McAfee Solidcore 5.1.0

Product Guide

Contents

Introduction

This guide describes how to use the McAfee Solidcore extension with McAfee ePolicy Orchestrator software versions 4.0 (Patch 5 or later) and 4.5.

To use this guide effectively, you need to be familiar with ePolicy Orchestrator. For more information, see the ePolicy Orchestrator Product Guide. The ePolicy Orchestrator software provides a single point of control for your McAfee products. Using ePolicy Orchestrator, you can configure Solidcore Agent on target computers across your network.

This guide includes the following information:

- McAfee Solidcore Overview
- Configuring the ePO
- Configuring Policies
- Configuring Client and Server Tasks
- Managing Alerts
- Reports and Queries
- Reconciliation
- Dashboards
- FAQs

NOTE: This guide does not provide detailed information about installing or using ePolicy Orchestrator software for more details, see *ePolicy Orchestrator Product Guide*.

Contents

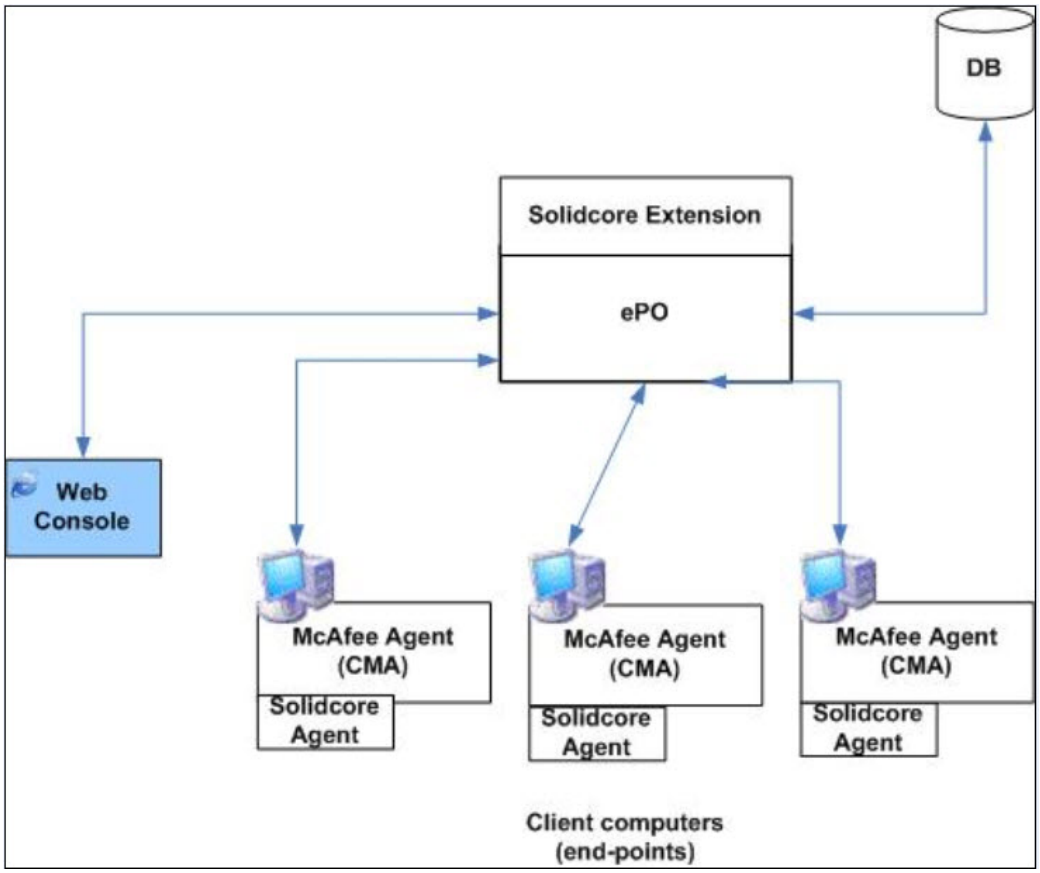
McAfee Solidcore overview

The Solidcore extension is installed on the McAfee ePolicy Orchestrator which acts as a central console. The ePO web server provides the UI for managing McAfee products and for running reports The Solidcore extension stores audit and configuration data in the ePO database.

