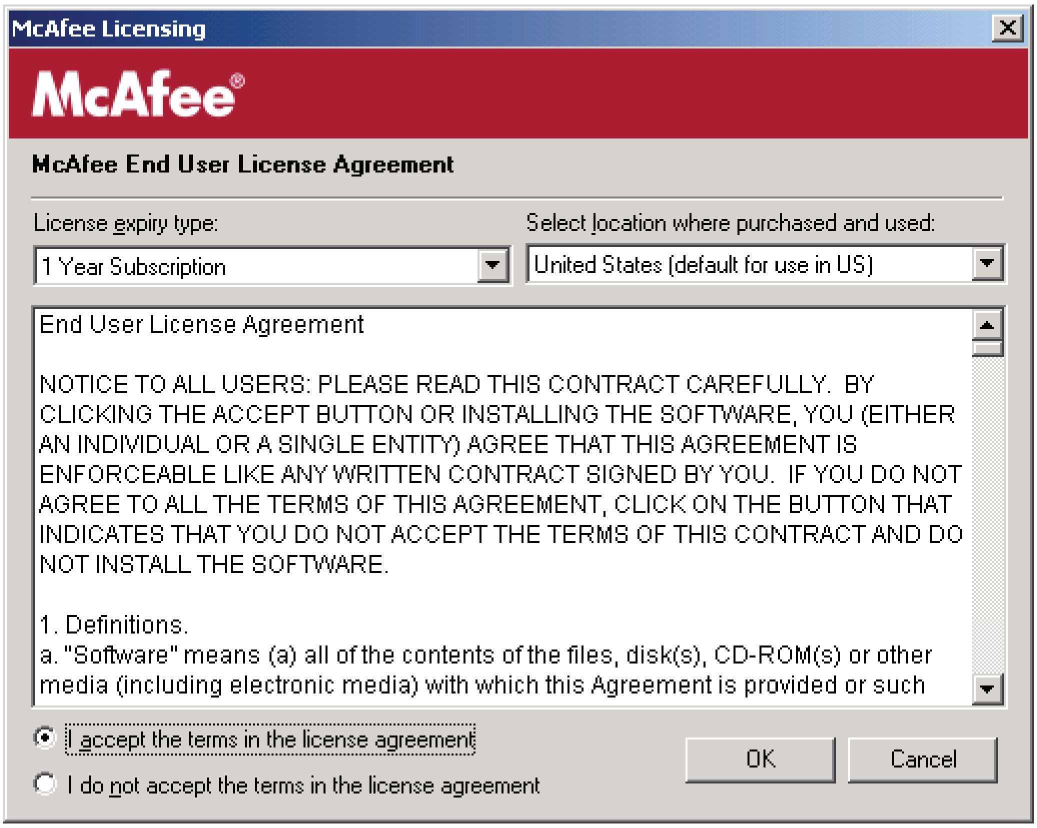
○ License Key:

● Evaluation

McAfee ePolicy Orchestrator 4.6 will periodically send back various system and network information, including threat information and license usage, to McAfee.

For more information, please find the FAQ on our download site.

12. Select "I accept the terms in the license agreement" to acknowledge the "McAfee End User License Agreement" in the next dialog.



McAfee End User License Agreement

License expiry type: 1 Year Subscription

Select location where purchased and used: United States (default for use in US)

End User License Agreement

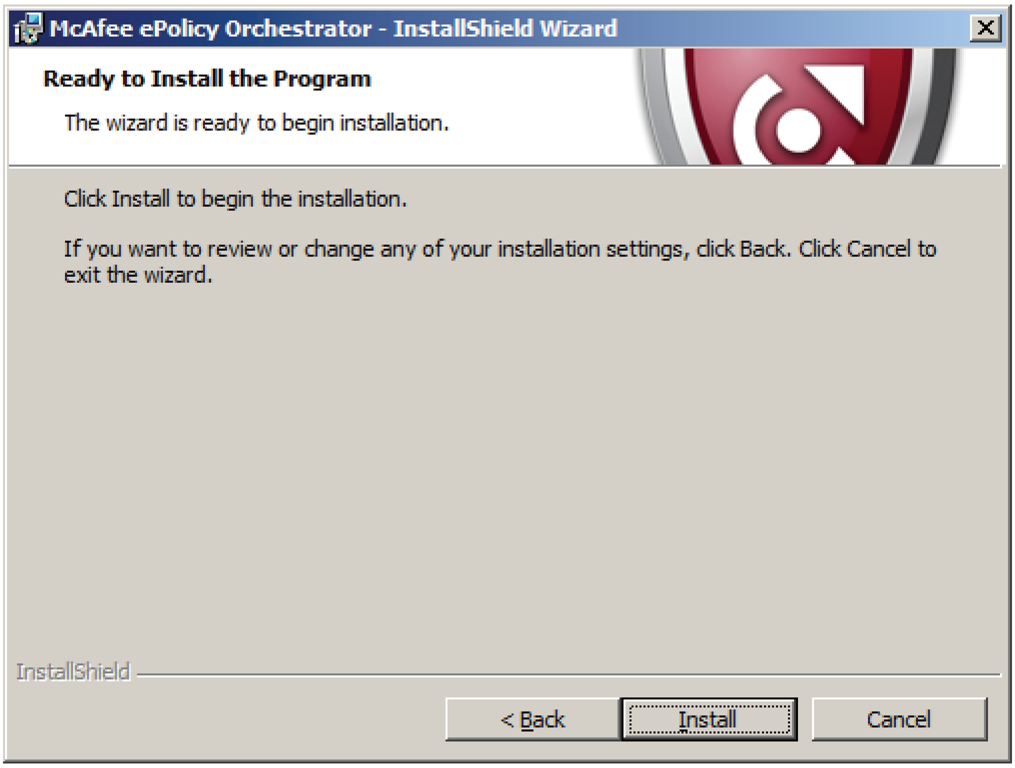
NOTICE TO ALL USERS: PLEASE READ THIS CONTRACT CAREFULLY. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS CONTRACT AND DO NOT INSTALL THE SOFTWARE.

1. Definitions.
a. "Software" means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

13. Click "Install" to launch the installation process that may take a few minutes. Setup is concluded by clicking "Finish" in the "InstallShield Wizard completed" dialog.



McAfee ePolicy Orchestrator - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

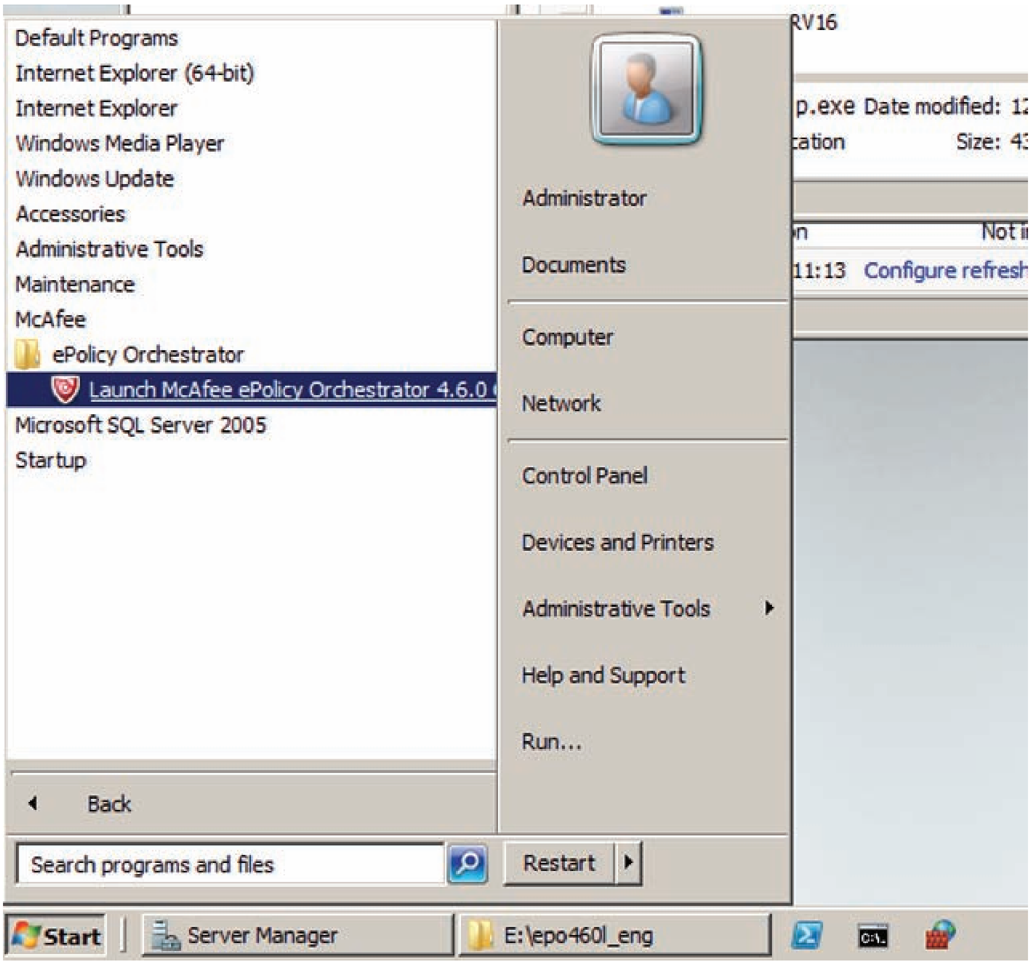
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

4.3.2 Installing the Solidcore Extension Package

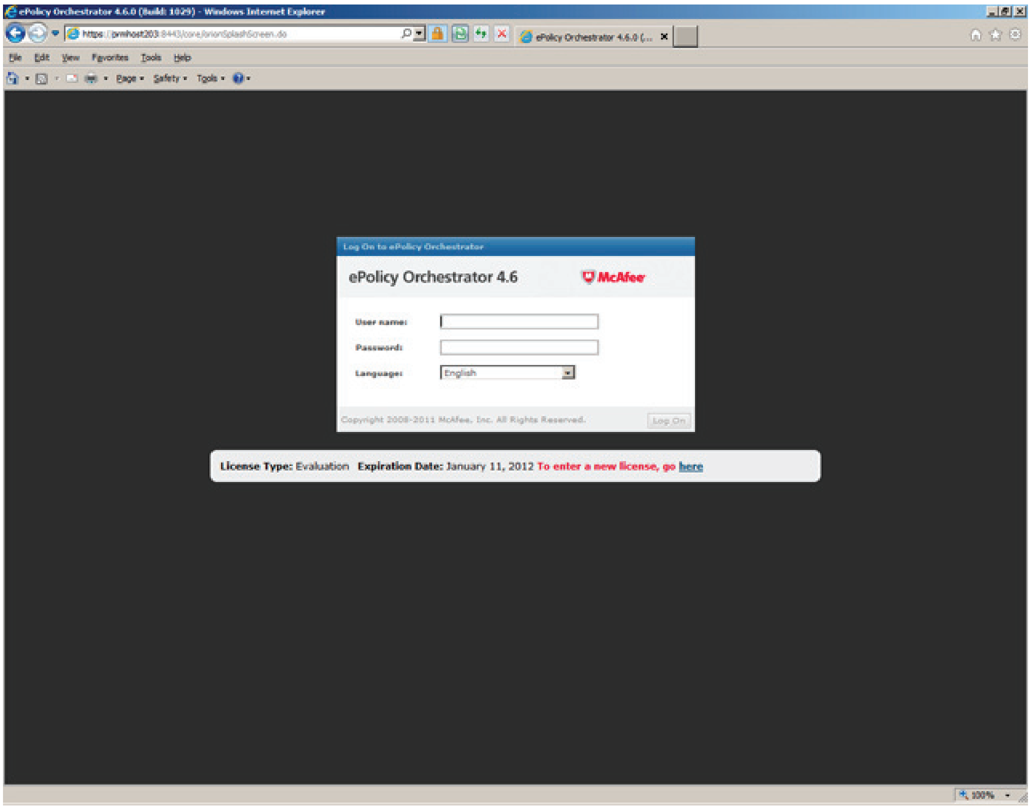
Installing the Solidcore Extension Package

On successful completion of your installation of McAfee ePolicy Orchestrator, install the "Solidcore Extension Package". Follow these steps:

1. Launch McAfee ePO by selecting
   Start > Programs > McAfee > ePolicy Orchestrator > Start McAfee ePolicy Orchestrator 4.6.0 Console



2. In the login dialog, enter the user name and password you specified during ePO installation.



ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
https://prmhost203:8443/core/orionSplashScreen.do
ePolicy Orchestrator 4.6.0 (...
File Edit View Favorites Tools Help
Page ▾ Safety ▾ Tools ▾
100%

Log On to ePolicy Orchestrator

ePolicy Orchestrator 4.6

McAfee

User name:

Password:

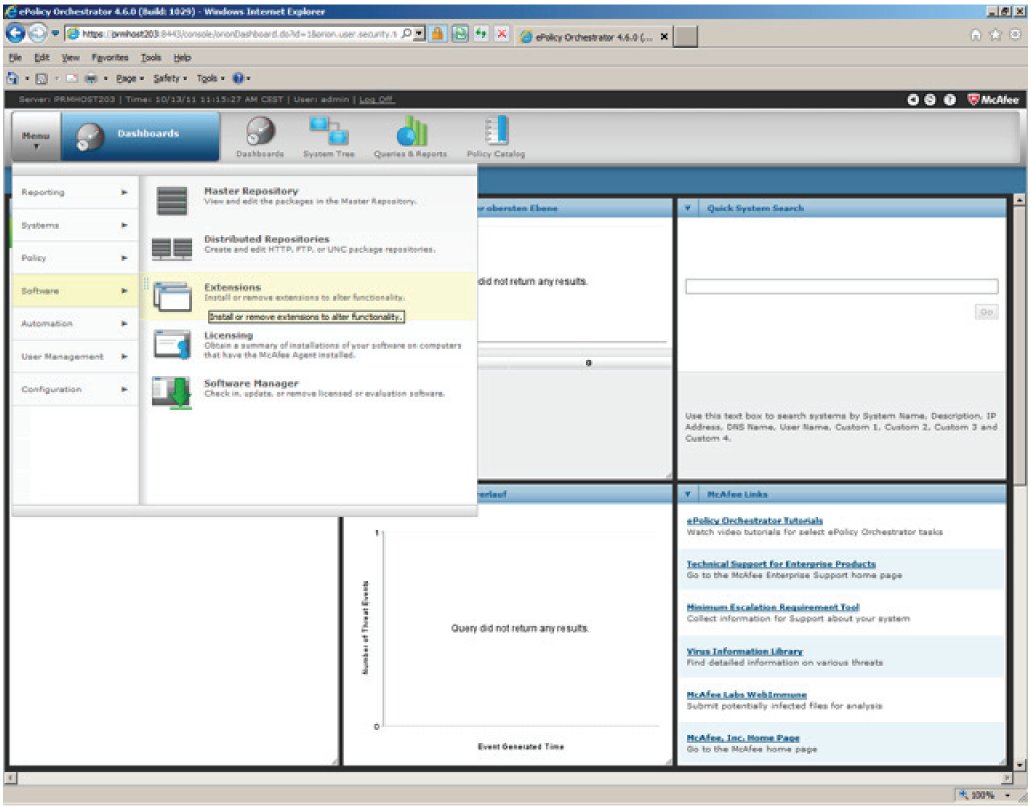
Language: English

Copyright 2008-2011 McAfee, Inc. All Rights Reserved.

Log On

License Type: Evaluation **Expiration Date:** January 11, 2012 To enter a new license, go here

3. Select the Software > Extensions command in the ePO 4.6 Console



Master Repository
View and edit the packages in the Master Repository.

Distributed Repositories
Create and edit HTTP, FTP, or UNC package repositories.

Extensions
Install or remove extensions to alter functionality.

Install or remove extensions to alter functionality.

Licensing
Obtain a summary of installations of your software on computers that have the McAfee Agent installed.

Software Manager
Check in, update, or remove licensed or evaluation software.

did not return any results.

0

Use this text box to search systems by System Name, Description, IP Address, DNS Name, User Name, Custom 1, Custom 2, Custom 3 and Custom 4.