A Solidcore Agent is installed on a McAfee Agent for enabling:

- Whitelisting with Application Control
- Tracking modifications (changes) to program code and configurations via Integrity Monitor
- Protecting application code and configuration from unapproved changes with Change Control

The Solidcore Agent generate events and send them to the McAfee Agent. The Agent in turn sends the events to the ePO where they can be viewed as queries and reports. The following diagram provides an overview of how the Solidcore extension and the Solidcore Agent fit in with the ePO.



McAfee Change Control overview

McAfee Change Control offers three distinct features:

- File Integrity Monitoring (FIM)
- Change Prevention
- Reconciliation (as an optional add-on)

File Integrity Monitoring gives you details regarding who made changes to what files, when and how the changes were made, thereby giving you comprehensive visibility into attempts to modify critical files and registry keys. Change Prevention can read-protect and or write-protect your critical files and registry keys from unauthorized tampering, such that changes are permitted only if the change is applied in accordance with the update policies. Finally, Reconciliation is the feature where the changes tracked are mapped to their corresponding tickets in a Change Management System (CMS) thereby providing an **evidence trail** for changes made in support of a Request for Change (RFC).

Update policies can be defined using pre-defined change windows, or due to the presence of an approved, open change ticket for a client, or a via a provisioning tool, for example, Opsware, Bladelogic, IBM Tivoli, Windows SMS, as an authorized updater, or via a trusted set of users.

Write protection

Applying write protection rules renders specified files as read only thereby protecting your valuable data from unanticipated updates. You can prevent the following operations on a write-protected file:

- Delete
- Rename
- Create hard links
- Modify contents
- Append
- Truncate
- Change owner
- Create Alternate Data Stream (Windows only)

Write protection for critical registry keys

Write protection on registry keys prevents their modification.

Read protection

Read protection prevents the content of specified files, directories and volumes from being read. When a directory or a volume is subject to read protection, all files in that directory or volume are added to the read protected list. The rules are inherited by sub-directories as well.

NOTE: Read protection is disabled by default and must be enabled at the client where you intended to use it. To enable read-protection, create a SC: Run Commands client task with command to enable the deny-read feature on the client system.

McAfee Integrity Monitor overview

McAfee Integrity Monitor provides real-time monitoring for file and registry changes. It captures every change, including the exact time of the change, who made the change, what program was used for making the change and whether the change was made manually or by an authorized program. It creates a comprehensive central database that is always up-to-date by logging all attempts to modify, or change, files, including Windows Registry keys. Filtering ensures that only relevant changes make it to the database

Real-time monitoring also eliminates the need to perform scan after scan on clients and identifies transient change violations such as when a file is changed and then restored to its earlier state.

NOTE: A scan-based solution cannot capture and report on such transient change violations.

Monitor file and directory changes

The Solidcore Agent monitors change actions in real time, as they happen on files and directories and generates events for the following types of actions:

- Creation
- Modification of contents
- Deletion
- Renaming
- File attribute modification

- ACL modification
- Owner modification

Customization of filters

Filters can be set on file names, directory names, registry keys, process names, file extensions, and user names. Filters can be configured in two different modes:

- Include filters cause events matching the filtering criterion to be reported to the user.
- Exclude filters cause events matching the condition to be suppressed and not reported to the user.

Filtering of Integrity Monitoring events is essential in order to govern the volume of change events, primarily because a large volume of changes are program-generated and may not be worth the attention of the system administrator. In the extreme situation, where there is a lot of programmatic and automatic change activity, a large volume of change events may overwhelm the system generating the events. Filters ensure that only relevant change events are recorded.

McAfee Application Control overview

McAfee Application Control uses dynamic whitelisting to ensure that only trusted applications run on servers and clients. This provides IT with the greatest degree of visibility and control over clients, and helps enforce software license compliance. Additionally, McAfee Application Control extends the viability of fixed function systems, without impacting system performance.

Gain complete protection against unwanted applications

Today's organizations struggle with ensuring that endpoints comply with corporate IT standards. End users can unintentionally introduce software that poses a risk to the business. What is needed is a way to standardize endpoints without impacting end-user productivity. McAfee Application Control augments traditional security solutions, enabling IT to allow only approved system and application software to run, and to easily block unauthorized or vulnerable applications that may compromise endpoints-without imposing operational overhead.

Extend the business viability of constrained systems

McAfee Application Control has already been deployed on thousands of devices, servers and desktops worldwide. It locks down these systems against malware threats, unwanted changes, without file system scanning or other periodic activity that could impact system performance. It is equally effective in standalone mode without network access, and has been designed to operate in a variety of network and firewall configurations.