Query did not return any results.

ePolicy Orchestrator Tutorials
Watch video tutorials for select ePolicy Orchestrator tasks

Technical Support for Enterprise Products
Go to the McAfee Enterprise Support home page

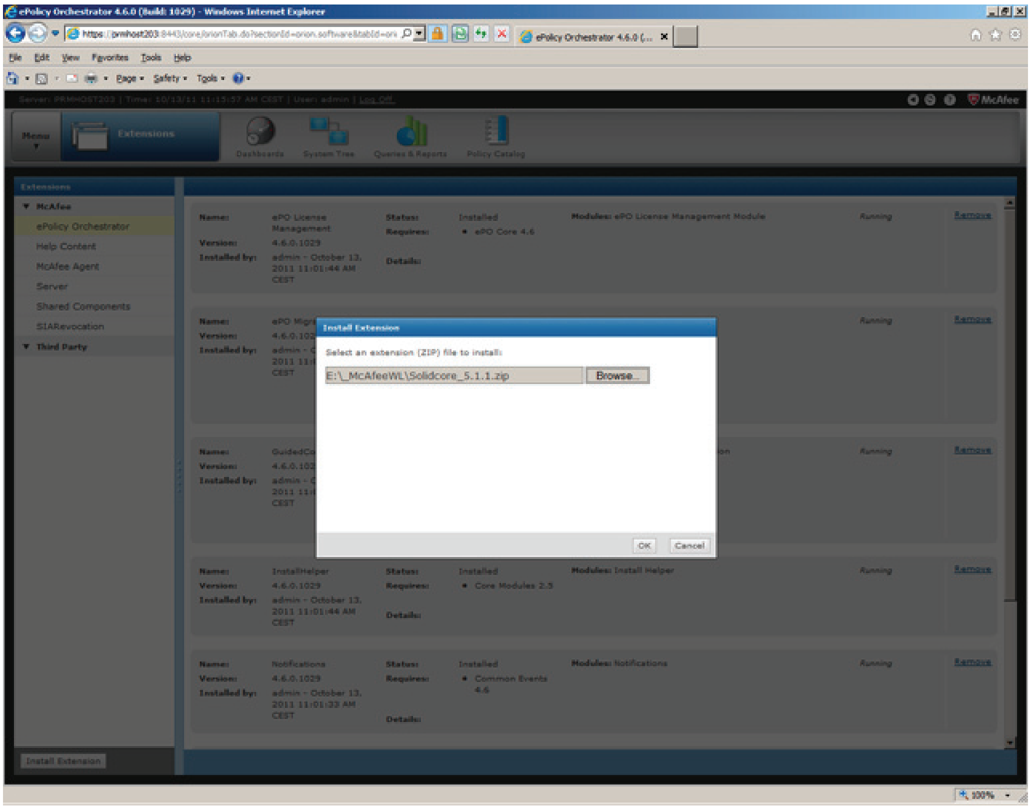
Minimum Escalation Requirement Tool
Collect information for Support about your system

Virus Information Library
Find detailed information on various threats

McAfee Labs WebImmune
Submit potentially infected files for analysis

McAfee, Inc. Home Page
Go to the McAfee home page

4. In the next dialog, "Install extension", click "Browse" to select the Solidcore Extension Package SOLIDCORE_5.0.0.ZIP.

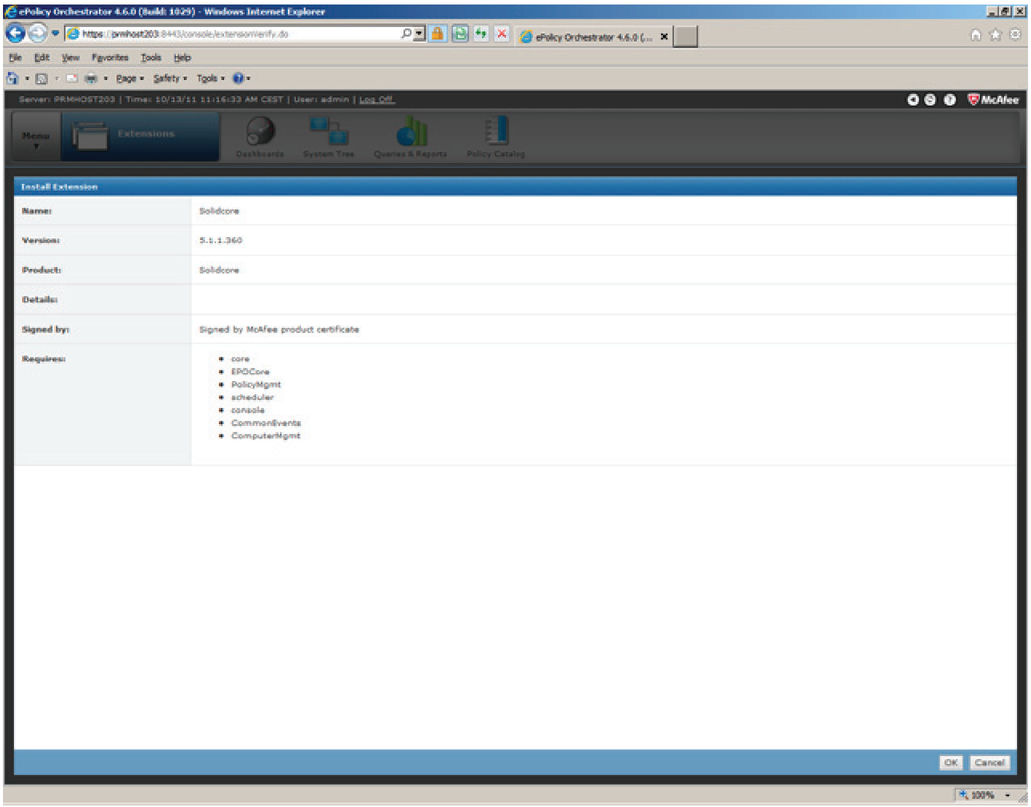


Install Extension

Select an extension (ZIP) file to install:

E:_McAfeeWL\Solidcore_5.1.1.zip

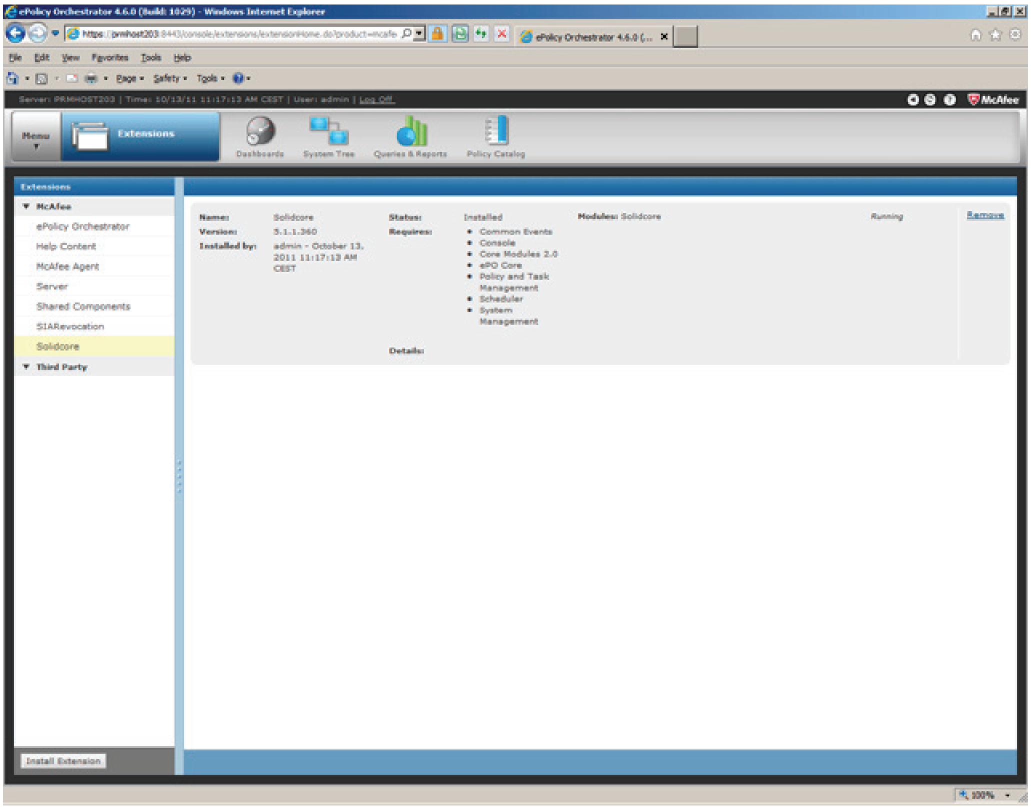
5. Click "OK" to confirm the summary that follows.


ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
https://prmhost203:8443/console/extensionVerify.do
ePolicy Orchestrator 4.6.0 (...
File
Edit
View
Favorites
Tools
Help
Page
Safety
Tools
Server: PRMHOST203 | Time: 10/13/11 11:16:33 AM CEST | User: admin | Log Off
McAfee
Menu
Extensions
Dashboards
System Tree
Queries & Reports
Policy Catalog
OK
Cancel
100%

Install Extension

Name:	Solidcore
Version:	5.1.1.360
Product:	Solidcore
Details:	
Signed by:	Signed by McAfee product certificate
Requires:	core EPOCore PolicyMgmt scheduler console CommonEvents ComputerMgmt

6. Check the list of installed extensions; the "Solidcore Extension Package" you just installed should be displayed.



ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
https://prmhost203:8443/console/extensions/extensionHome.do?product=mcafe
ePolicy Orchestrator 4.6.0 (...
File Edit View Favorites Tools Help
Page Safety Tools
Server: PRMHOST203 | Time: 10/13/11 11:17:13 AM CEST | User: admin | Log Off
McAfee
Menu
Extensions
Dashboards
System Tree
Queries & Reports
Policy Catalog
Extensions
McAfee
ePolicy Orchestrator
Help Content
McAfee Agent
Server
Shared Components
SIARevocation
Solidcore
Third Party
Install Extension
100%

Name: Solidcore
Version: 5.1.1.360
Installed by: admin - October 13, 2011 11:17:13 AM CEST
Status: Installed
Requires:
- Common Events
- Console
- Core Modules 2.0
- ePO Core
- Policy and Task Management
- Scheduler
- System Management

Details:

Modules: Solidcore

Running

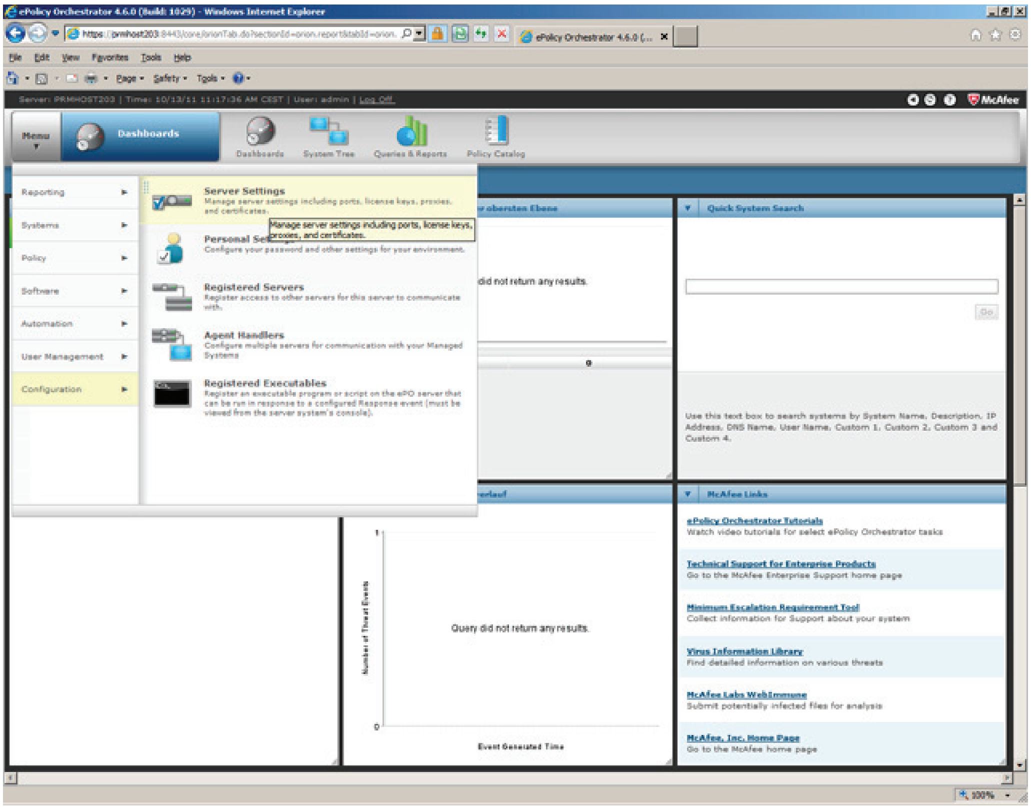
Remove

4.3.3 Installing the license for Solidcore, or McAfee Application Control

Installing the license for Solidcore, or McAfee Application Control

Install the valid Application Control license key. Follow these steps:

1. In the ePO 4.6 console, point to Configuration > Server settings



Server Settings: Manage server settings including ports, license keys, proxies, and certificates.

Manage server settings including ports, license keys, proxies, and certificates.

Personal Settings: Configure your password and other settings for your environment.

Registered Servers: Register access to other servers for this server to communicate with.

Agent Handlers: Configure multiple servers for communication with your Managed Systems

Registered Executables: Register an executable program or script on the ePO server that can be run in response to a configured Response event (must be viewed from the server system's console).

Query did not return any results.

Use this text box to search systems by System Name, Description, IP Address, DNS Name, User Name, Custom 1, Custom 2, Custom 3 and Custom 4.

ePolicy Orchestrator Tutorials: Watch video tutorials for select ePolicy Orchestrator tasks

Technical Support for Enterprise Products: Go to the McAfee Enterprise Support home page

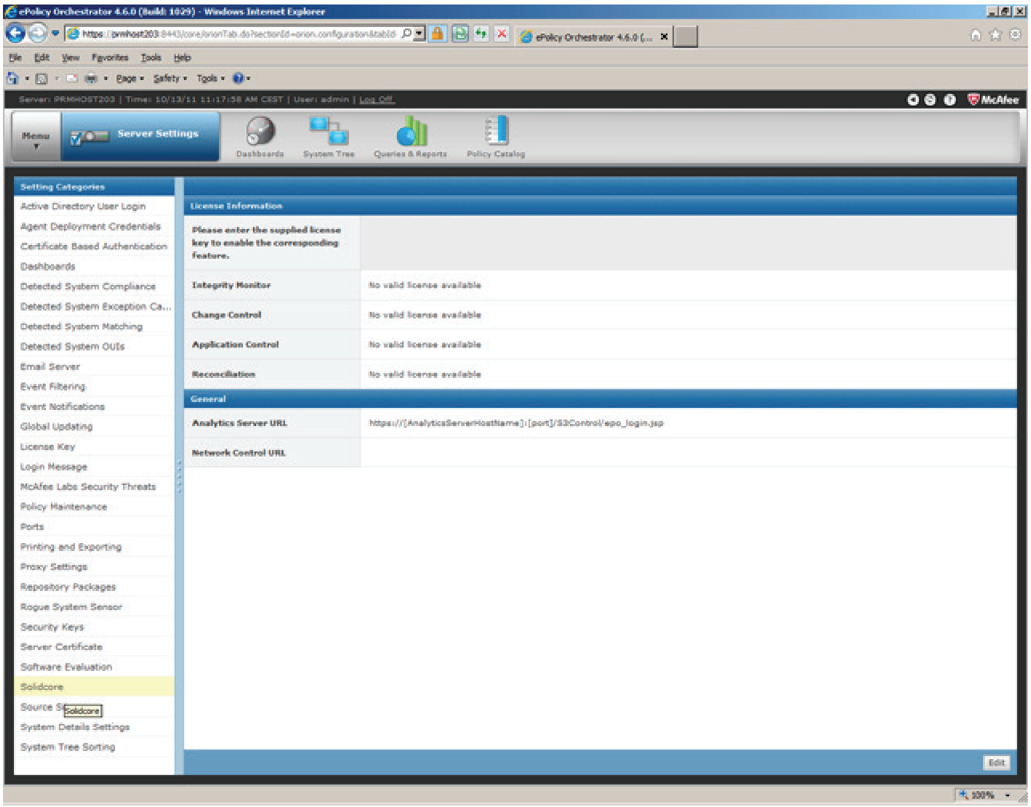
Minimum Escalation Requirement Tool: Collect information for Support about your system