Features

- Dynamic whitelisting through a trusted source.
- McAfee Application Control eliminates the need for IT administrators to manually maintain lists of approved applications. This enables IT departments to adopt a flexible approach where a repository of trusted applications can run on clients. This prevents execution of all unauthorized software binaries and dynamic link libraries (DLLs), and further defends against memory exploits Low overhead footprint.
- McAfee Application Control runs transparently on clients, and can be set up quickly, with very low initial and ongoing operational overhead Minimal impact on CPU cycles.
- McAfee Application Control uses less than 10 MB of RAM, with no file system scanning that could affect system performance.

Today's IT departments face tremendous pressure to ensure that their endpoint nodes comply with many different security policies, operating procedures, and regulations. Extending the viability of fixed function devices such as point-of-sale (POS) terminals, customer service terminals, and legacy NT platforms has become critical.

With McAfee Application Control, IT departments now have a way to eliminate unauthorized software on endpoint nodes, while providing employees greater flexibility to use the resources they need to get their jobs done. McAfee's dynamic whitelisting trust model eliminates the labor and cost associated with other whitelisting technologies, thereby reducing overhead and increasing continuity.

Application Control protects your organization against malware attacks before they occur by proactively controlling the applications executing on your desktops, laptops, and servers.

ePolicy Orchestrator and Solidcore integration

Solidcore integrates with ePolicy Orchestrator versions 4.0 and 4.5 as a separately installed extension. This table lists features and briefly describes how they are used by Solidcore.

ePO feature	Location	Used by Solidcore to
Client Tasks	Systems | System Tree | Client Tasks	The following tasks apply to all Solidcore products: • SC: Enable (Solidcore 5.1.0) - used too enable the Solidcore Agent on client computers • SC: Collect Debug Info (Solidcore 5.1.0) - used to debug configuration information • SC: Disable (Solidcore 5.1.0) - used to disable the Solidcore Agent • SC: Change Local CLI Access (Solidcore 5.1.0) - used to lockdown the McAfee Solidcore Agent CLI console • SC: Run Commands (Solidcore 5.1.0) - used to run any Solidcore specific commands on a client • SC: Begin Update Mode (Solidcore 5.1.0) - used to open an update window • SC: End Update Mode (Solidcore 5.1.0) - used to close an update window • SC: Initial Scan to create whitelist (Solidcore 5.1.0) - used run initial scan on the client system The following task applies only to Application Control • SC: Pull Inventory (Solidcore 5.1.0) - used to pull the list of all executables lying on client computers and their details whether they are authorized or unauthorized • SC: Get Diagnostics for programs (Solidcore 5.1.0) - used to extract a list of potential updaters that are available in the Application Control, Policy Catalog for applying to a client
Configuration	Configuration | Solidcore	• Create Rule Groups - applies to all Solidcore products The following apply only to Application Control • Publishers • Installers
Dashboards	Dashboards	• Create dashboards containing monitors to keep a constant watch on your environment

ePO feature	Location	Used by Solidcore to
		• Manage dashboards • Access information about your systems
Policy Assignment	Systems | System Tree | Policies	Assign policies to managed systems. You can view policy assignments, where they are applied, and if they are enforced.
Policy Catalog	Systems | Policy Catalog	• Create Change Control policies • Create Integrity Monitor policies • Create Application Control policies • Create General policies
Queries	Reporting | Queries	To create and maintain database queries regarding system security information. Queries are configurable objects that retrieve and display data from the database. The results of queries are displayed in charts and tables.
Reports	Reporting | Solidcore	• View Solidcore alerts • View Solidcore events • View Solidcore inventory lists • Reconciliation - optional Change Control feature • Network Control • DB Audit • Image Deviation
Repositories	Software | Master Repository	To check in and manage content required by Solidcore.
Server Tasks	Automation | Server Tasks	• Solidcore: Purge Task - used to purge Solidcore generated results The following apply only to Application Control • Solidcore: Scan a Software Repository - used to scan an organization's software repository to collect publishers and certificates • Solidcore: Update Inventory Search Indexes - used after inventory has been pulled to create search indexes • Solidcore: Run Image Deviation - used to compare the inventory of a system with the golden inventory which is fetched from a designated gold system
user Management	User Management | Users User Management | Permissions sets	• Assign Users • Assign permission sets

Getting product information

Unless otherwise noted, product documentation comes as Adobe Acrobat .PDF files, available on the product CD from the McAfee download site.

- *Installation Guide*: Provides instructions for installing and enabling the software.
- *Product Guide*: Provides an introduction to the product and its features; detailed instructions for configuring the software; information on deployment, recurring tasks, and operating procedures.

- *Change Control Evaluation Guide*: Provides an introduction to Change Control and detailed procedures for configuring Change Control use cases.
- *Integrity Monitor Evaluation Guide*: Provides an introduction to Integrity Monitoring and detailed procedures for configuring Integrity Monitor use cases.
- *Application Control Evaluation Guide*: Provides an introduction to Application Control and detailed procedures for configuring Application Control use cases.
- *When Should You Implement the Analytics Server?*: Provides a list of platforms that are not supported by the ePolicy Orchestrator.
- *Release Notes*: Provides a readme Product Information, resolved issues, any known issues, and last minute additions or changes to the product or its documentation. *A text file is included with the software application and on the product CD*.

Finding documentation for McAfee Solidcore extension products

To access the documentation for the McAfee Solidcore extension products, use the McAfee ServicePortal.

1. Go to the McAfee ServicePortal (http://mysupport.mcafee.com)and, under Self Service click **Product Documentation**.
2. Select the **Product**.
3. Select a **Version**.
4. Select a product document.

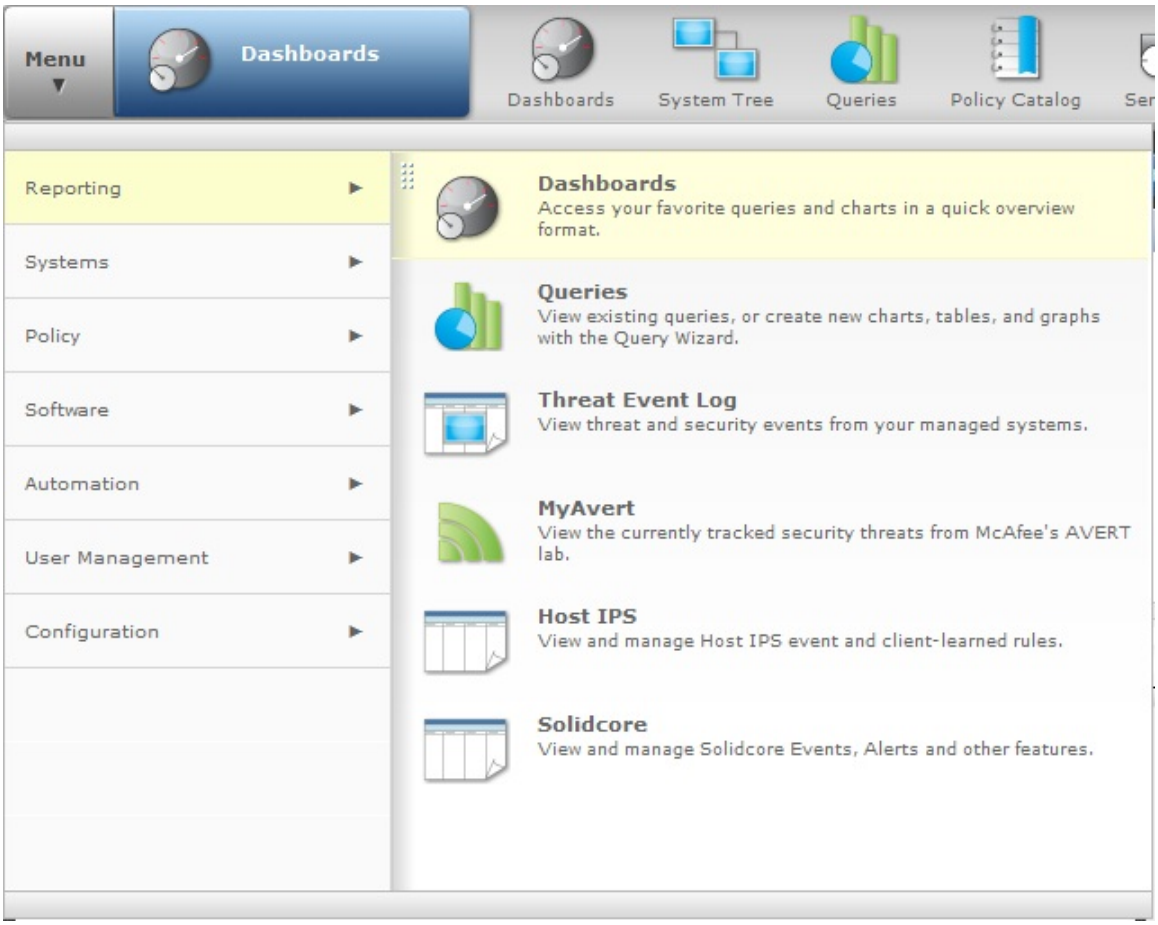
ePolicy Orchestrator menus and navigation