Virus Information Library: Find detailed information on various threats

McAfee Labs WebImmune: Submit potentially infected files for analysis

McAfee, Inc. Home Page: Go to the McAfee home page

2. In the left of the next window, select the "Solidcore" menu command and then click "Edit".



Server: PRMHOST203 | Time: 10/13/11 11:17:58 AM CEST | User: admin | Log Off

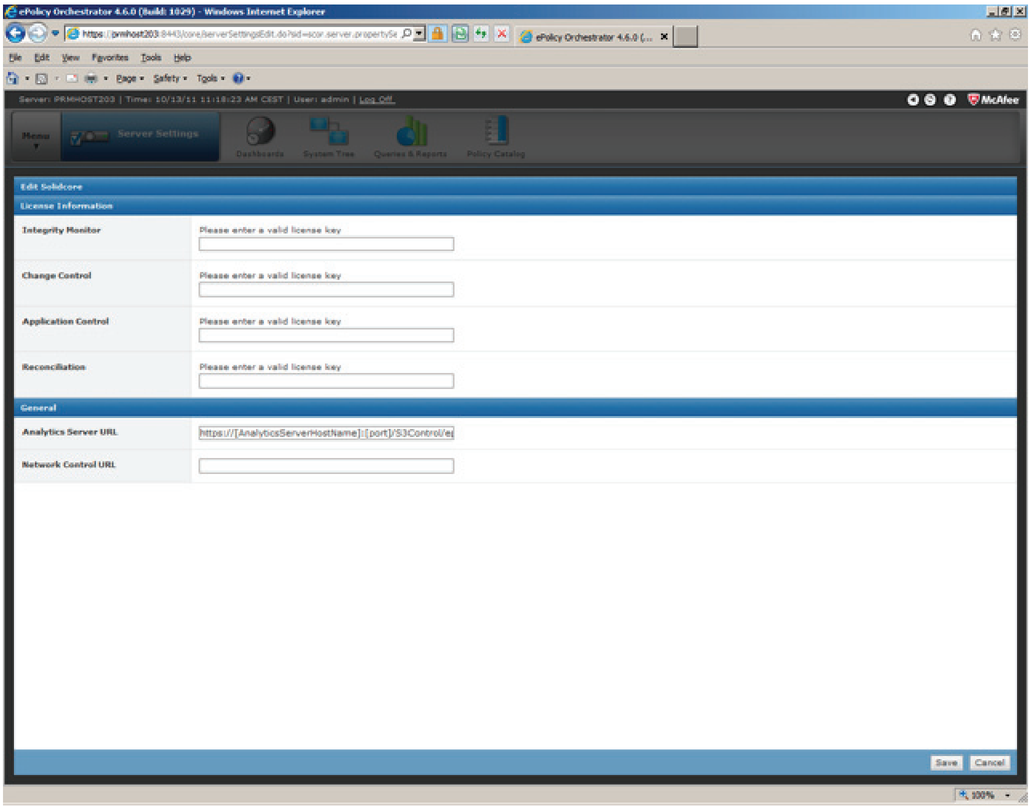
License Information

Please enter the supplied license key to enable the corresponding feature.	
Integrity Monitor	No valid license available
Change Control	No valid license available
Application Control	No valid license available
Reconciliation	No valid license available

General

Analytics Server URL	https://[AnalyticsServerHostName]:[port]/S3Control/epo_login.jsp
Network Control URL	

3. Enter the valid Application Control license key in the "Edit Solidcore - License information" window and then click "Save".



ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
https://prmhost203:8443/core/serverSettingsEdit.do?sid=scor.server.propertySe
ePolicy Orchestrator 4.6.0 (...
File Edit View Favorites Tools Help
Page Safety Tools
Server: PRMHOST203 | Time: 10/13/11 11:18:23 AM CEST | User: admin | Log Off
McAfee
Menu
Server Settings
Dashboards
System Tree
Queries & Reports
Policy Catalog
Save
Cancel
100%

Edit Solidcore

License Information

Integrity Monitor	Please enter a valid license key
Change Control	Please enter a valid license key
Application Control	Please enter a valid license key
Reconciliation	Please enter a valid license key

General

Analytics Server URL	https://[AnalyticsServerHostName]:[port]/S3Control/e
Network Control URL	

You successfully completed installation of the McAfee ePolicy Orchestrator Server.

Continue by installing the McAfee Solidcore client.

4.3.4 Installing the McAfee Solidcore clients

Installation of the McAfee Solidcore Agent on the clients is based on the following procedures:

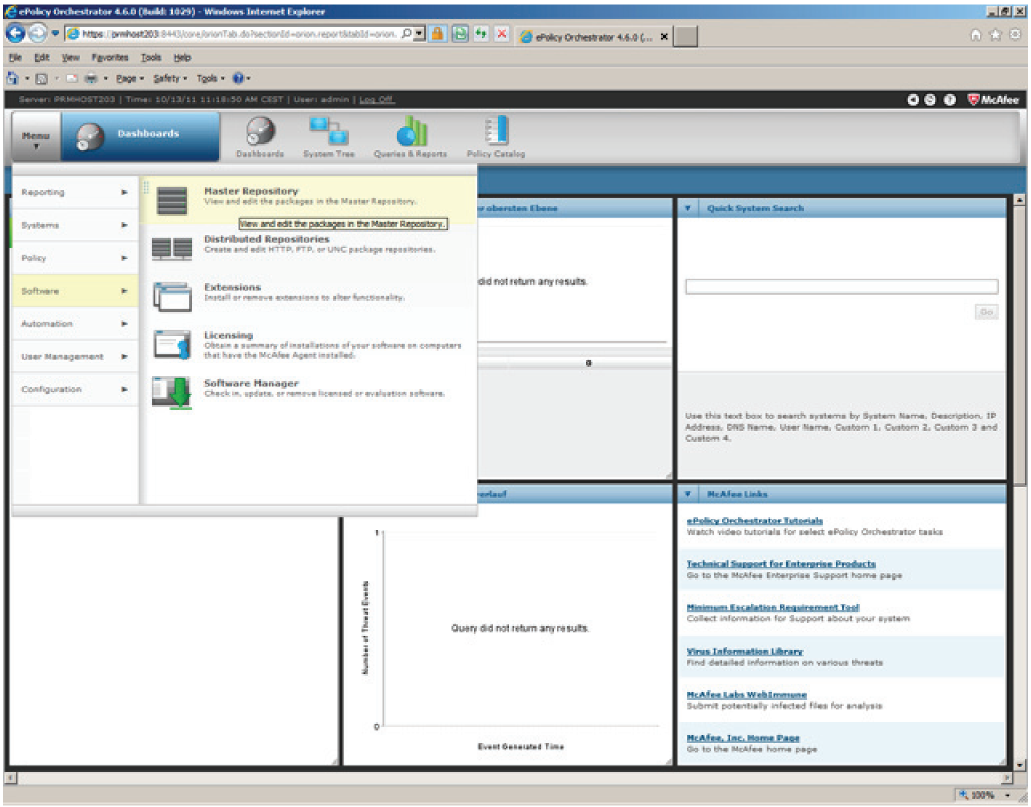
- Adding the Solidcore Agent Deployment Package to the ePO Repository
- Integrating the client systems into the ePO Console
- Installation of the Solidcore Agent on the clients
- Activating the Solidcore Agent on the clients

4.3.5 Adding the Solidcore Agent Deployment Package to the ePO Repository

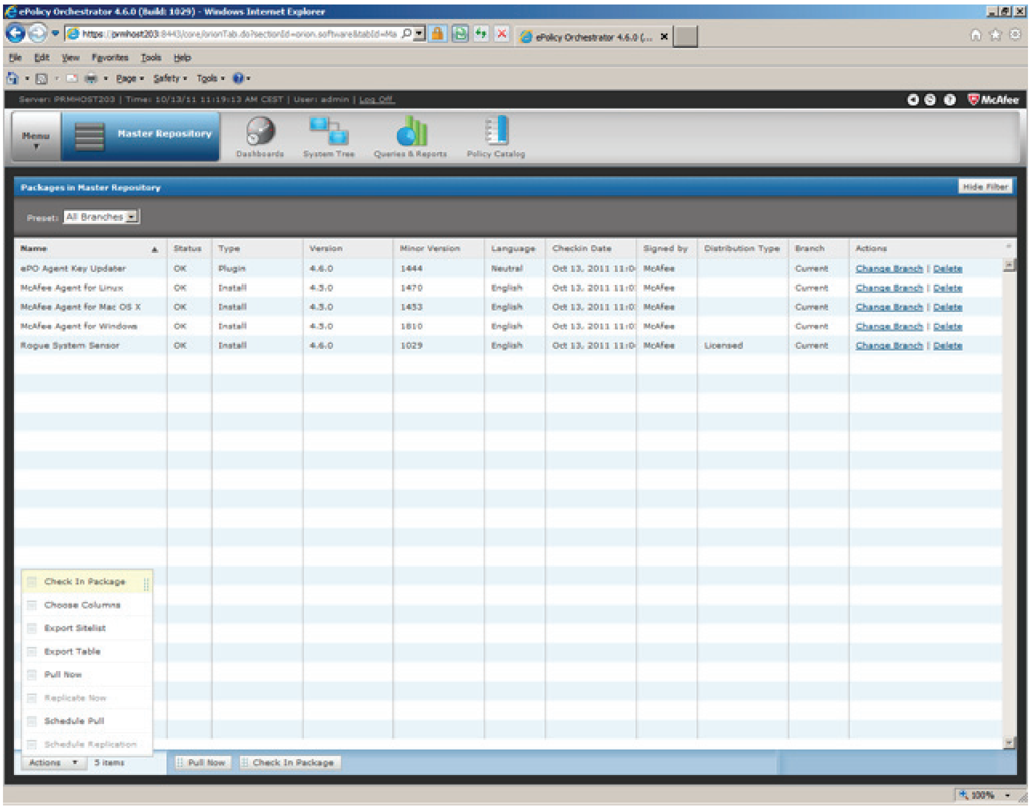
Adding the Solidcore Agent Deployment Package to the ePO Repository

Follow these steps to add the Solidcore Agent Deployment Package to the ePO Software Repository:

1. In the ePO 4.6 console, point to the menu Software > Master Repository.

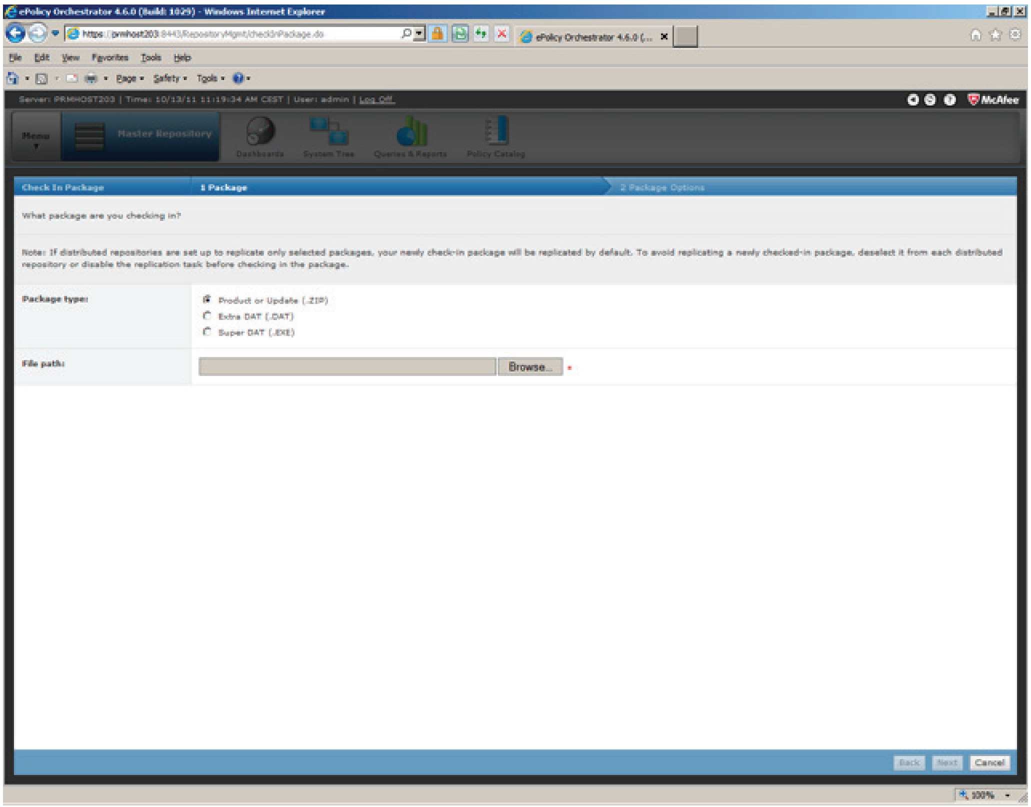

ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
File Edit View Favorites Tools Help
Page Safety Tools
Server: PRMHOST203 | Time: 10/13/11 11:18:50 AM CEST | User: admin | Log Off
McAfee
Menu
Dashboards
Dashboards
System Tree
Queries & Reports
Policy Catalog
Reporting
Systems
Policy
Software
Automation
User Management
Configuration
Master Repository
View and edit the packages in the Master Repository.
View and edit the packages in the Master Repository.
Distributed Repositories
Create and edit HTTP, FTP, or UNC package repositories.
Extensions
Install or remove extensions to alter functionality.
Licensing
Obtain a summary of installations of your software on computers that have the McAfee Agent installed.
Software Manager
Check in, update, or remove licensed or evaluation software.
Quick System Search
Go
Use this text box to search systems by System Name, Description, IP Address, DNS Name, User Name, Custom 1, Custom 2, Custom 3 and Custom 4.
McAfee Links
ePolicy Orchestrator Tutorials
Watch video tutorials for select ePolicy Orchestrator tasks
Technical Support for Enterprise Products
Go to the McAfee Enterprise Support home page
Minimum Escalation Requirement Tool
Collect information for Support about your system
Virus Information Library
Find detailed information on various threats
McAfee Labs WebImmune
Submit potentially infected files for analysis
McAfee, Inc. Home Page
Go to the McAfee home page
Query did not return any results.
Number of Threat Events
Event Generated Time
100%

2. In the "Packages in the Master Repository" window, click "Actions" to select the "Check In Package" action.



Name	Status	Type	Version	Minor Version	Language	Checkin Date	Signed by	Distribution Type	Branch	Actions
ePO Agent Key Updater	OK	Plugin	4.6.0	1444	Neutral	Oct 13, 2011 11:0	McAfee		Current	Change Branch | Delete
McAfee Agent for Linux	OK	Install	4.5.0	1470	English	Oct 13, 2011 11:0	McAfee		Current	Change Branch | Delete
McAfee Agent for Mac OS X	OK	Install	4.5.0	1453	English	Oct 13, 2011 11:0	McAfee		Current	Change Branch | Delete
McAfee Agent for Windows	OK	Install	4.5.0	1810	English	Oct 13, 2011 11:0	McAfee		Current	Change Branch | Delete
Rogue System Sensor	OK	Install	4.6.0	1029	English	Oct 13, 2011 11:0	McAfee	Licensed	Current	Change Branch | Delete

3. Select the "Product or Update (.ZIP)" package type. You can click "Browse…" to select the Solidcore Agent Package.



ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
https://prmhost203:8443/RepositoryMgmt/checkInPackage.do
ePolicy Orchestrator 4.6.0 (...
File Edit View Favorites Tools Help
Page Safety Tools
Server: PRMHOST203 | Time: 10/13/11 11:19:34 AM CEST | User: admin | Log Off
McAfee
Menu
Master Repository
Dashboards
System Tree
Queries & Reports
Policy Catalog
Check In Package
1 Package
2 Package Options
Back
Next
Cancel
100%

What package are you checking in?

Note: If distributed repositories are set up to replicate only selected packages, your newly check-in package will be replicated by default. To avoid replicating a newly checked-in package, deselect it from each distributed repository or disable the replication task before checking in the package.

Package type:
- ● Product or Update (.ZIP)
- ○ Extra DAT (.DAT)
- ○ Super DAT (.EXE)

File path: Browse... *

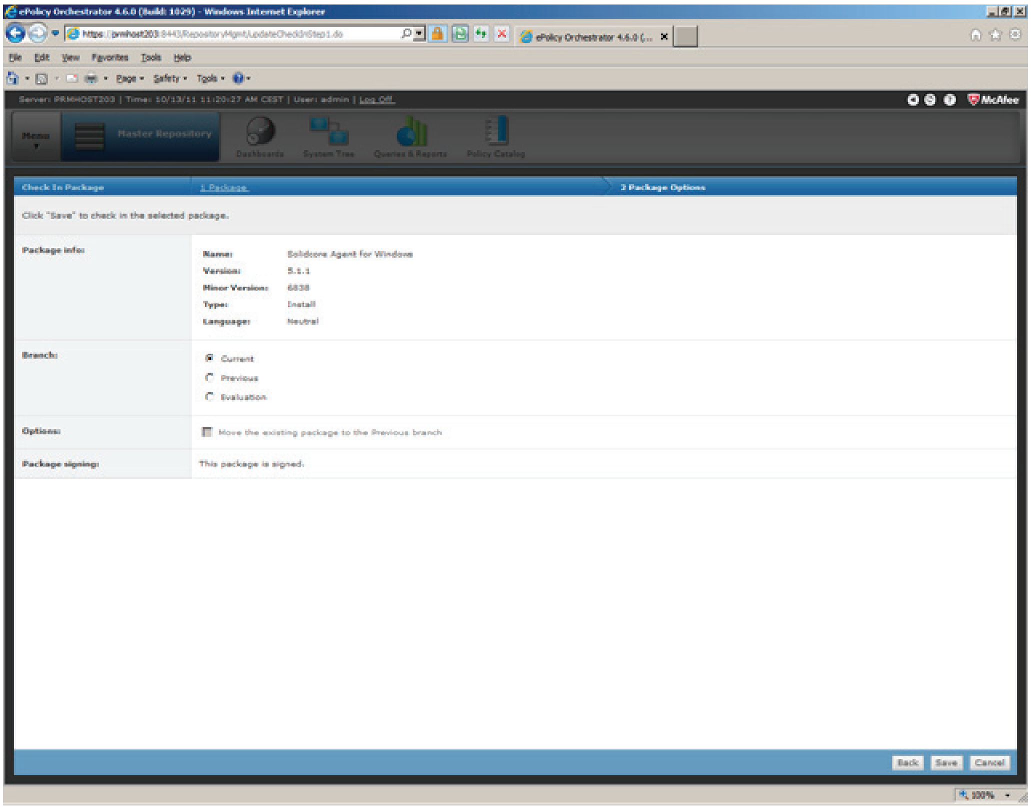
4. Click Next. The Package Options page appears.

   Confirm the following:

   – Package Info: Confirm that this is the correct package (correct name, version, type, and language).

   – Branch: "Current" must be selected.

   – Package signing: This specifies if the package is signed by McAfee or is a third-party package.

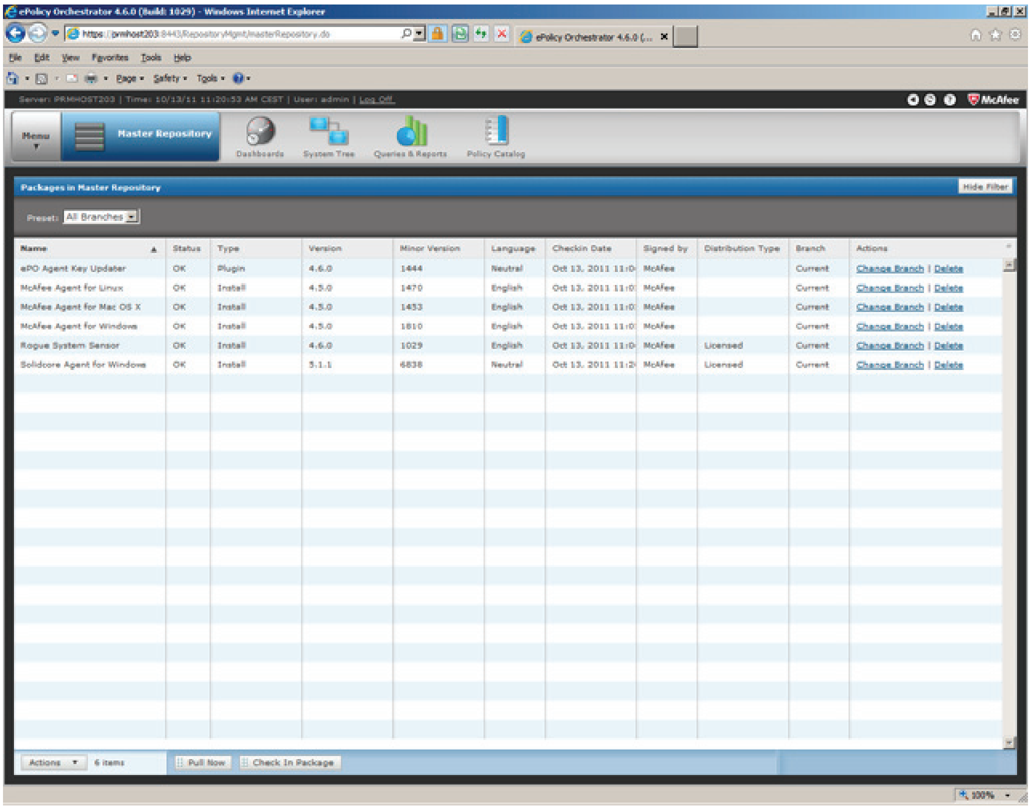


ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
https://prmhost203:8443/RepositoryMgmt/updateCheckInStep1.do
ePolicy Orchestrator 4.6.0 (...
File Edit View Favorites Tools Help
Page Safety Tools
Server: PRMHOST203 | Time: 10/13/11 11:20:27 AM CEST | User: admin | Log Off
McAfee
Menu
Master Repository
Dashboards
System Tree
Queries & Reports
Policy Catalog
Check In Package
1 Package
2 Package Options

Click "Save" to check in the selected package.

Package info:	Name: Solidcore Agent for Windows Version: 5.1.1 Minor Version: 6838 Type: Install Language: Neutral
Branch:	● Current ○ Previous ○ Evaluation
Options:	□ Move the existing package to the Previous branch
Package signing:	This package is signed.

5. Click "Save" to begin checking in the package. The new package appears in Packages in Master Repository list on the Master Repository tab.



ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
File Edit View Favorites Tools Help
Page Safety Tools
Server: PRMHOST203 | Time: 10/13/11 11:20:53 AM CEST | User: admin | Log Off
McAfee
Menu
Master Repository
Dashboards
System Tree
Queries & Reports
Policy Catalog
Hide Filter
Actions
Pull Now
Check In Package
100%

Packages in Master Repository

Preset: All Branches

Name	Status	Type	Version	Minor Version	Language	Checkin Date	Signed by	Distribution Type	Branch	Actions
ePO Agent Key Updater	OK	Plugin	4.6.0	1444	Neutral	Oct 13, 2011 11:0	McAfee		Current	Change Branch | Delete
McAfee Agent for Linux	OK	Install	4.5.0	1470	English	Oct 13, 2011 11:0	McAfee		Current	Change Branch | Delete
McAfee Agent for Mac OS X	OK	Install	4.5.0	1453	English	Oct 13, 2011 11:0	McAfee		Current	Change Branch | Delete
McAfee Agent for Windows	OK	Install	4.5.0	1810	English	Oct 13, 2011 11:0	McAfee		Current	Change Branch | Delete
Rogue System Sensor	OK	Install	4.6.0	1029	English	Oct 13, 2011 11:0	McAfee	Licensed	Current	Change Branch | Delete
Solidcore Agent for Windows	OK	Install	5.1.1	6838	Neutral	Oct 13, 2011 11:2	McAfee	Licensed	Current	Change Branch | Delete

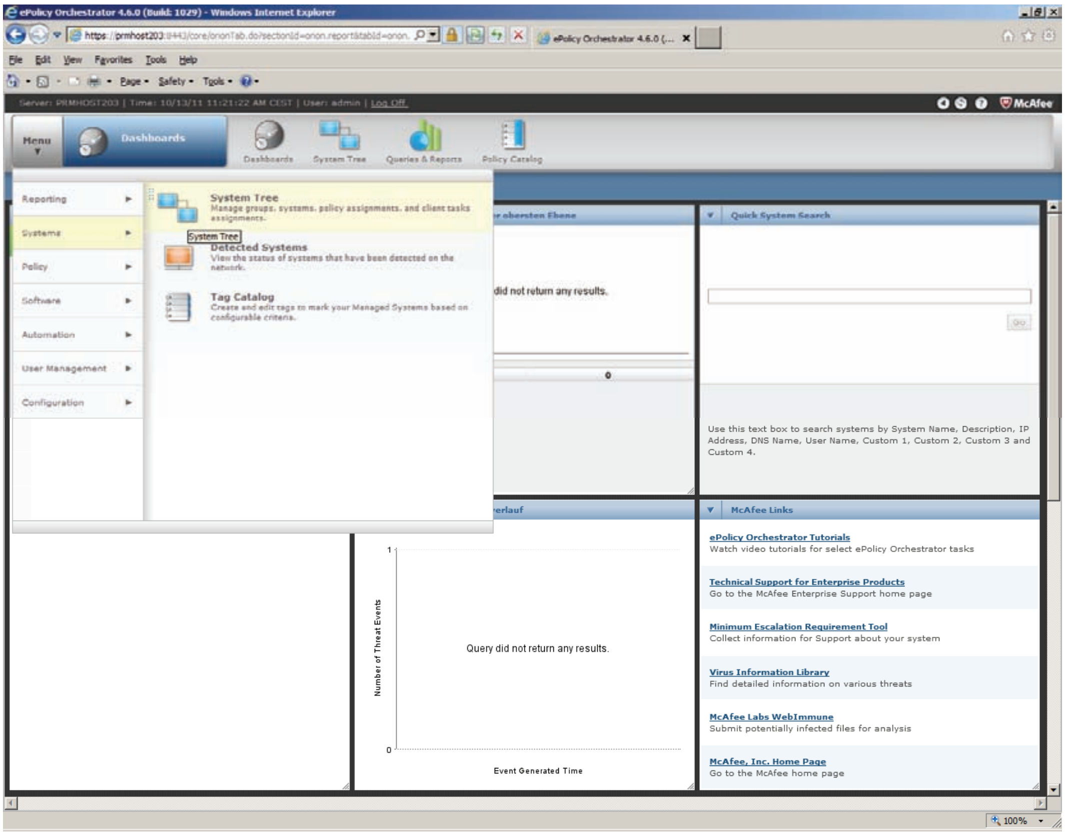
6 items

4.3.6 Integrating the client systems into the ePO Console

Integrating the client systems into the ePO Console

Integrate all clients as new systems in the ePO Console before you install the Solidcore Agent on the clients. Follow these steps:

1. In the ePO 4.6 console, point to the menu Systems > System Tree.



Manage groups, systems, policy assignments, and client tasks assignments.

View the status of systems that have been detected on the network.

Create and edit tags to mark your Managed Systems based on configurable criteria.

did not return any results.

Use this text box to search systems by System Name, Description, IP Address, DNS Name, User Name, Custom 1, Custom 2, Custom 3 and Custom 4.

Query did not return any results.

ePolicy Orchestrator Tutorials
Watch video tutorials for select ePolicy Orchestrator tasks

Technical Support for Enterprise Products
Go to the McAfee Enterprise Support home page

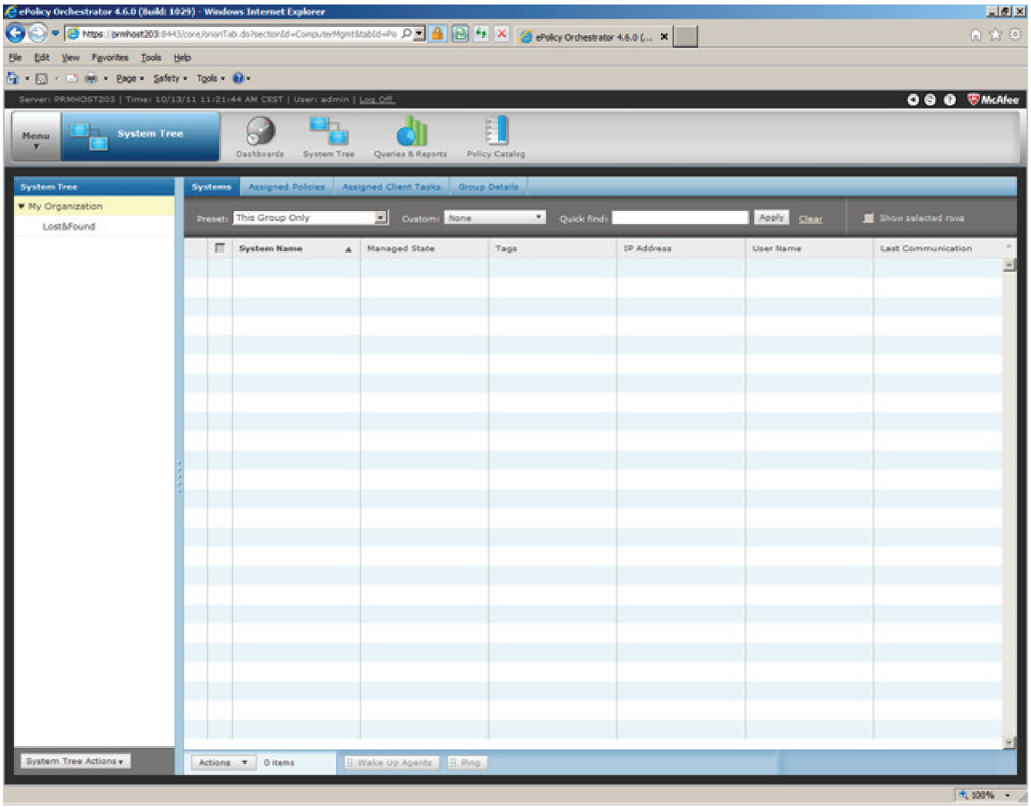
Minimum Escalation Requirement Tool
Collect information for Support about your system

Virus Information Library
Find detailed information on various threats

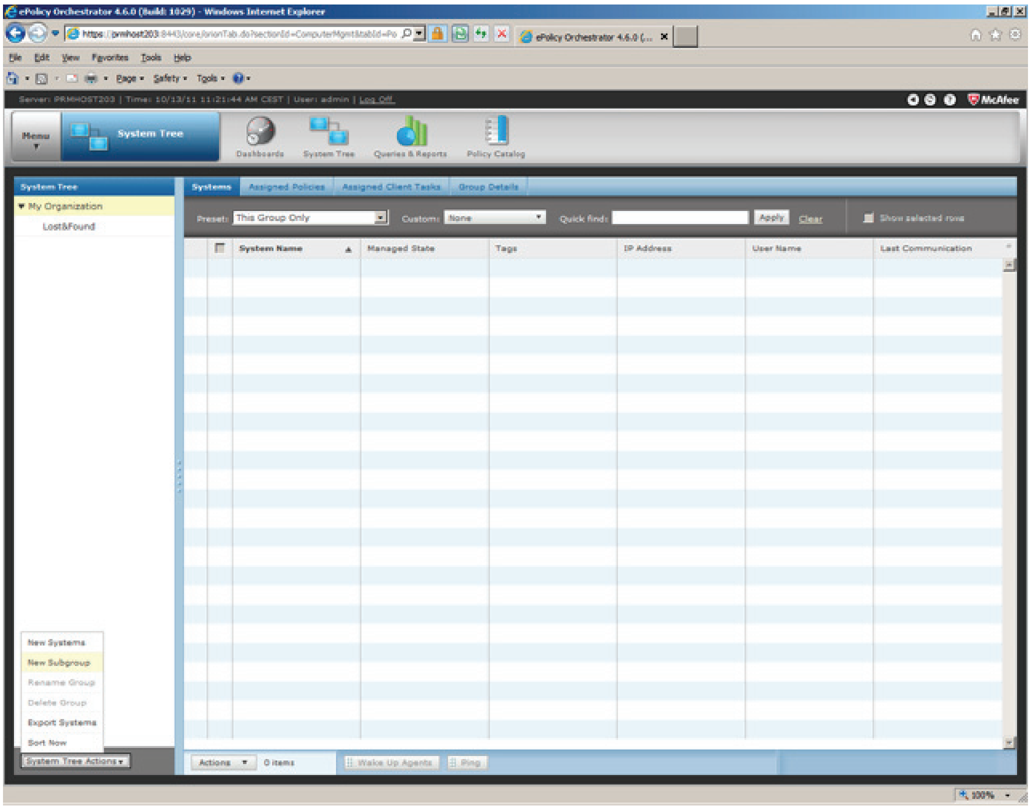
McAfee Labs WebImmune
Submit potentially infected files for analysis

McAfee, Inc. Home Page
Go to the McAfee home page

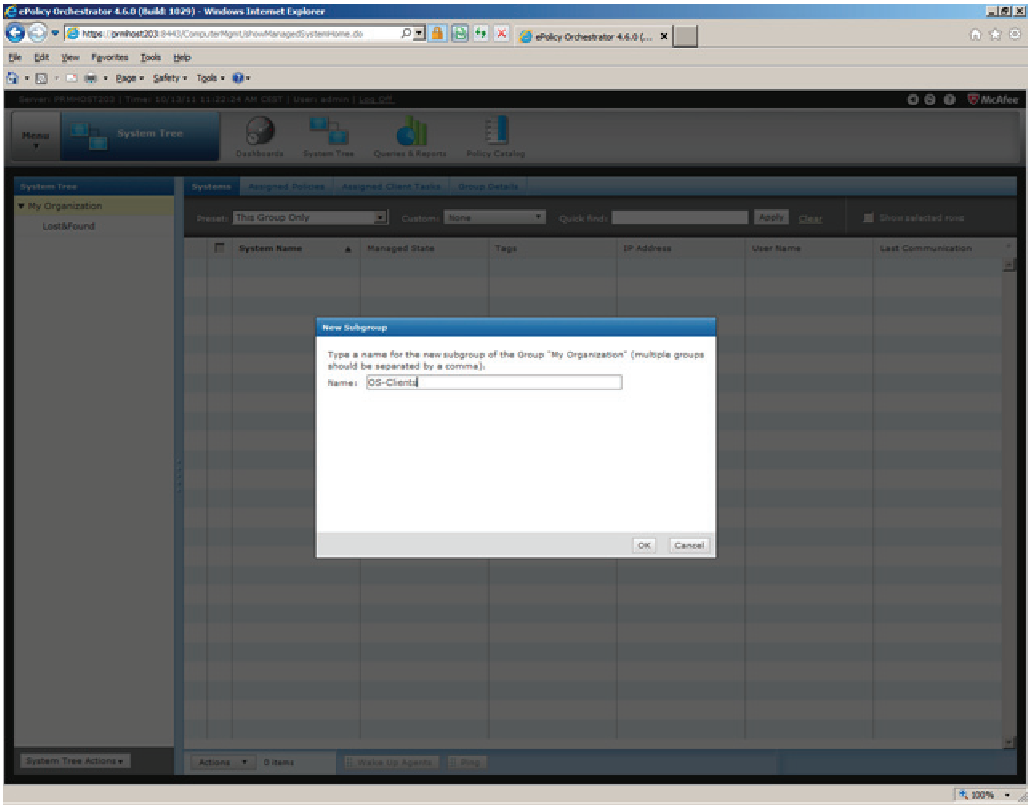
2. The "System Tree" window opens



3. You may assign your clients to different subgroup structures. To create a new subgroup, click on "System Tree Actions" and select the "New Subgroup" command from the menu that is displayed.



4. Enter a name for the subgroup to be created.

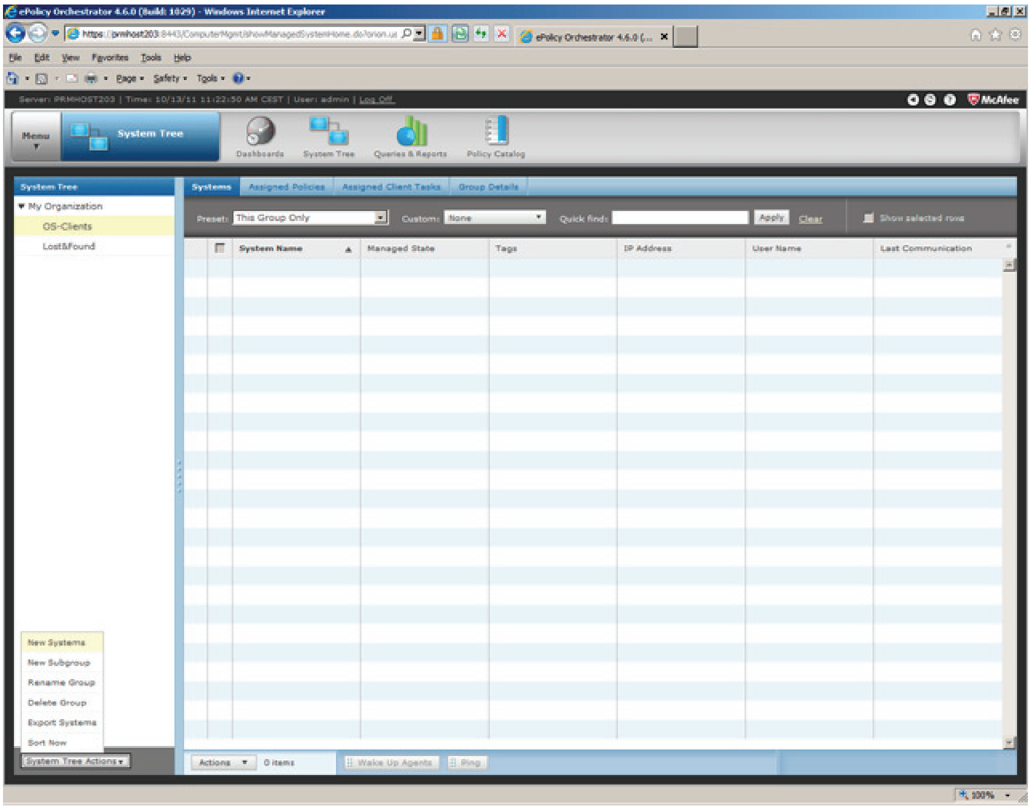


New Subgroup

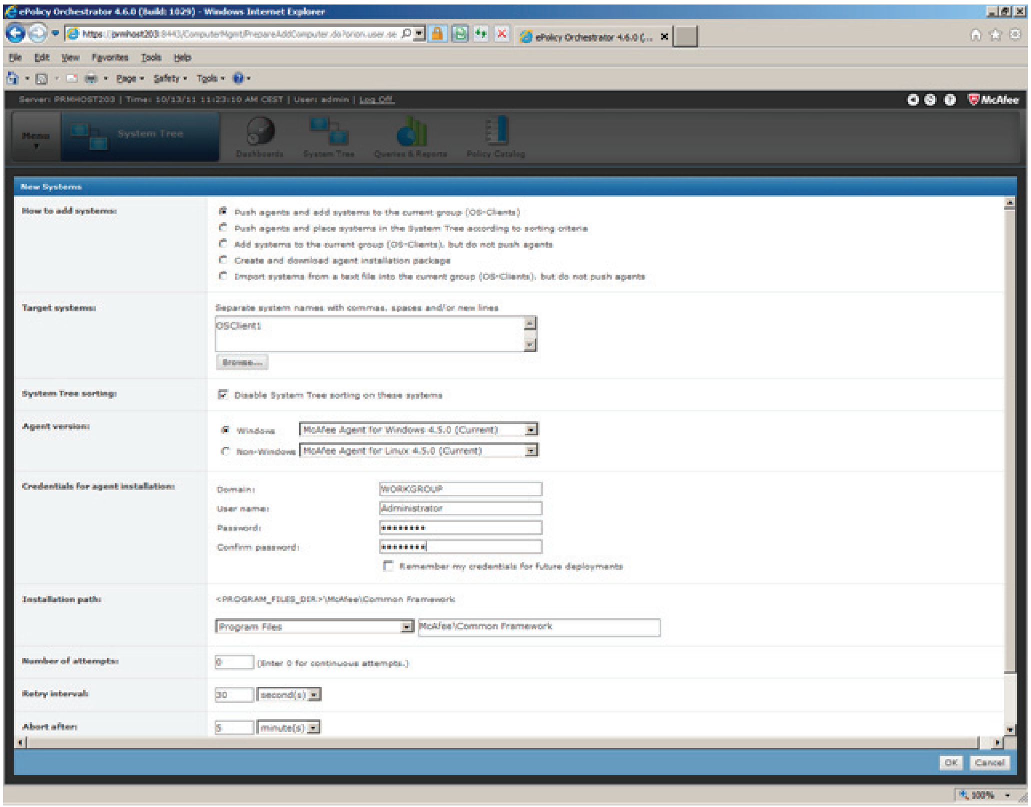
Type a name for the new subgroup of the Group "My Organization" (multiple groups should be separated by a comma).

Name: OS-Clients

5. This new subgroup is now ready for integration of new systems. To add systems, click on "System Tree Actions" and select the "New Systems" command from the menu that is displayed.



6. Enter the following data in the "New Systems" window:
   - Method for adding new systems:
     Push the agents and add the systems to the current group (…).
   - System to add:
     System names of the system(s) to add
   - Agent version:
     McAfee Agent for Windows 4.6.0 (current)
   - Installation path:
     <PROGRAM_FILES_DIR>\McAfee\Common Framework
   - Login information for agent installation:
     Domain:domain or workgroup name
     Username:user name
     Password:password
   - Number of attempts:
     0 = any
   - Retry interval:
     30 seconds
   - Cancellation after:
     5 minutes
   - Connection setup using:
     all agent controls


ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
File Edit View Favorites Tools Help
Page Safety Tools
Server: PRMHOST203 | Time: 10/13/11 11:23:10 AM CEST | User: admin | Log Off
McAfee
Menu
System Tree
Dashboards
System Tree
Queries & Reports
Policy Catalog

New Systems

How to add systems:
● Push agents and add systems to the current group (OS-Clients)
○ Push agents and place systems in the System Tree according to sorting criteria
○ Add systems to the current group (OS-Clients), but do not push agents
○ Create and download agent installation package
○ Import systems from a text file into the current group (OS-Clients), but do not push agents

Target systems: Separate system names with commas, spaces and/or new lines
OSClient1
Browse...

System Tree sorting: ☑ Disable System Tree sorting on these systems

Agent version:
● Windows: McAfee Agent for Windows 4.5.0 (Current)
○ Non-Windows: McAfee Agent for Linux 4.5.0 (Current)

Credentials for agent installation:
Domain: WORKGROUP
User name: Administrator
Password: ••••••••
Confirm password: ••••••••
□ Remember my credentials for future deployments

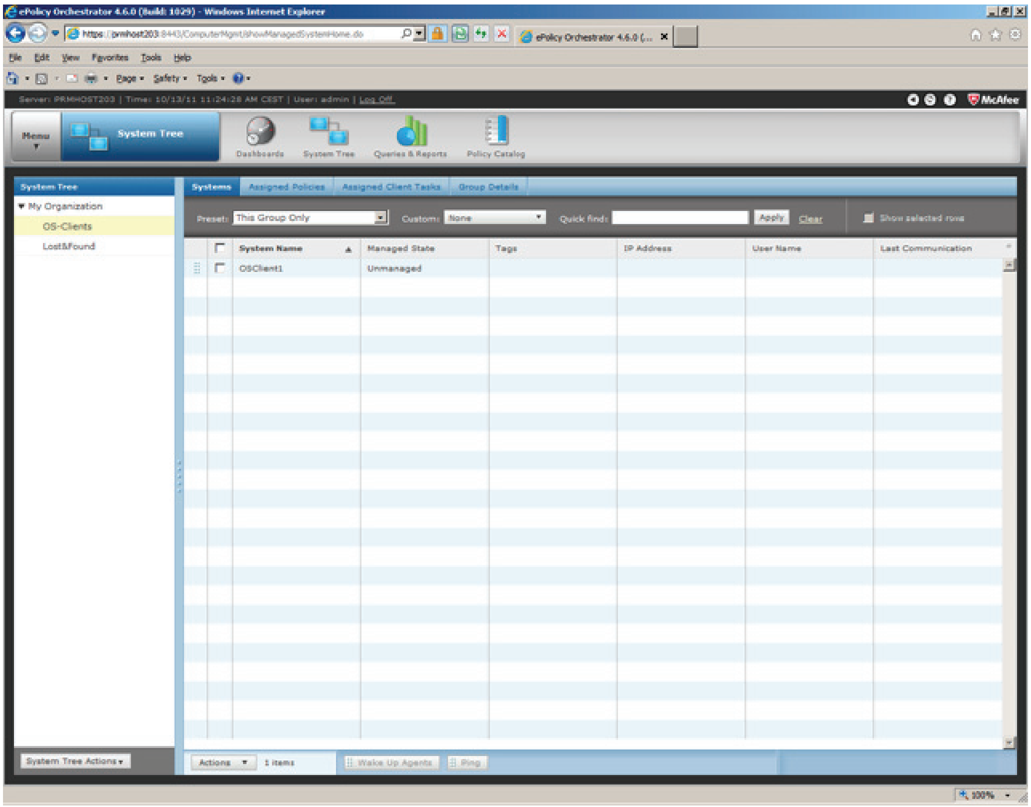
Installation path: <PROGRAM_FILES_DIR>\McAfee\Common Framework
Program Files | McAfee\Common Framework

Number of attempts: 0 (Enter 0 for continuous attempts.)

Retry interval: 30 second(s)

Abort after: 5 minute(s)

7. Confirm your entries with "OK".



Preset: This Group Only   Custom: None   Quick find:

System Name	Managed State	Tags	IP Address	User Name	Last Communication
OSClient1	Unmanaged				

1 items

Repeat items 5 to 7 and, if necessary, items 1 to 4 until you integrated all clients in the ePO Console.

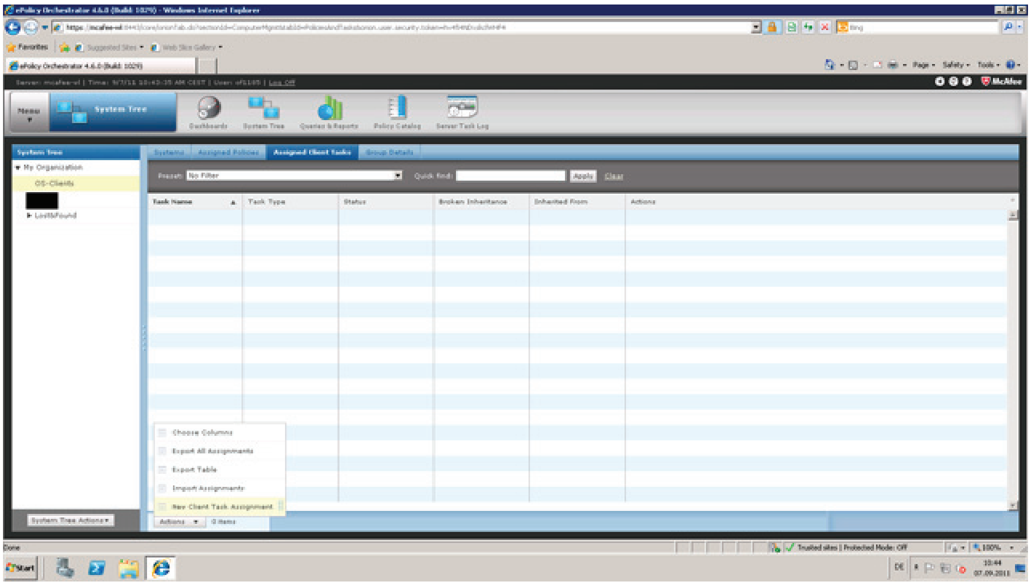
4.3.7 Installing the Solidcore Agent on the clients

Installing the Solidcore Agent on the clients

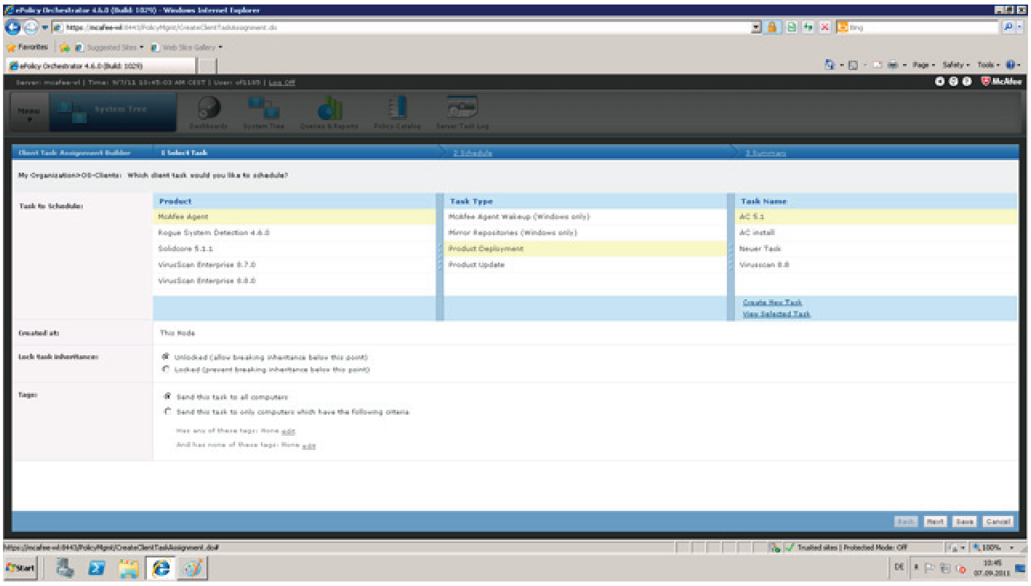
Once you completed integration of all clients in the McAfee ePO Console, you can install the Solidcore Agent on the clients. Follow these steps:

1. In the "System Tree" window, select the "Assigned client tasks" menu.

   Then click on the "Actions" button and select "New client task assignment".



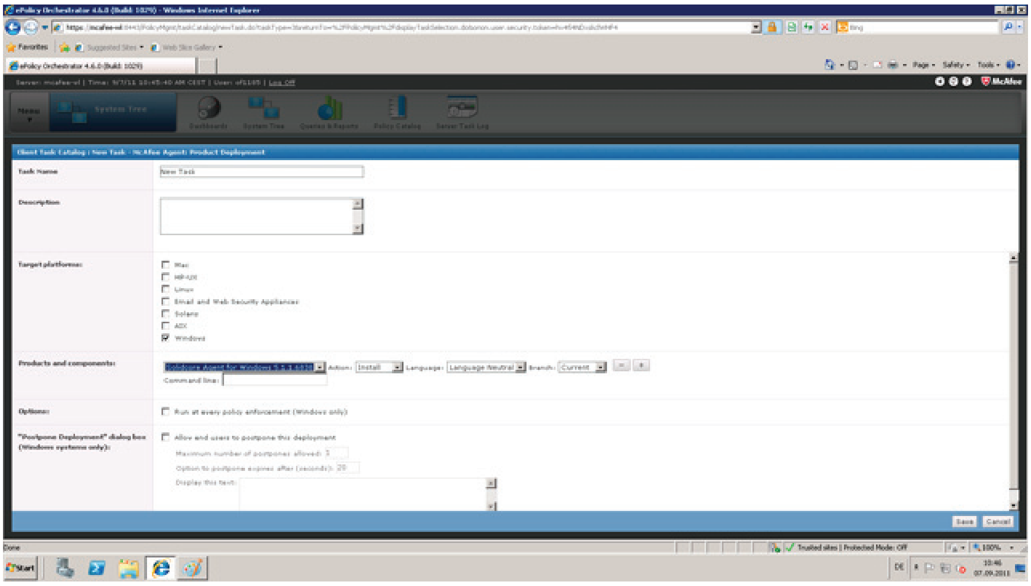
2. In the subsequent window, select McAfee Agent under "Product", select Product Deployment under "Task type" and click on "Create new task". In the Tags area, select the "Send this task to all computers" check box.


ePolicy Orchestrator 4.6.0 (Build: 1029) - Windows Internet Explorer
Client Task Assignment Builder
1 Select Task
2 Schedule
3 Summary
My Organization>OS-Clients: Which client task would you like to schedule?
Task to Schedule:
Product
McAfee Agent
Rogue System Detection 4.6.0
Solidcore 5.1.1
VirusScan Enterprise 8.7.0
VirusScan Enterprise 8.8.0
Task Type
McAfee Agent Wakeup (Windows only)
Mirror Repositories (Windows only)
Product Deployment
Product Update
Task Name
AC 5.1
AC install
Neuer Task
Virusscan 8.8
Create New Task
View Selected Task
Created at:
This Node
Lock task inheritance:
Unlocked (allow breaking inheritance below this point)
Locked (prevent breaking inheritance below this point)
Tags:
Send this task to all computers
Send this task to only computers which have the following criteria:
Has any of these tags: None edit
And has none of these tags: None edit
Back
Next
Save
Cancel

3. In the subsequent window, assign the new task a name and a message text. Select the following:
   - for "Target platforms"

     "Windows"
   - for "Products and components"

     "Solidcore Agent for Windows 5.1.1.xxx ".
   - Then click "Save".



Client Task Catalog : New Task - McAfee Agent: Product Deployment

Task Name: New Task

Description:

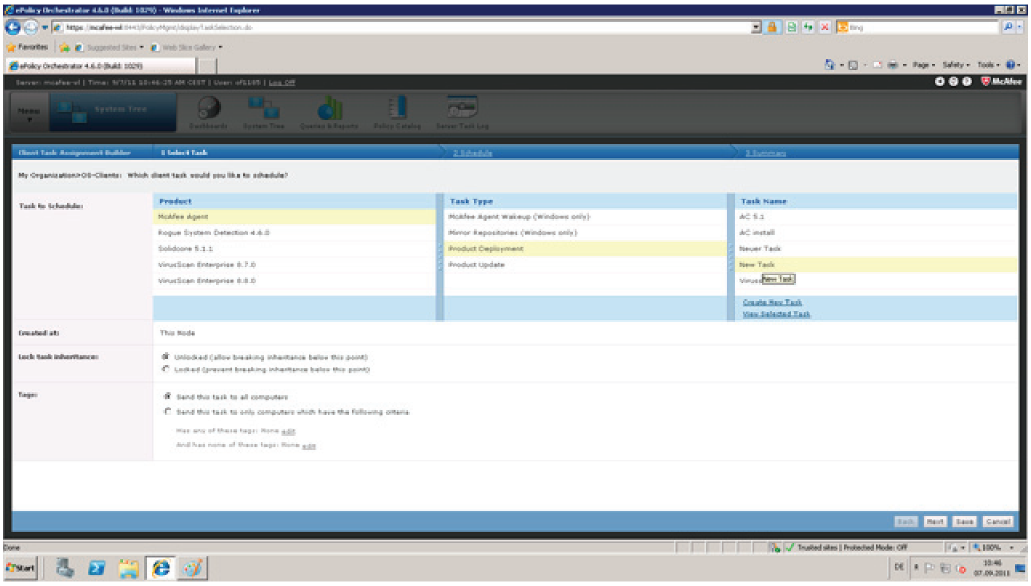
Target platforms:
☐ Mac
☐ HP-UX
☐ Linux
☐ Email and Web Security Appliances
☐ Solaris
☐ AIX
☑ Windows

Products and components: Solidcore Agent for Windows 5.1.1.xxx Action: Install Language: Language Neutral Branch: Current
Command line:

Options: ☐ Run at every policy enforcement (Windows only)

"Postpone Deployment" dialog box (Windows systems only): ☐ Allow end users to postpone this deployment
Maximum number of postpones allowed: 1
Option to postpone expires after (seconds): 20
Display this text:

4. Now select your task under "Task name" and click "Next".



Client Task Assignment Builder — 1 Select Task — 2 Schedule — 3 Summary

My Organization>OS-Clients: Which client task would you like to schedule?

Task to Schedule:

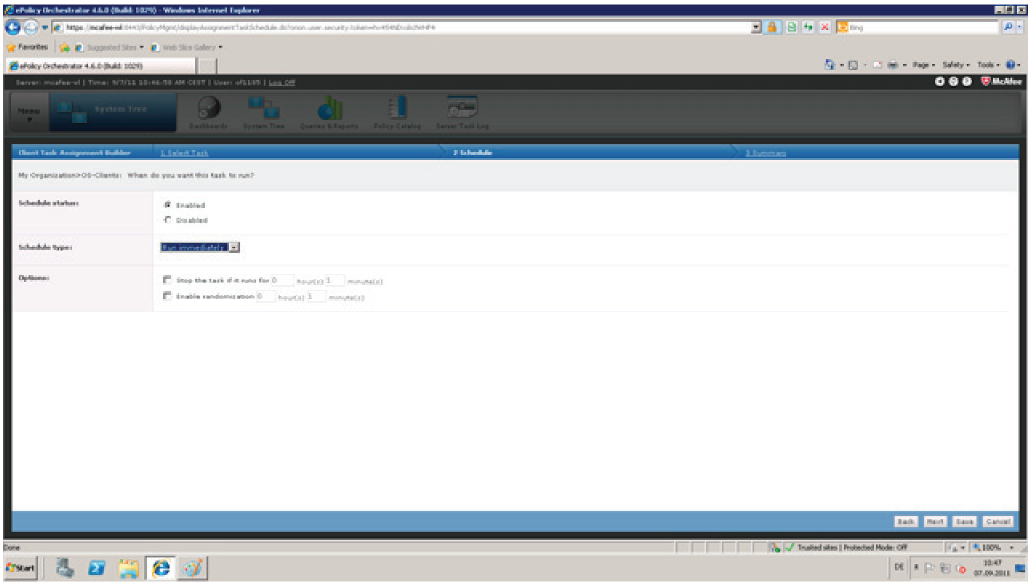
Product	Task Type	Task Name
McAfee Agent	McAfee Agent Wakeup (Windows only)	AC 5.1
Rogue System Detection 4.6.0	Mirror Repositories (Windows only)	AC install
Solidcore 5.1.1	Product Deployment	Neuer Task
VirusScan Enterprise 8.7.0	Product Update	New Task
VirusScan Enterprise 8.8.0		Virus...

Created at: This Node

Lock task inheritance:
● Unlocked (allow breaking inheritance below this point)
○ Locked (prevent breaking inheritance below this point)

Tags:
● Send this task to all computers
○ Send this task to only computers which have the following criteria:
Has any of these tags: None edit
And has none of these tags: None edit

5. In this window, you plan the execution of tasks on the client station. Select the "Activated" option as corresponding planning status. Select "Execute immediately" from the selection list for the planning status.



Client Task Assignment Builder | 1 Select Task | 2 Schedule | 3 Summary

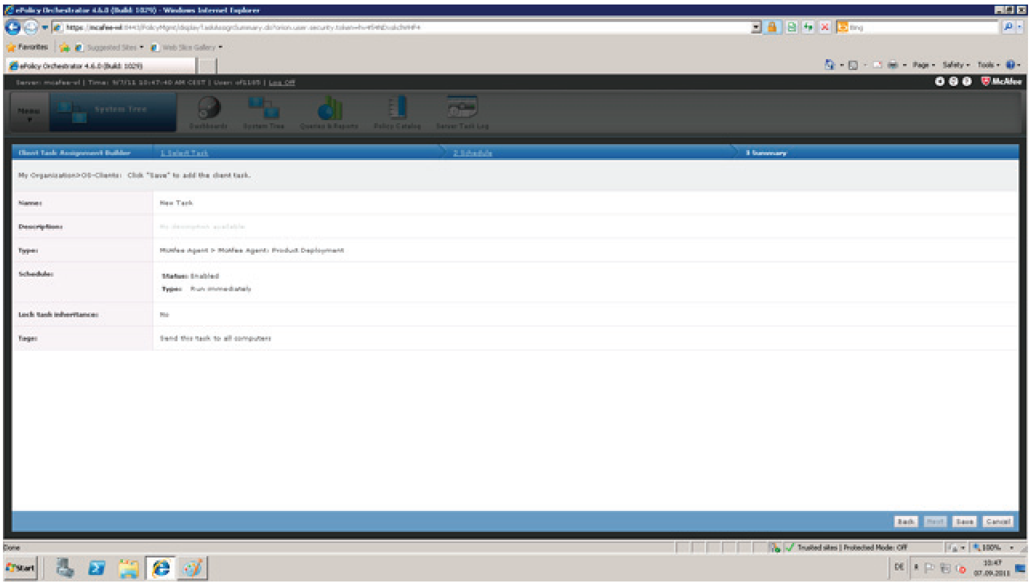
My Organization>OS-Clients: When do you want this task to run?

Schedule status: ● Enabled ○ Disabled

Schedule type: Run immediately

Options: □ Stop the task if it runs for 0 hour(s) 1 minute(s)
□ Enable randomization 0 hour(s) 1 minute(s)

6. Click "Next" to open a window that once again displays the settings you made for this new client task. Check the settings you made. Keep clicking the "Back" button until the window opens in which you can correct the relevant setting. Click "Save" if all settings are OK.



Client Task Assignment Builder | 1 Select Task | 2 Schedule | 3 Summary

My Organization>OS-Clients: Click "Save" to add the client task.

Name:	New Task
Description:	No description available
Type:	McAfee Agent > McAfee Agent: Product Deployment
Schedule:	Status: Enabled Type: Run immediately
Lock task inheritance:	No
Tags:	Send this task to all computers

7. The clients will now start automatic installation of the Solidcore Agent. You can monitor the status in the "System Tree" view.

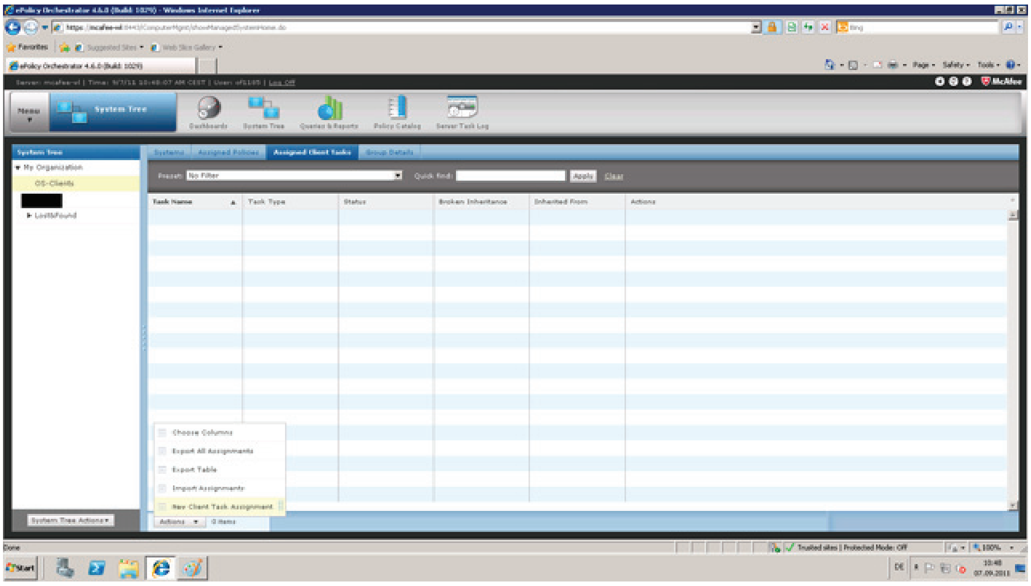
4.3.8 Activating the Solidcore Agent on the clients

Activating the Solidcore Agent on the clients

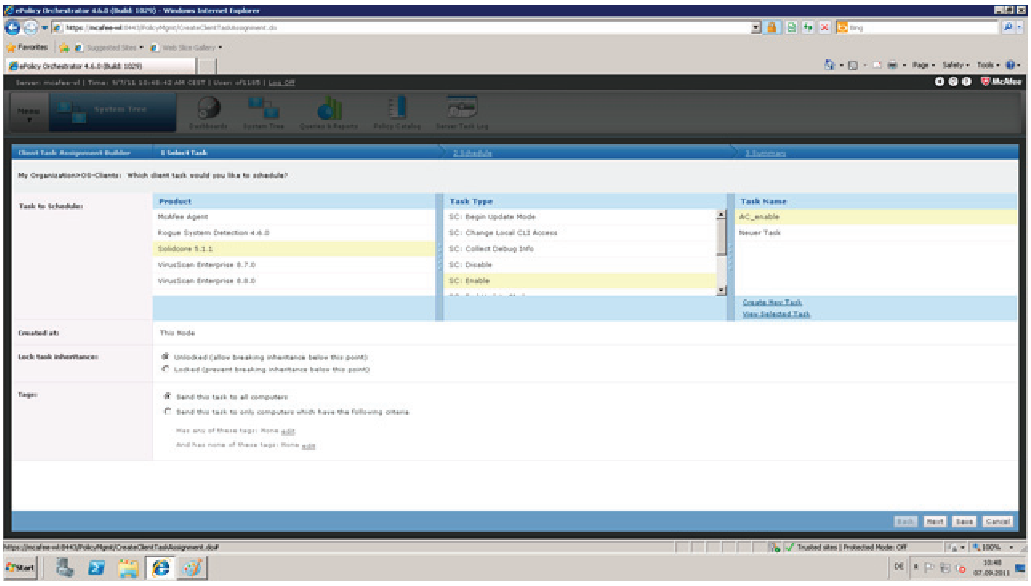
After having installed the Solidcore Agent on all clients, activate McAfee Application Control or Solidcore on the clients. However, before you activate the clients you need to run a "solidify" action exactly as in local administration to create the Whitelist. You can initiate this action, namely solidification and activation of Solidcore on the clients, by means of a client task. Follow these steps to create this client task:

1. In the "System Tree" window, select the "Assigned client tasks" menu.

   Then click on the "Actions" button and select "New client task assignment".



2. In the subsequent dialog, select Solidcore 5.1.1 under "Product" and, under Task-type", SC: Activate and click on "Create new task". In the Tags area, select the "Send this task to all computers" check box.



Client Task Assignment Builder | 1 Select Task | 2 Schedule | 3 Summary

My Organization>OS-Clients: Which client task would you like to schedule?

Task to Schedule:

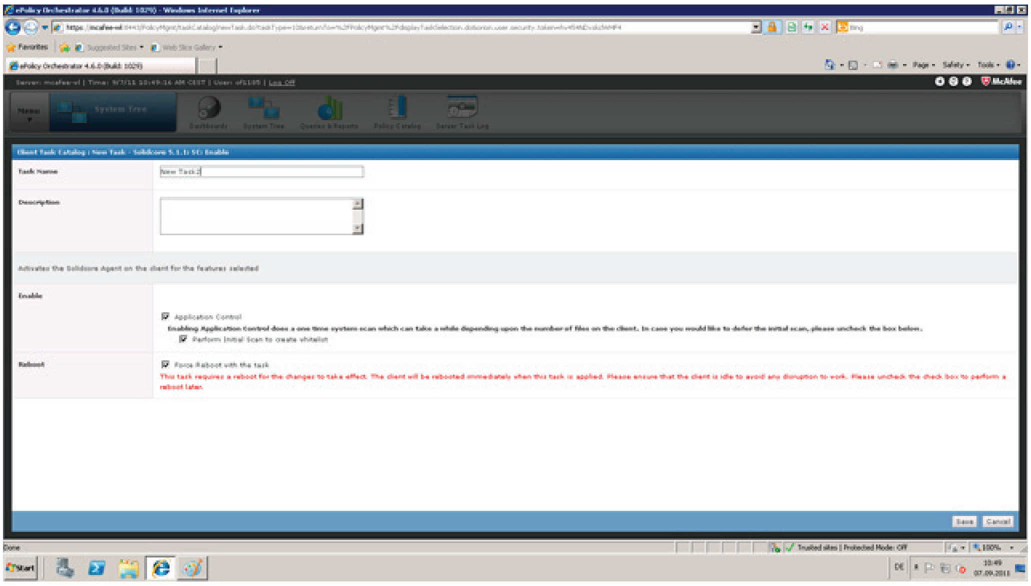
Product	Task Type	Task Name
McAfee Agent	SC: Begin Update Mode	AC_enable
Rogue System Detection 4.6.0	SC: Change Local CLI Access	Neuer Task
Solidcore 5.1.1	SC: Collect Debug Info	
VirusScan Enterprise 8.7.0	SC: Disable	
VirusScan Enterprise 8.8.0	SC: Enable	

Created at: This Node

Lock task inheritance:
● Unlocked (allow breaking inheritance below this point)
○ Locked (prevent breaking inheritance below this point)

Tags:
● Send this task to all computers
○ Send this task to only computers which have the following criteria.
Has any of these tags: None edit
And has none of these tags: None edit

3. Enter the jobs that this new task has to execute. Select "Application Control" for the "Activate" menu command and "Execute initial scan to create the whitelist" to specify that Solidcore Agent has to solidify the client. In the "Restart" field, select "Force restart for this task". Then click "Save".



Client Task Catalog : New Task - Solidcore 5.1.1: SC: Enable

Task Name: New Task2

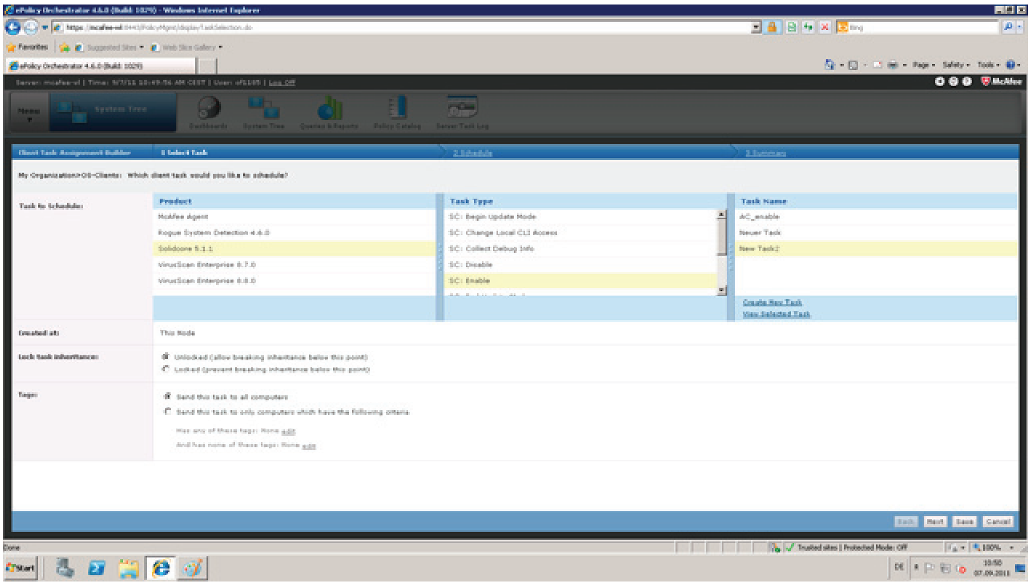
Description:

Activates the Solidcore Agent on the client for the features selected

Enable:
☑ Application Control
Enabling Application Control does a one time system scan which can take a while depending upon the number of files on the client. In case you would like to defer the initial scan, please uncheck the box below.
☑ Perform Initial Scan to create whitelist

Reboot:
☑ Force Reboot with the task
This task requires a reboot for the changes to take effect. The client will be rebooted immediately when this task is applied. Please ensure that the client is idle to avoid any disruption to work. Please uncheck the check box to perform a reboot later.

4. Select your task under "Task name" and click "Next".



Client Task Assignment Builder | 1 Select Task | 2 Schedule | 3 Summary

My Organization>OS-Clients: Which client task would you like to schedule?

Task to Schedule:

Product	Task Type	Task Name
McAfee Agent	SC: Begin Update Mode	AC_enable
Rogue System Detection 4.6.0	SC: Change Local CLI Access	Neuer Task
Solidcore 5.1.1	SC: Collect Debug Info	New Task2
VirusScan Enterprise 8.7.0	SC: Disable	
VirusScan Enterprise 8.8.0	SC: Enable	

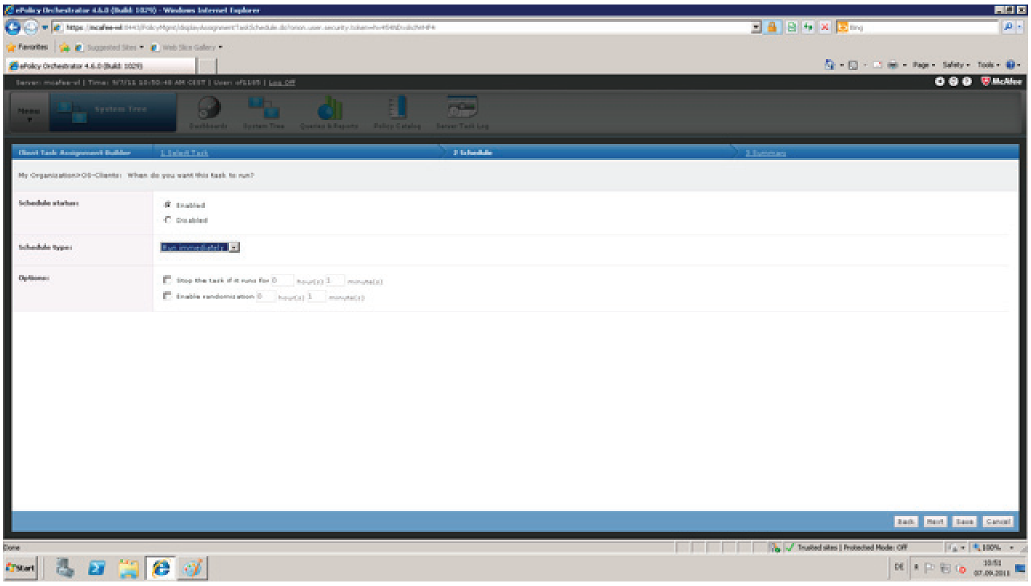
Create New Task
View Selected Task

Created at: This Node

Lock task inheritance:
● Unlocked (allow breaking inheritance below this point)
○ Locked (prevent breaking inheritance below this point)

Tags:
● Send this task to all computers
○ Send this task to only computers which have the following criteria:
Has any of these tags: None edit
And has none of these tags: None edit

5. Click "Next" to open the planning window of the new task. In this window, you plan the execution of tasks on the client station. Select the "Activated" option as corresponding planning status. Select "Execute immediately" from the selection list for the planning status.



Client Task Assignment Builder | 1 Select Task | 2 Schedule | 3 Summary

My Organization>OS-Clients: When do you want this task to run?

Schedule status:
● Enabled
○ Disabled

Schedule type: Run immediately

Options:
□ Stop the task if it runs for 0 hour(s) 1 minute(s)
□ Enable randomization 0 hour(s) 1 minute(s)

6. Click "Next" to open a window that once again displays the settings you made for this new client task. Check the settings you made. Keep clicking the "Back" button until the window opens in which you can correct the relevant setting. Click "Save" if all settings are OK.

7. The clients will automatically start the scan (solidify) to generate the Whitelist. Application Control is then activated and the client restarted by the Client Solidcore Agent as specified in the menu command "Restart". You can monitor the status in the "System Tree" view.

4.3.9 Additional client tasks

The procedure described above can be employed to create additional client tasks for controlling the Solidcore Agent on the clients. For example, it is possible to disable Solidcore Agent on the client(s)
(SC: Disable (Solidcore 5.1.1)". Proceed exactly as described above and select the corresponding type of client task using the "Type" menu command.

Update installation 5

5.1 Update installation

You can only run authorized applications on computers that are protected with McAfee Application Control. However, in certain scenarios it is possibly necessary to install new applications on a computer, or install an update or hotfix for authorized application.

Examples of such a scenario:

- Installation of Microsoft Security Updates, or Important Updates within the framework of Patch Management.
- Installation of virus pattern updates, or update of the VirusScan engine.
- Installation of hotfixes for SIMATIC products.
- Installation of additional diagnostics tools.

McAfee Application Control offers various options or procedures for authorizing new applications:

- By means of a defined file (binary file)
- By trusted users
- By trusted manufacturers (certificate)
- From a trusted directory
- Installation programs
- By means of Updater (update programs such as WSUS, or virus scanners)

Most users fall back on the use of an update program, namely an "Updater".
An "Updater" is a tool that may be used to modify registered files, or add new files to the "Whitelist". The use of such a tool may be necessary for Windows Updates.

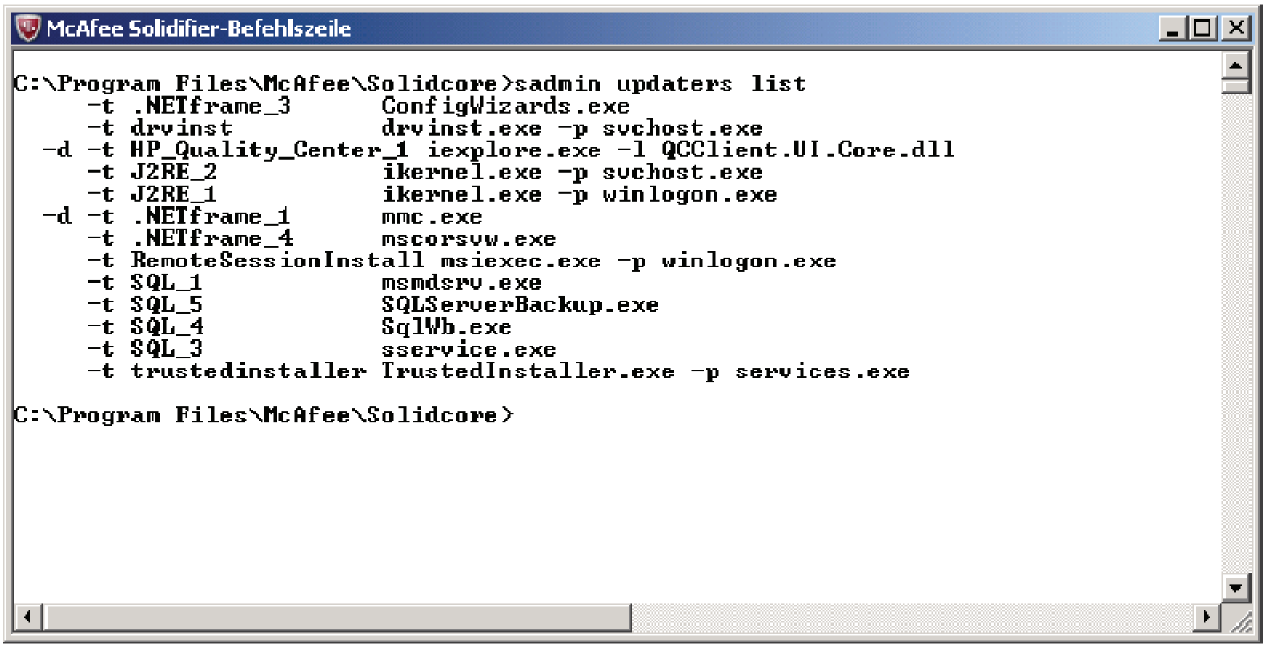
Procedures depend on the way you manage the system.

5.2 Local administration

Local administration

For local administration of McAfee Application Control, the security measures such as Windows Update (Patch Management) or virus scanners that run system updates at cyclic intervals can be enabled using the "finetune.bat" batch file that is available in "C:\Programs\McAfee\Solidcore". This self-explanatory script helps you to enable updates for programs such as WSUS Update Clients.

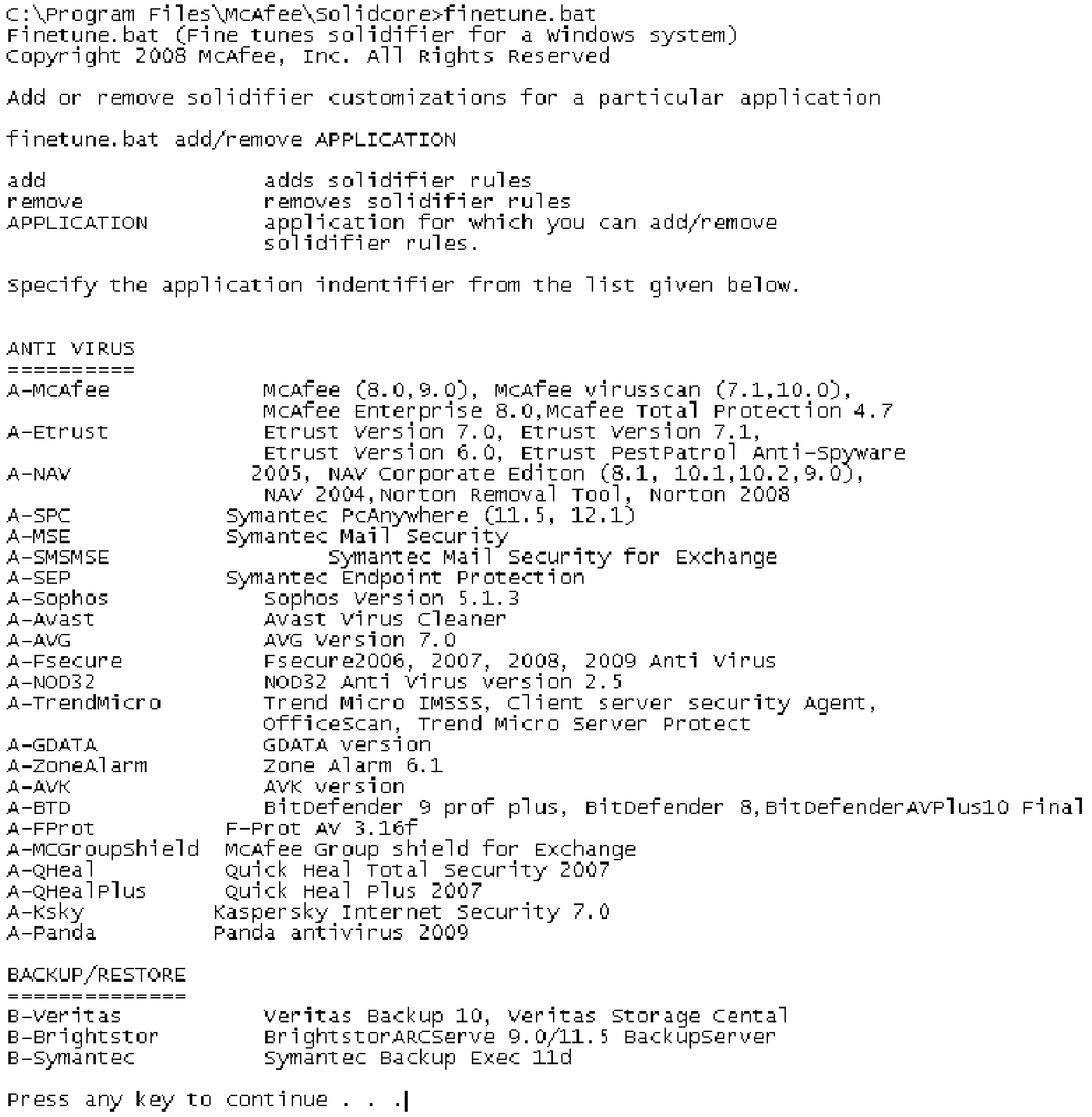
To view the list of authorized update programs, enter the "sadmin updaters list" command at the McAfee Solidifier command line.



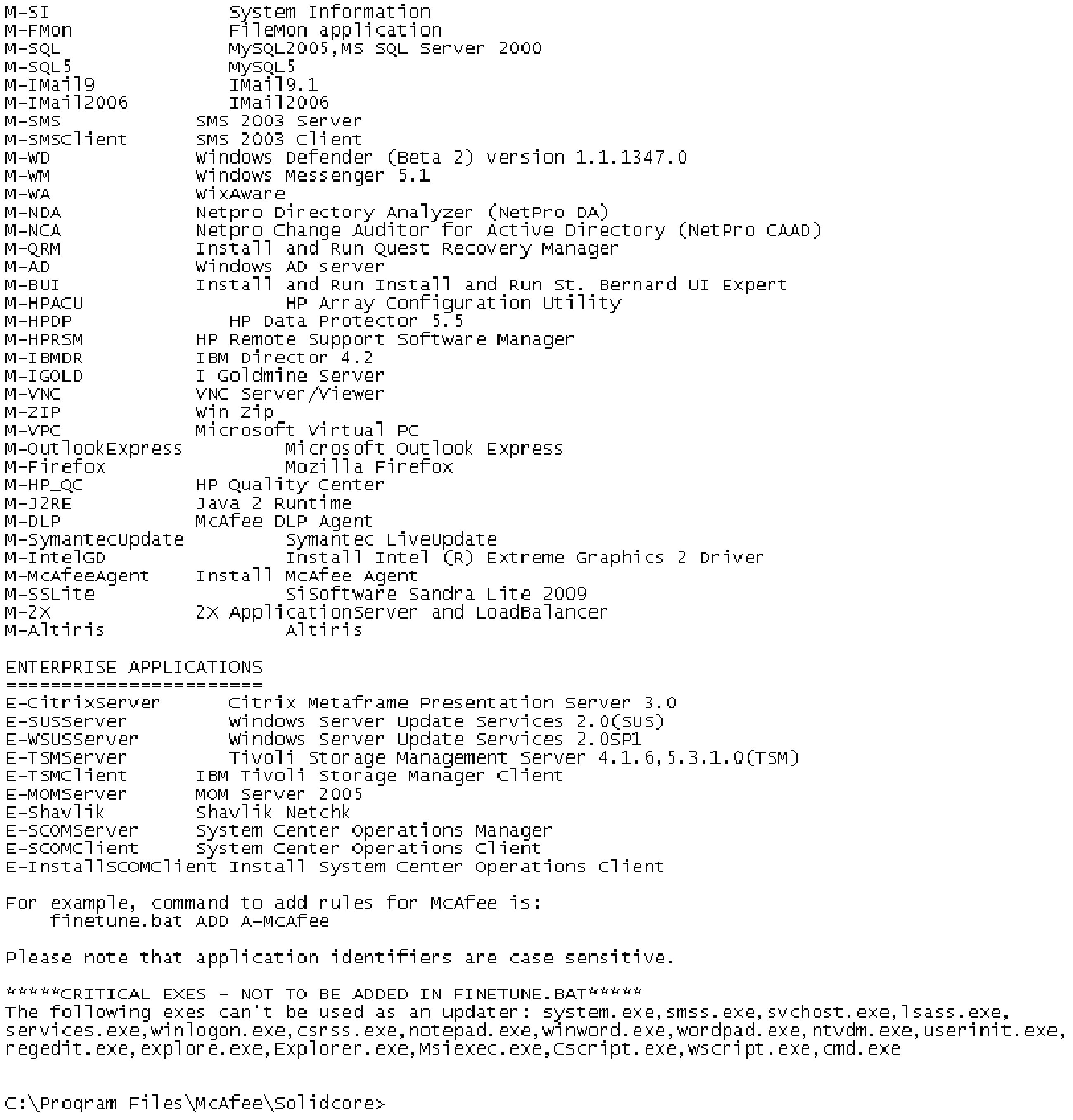
```
C:\Program Files\McAfee\Solidcore>sadmin updaters list
     -t .NETframe_3       ConfigWizards.exe
     -t drvinst           drvinst.exe -p svchost.exe
  -d -t HP_Quality_Center_1 iexplore.exe -l QCClient.UI.Core.dll
     -t J2RE_2            ikernel.exe -p svchost.exe
     -t J2RE_1            ikernel.exe -p winlogon.exe
  -d -t .NETframe_1       mmc.exe
     -t .NETframe_4       mscorsvw.exe
     -t RemoteSessionInstall msiexec.exe -p winlogon.exe
     -t SQL_1             msmdsrv.exe
     -t SQL_5             SQLServerBackup.exe
     -t SQL_4             SqlWb.exe
     -t SQL_3             sservice.exe
     -t trustedinstaller TrustedInstaller.exe -p services.exe

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

Follows these steps to add one of the available update programs:

1. Enter the "finetune.bat" command at the McAfee Solidifier command line. The batch file will list all available updaters:

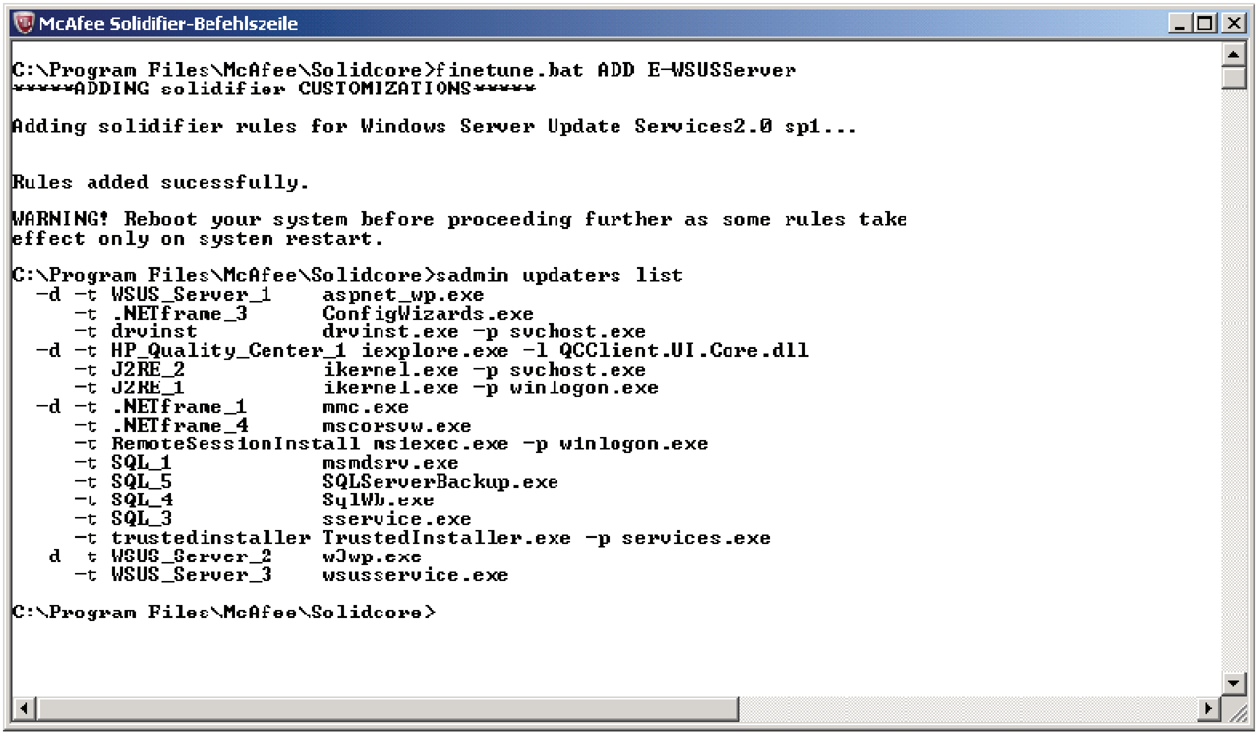


```
C:\Program Files\McAfee\Solidcore>finetune.bat
Finetune.bat (Fine tunes solidifier for a Windows system)
Copyright 2008 McAfee, Inc. All Rights Reserved

Add or remove solidifier customizations for a particular application

finetune.bat add/remove APPLICATION

add                 adds solidifier rules
remove              removes solidifier rules
APPLICATION         application for which you can add/remove
                    solidifier rules.

Specify the application indentifier from the list given below.


ANTI VIRUS
==========
A-McAfee            McAfee (8.0,9.0), McAfee virusscan (7.1,10.0),
                    McAfee Enterprise 8.0,Mcafee Total Protection 4.7
A-Etrust            Etrust Version 7.0, Etrust Version 7.1,
                    Etrust Version 6.0, Etrust PestPatrol Anti-Spyware
A-NAV              2005, NAV Corporate Editon (8.1, 10.1,10.2,9.0),
                    NAV 2004,Norton Removal Tool, Norton 2008
A-SPC             Symantec PcAnywhere (11.5, 12.1)
A-MSE             Symantec Mail Security
A-SMSMSE                  Symantec Mail Security for Exchange
A-SEP             Symantec Endpoint Protection
A-Sophos            Sophos Version 5.1.3
A-Avast             Avast Virus Cleaner
A-AVG               AVG Version 7.0
A-Fsecure           Fsecure2006, 2007, 2008, 2009 Anti Virus
A-NOD32             NOD32 Anti Virus version 2.5
A-TrendMicro        Trend Micro IMSSS, Client server security Agent,
                    OfficeScan, Trend Micro Server Protect
A-GDATA             GDATA version
A-ZoneAlarm         Zone Alarm 6.1
A-AVK               AVK version
A-BTD               BitDefender 9 prof plus, BitDefender 8,BitDefenderAVPlus10 Final
A-FProt           F-Prot AV 3.16f
A-MCGroupShield   McAfee Group shield for Exchange
A-QHeal           Quick Heal Total Security 2007
A-QHealPlus       Quick Heal Plus 2007
A-Ksky           Kaspersky Internet Security 7.0
A-Panda          Panda antivirus 2009

BACKUP/RESTORE
==============
B-Veritas           Veritas Backup 10, Veritas Storage Cental
B-Brightstor        BrightstorARCServe 9.0/11.5 BackupServer
B-Symantec          Symantec Backup Exec 11d

Press any key to continue . . .|
```



```
M-SI                System Information
M-FMon              FileMon application
M-SQL               MySQL2005,MS SQL Server 2000
M-SQL5              MySQL5
M-IMail9            IMail9.1
M-IMail2006         IMail2006
M-SMS            SMS 2003 Server
M-SMSClient      SMS 2003 Client
M-WD             Windows Defender (Beta 2) version 1.1.1347.0
M-WM             Windows Messenger 5.1
M-WA             WixAware
M-NDA            Netpro Directory Analyzer (NetPro DA)
M-NCA            Netpro Change Auditor for Active Directory (NetPro CAAD)
M-QRM            Install and Run Quest Recovery Manager
M-AD             Windows AD server
M-BUI            Install and Run Install and Run St. Bernard UI Expert
M-HPACU                  HP Array Configuration Utility
M-HPDP              HP Data Protector 5.5
M-HPRSM          HP Remote Support Software Manager
M-IBMDR          IBM Director 4.2
M-IGOLD          I Goldmine Server
M-VNC            VNC Server/Viewer
M-ZIP            Win Zip
M-VPC            Microsoft Virtual PC
M-OutlookExpress         Microsoft Outlook Express
M-Firefox                Mozilla Firefox
M-HP_QC          HP Quality Center
M-J2RE           Java 2 Runtime
M-DLP            McAfee DLP Agent
M-SymantecUpdate         Symantec LiveUpdate
M-IntelGD                Install Intel (R) Extreme Graphics 2 Driver
M-McAfeeAgent    Install McAfee Agent
M-SSLite                 SiSoftware Sandra Lite 2009
M-2X             2X ApplicationServer and LoadBalancer
M-Altiris                Altiris

ENTERPRISE APPLICATIONS
=======================
E-CitrixServer      Citrix Metaframe Presentation Server 3.0
E-SUSServer         Windows Server Update Services 2.0(SUS)
E-WSUSServer        Windows Server Update Services 2.0SP1
E-TSMServer         Tivoli Storage Management Server 4.1.6,5.3.1.0(TSM)
E-TSMClient      IBM Tivoli Storage Manager Client
E-MOMServer      MOM Server 2005
E-Shavlik        Shavlik Netchk
E-SCOMServer     System Center Operations Manager
E-SCOMClient     System Center Operations Client
E-InstallSCOMClient Install System Center Operations Client

For example, command to add rules for McAfee is:
    finetune.bat ADD A-McAfee

Please note that application identifiers are case sensitive.

*****CRITICAL EXES - NOT TO BE ADDED IN FINETUNE.BAT*****
The following exes can't be used as an updater: system.exe,smss.exe,svchost.exe,lsass.exe,
services.exe,winlogon.exe,csrss.exe,notepad.exe,winword.exe,wordpad.exe,ntvdm.exe,userinit.exe,
regedit.exe,explore.exe,Explorer.exe,Msiexec.exe,Cscript.exe,wscript.exe,cmd.exe


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

2. To add an updater, enter
   C:\Program Files\McAfee\Solidcore\finetune.bat ADD E-WSUSServer
   . This command adds Windows Server Update Service 2.0 SP1 to the list of updaters on the computer. This means that McAfee Application Control will accept all future changes on the computer which have been made using WSUS 2.0SP1.
3. On completion of this step, you can view the list of authorized updaters (sadmin updaters list) to check whether WSUS has been added.



```
C:\Program Files\McAfee\Solidcore>finetune.bat ADD E-WSUSServer
*****ADDING solidifier CUSTOMIZATIONS*****

Adding solidifier rules for Windows Server Update Services2.0 sp1...


Rules added sucessfully.

WARNING! Reboot your system before proceeding further as some rules take
effect only on systen restart.

C:\Program Files\McAfee\Solidcore>sadmin updaters list
  -d -t WSUS_Server_1    aspnet_wp.exe
     -t .NETframe_3      ConfigWizards.exe
     -t drvinst          drvinst.exe -p svchost.exe
  -d -t HP_Quality_Center_1 iexplore.exe -l QCClient.UI.Core.dll
     -t J2RE_2           ikernel.exe -p svchost.exe
     -t J2RE_1           ikernel.exe -p winlogon.exe
  -d -t .NETframe_1      mmc.exe
     -t .NETframe_4      mscorsvw.exe
     -t RemoteSessionInstall msiexec.exe -p winlogon.exe
     -t SQL_1            msmdsrv.exe
     -t SQL_5            SQLServerBackup.exe
     -t SQL_4            SqlWb.exe
     -t SQL_3            sservice.exe
     -t trustedinstaller TrustedInstaller.exe -p services.exe
   d  t WSUS_Server_2    w3wp.exe
     -t WSUS_Server_3    wsusservice.exe

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

To add the updater for McAfee VirusScan, enter the command
C:\Program Files\McAfee\Solidcore\finetune.bat ADD A-McAfee
.