Prerequisite

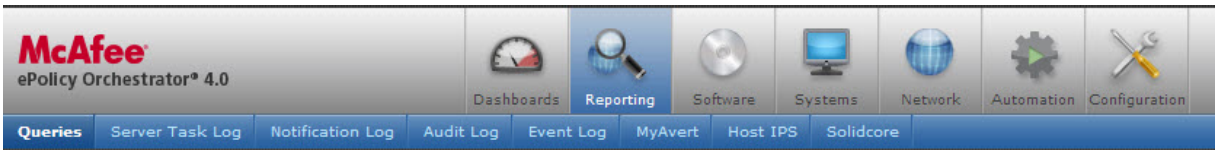
Before configuring Solidcore Products ensure that you have:

1. An EPO management server and database to be in place. For details on system requirements and instructions for setting up the ePolicy Orchestrator environment, see the *ePolicy Orchestrator 4.0 Installation Guide* or the *ePolicy Orchestrator 4.5 Installation Guide*.
2. Install the Solidcore extension; see the *McAfee Solidcore 5.1.0 Installation Guide*.
3. Install the Solidcore Agent; see the *McAfee Solidcore 5.1.0 Installation Guide*.
4. Product Licenses have been applied see the *McAfee Solidcore 5.1.0 Installation Guide*.

Version 4.5 of ePolicy Orchestrator software uses a menu to categorize the various features and functionality. When an item is the Menu is highlighted, its choices appear in the details pane of the console.



Version 4.0 of the ePolicy Orchestrator software primarily uses a navigation bar, which is comprised of a fixed group of section icons that organize functionality into categories.



NOTE: All procedures in this guide contain menu navigation for ePolicy Orchestrator versions 4.0 and 4.5.

Configuring ePolicy Orchestrator

The ePO server is the center of your managed environment, providing a single location from which to administer system security throughout your network.

When configuring the ePO server for the first time:

1. Decide how to implement the flexibility of permission sets.
2. Create user accounts and permission sets, and assign the permission sets to the user accounts as needed.

Contents

Assigning permission sets

Assign permission sets for your ePO users. Permission sets allow you to define what users are allowed to do with the software. You can assign permission sets to individuals or to groups.

User accounts provide a means for users to access and use the software. They are associated with permission sets, which define what users, are allowed to do with the software.

You must create user accounts and permission sets to accommodate the needs of each user that logs on to the ePO server. You can create accounts for individual users, or you can create a permission set that maps to users or groups.

There are two types of users, global administrators and users with limited permissions.

How permission sets work

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. One or more permission sets can be assigned to users who are not global administrators (global administrators have all permissions to all products and features).

Permission sets only grant rights and access — no permission ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks. Consider this as you plan your strategy for granting permissions to the users in your environment.

When a new product extension is installed, it can add one or more groups of permissions to the permission sets. For example, when you install a Solidcore extension, a Solidcore section is added to each permission set. Initially, the newly added section is listed in each permission set with no permissions yet granted.

Solidcore default permission sets

The Solidcore extension contains two default permission sets that provide permissions to ePolicy Orchestrator functionality. These are:

- **Solidcore Admin** — Provides view and change permissions across ePolicy Orchestrator features. Users that are assigned this permission set each need at least one more permission set that grants access to needed products and groups of the System Tree. After creating the Solidcore Admin permissions need to be edited and enabled per user requirements.
- **Solidcore Reviewer** — Provides view permissions across ePolicy Orchestrator features. Users that are assigned this permission set each need at least one more permission set that grants access to needed products and groups of the System Tree.

Working with permission sets

Use these procedures to create and maintain permission sets.

- Creating permission sets for user accounts
- Deleting permission sets

Creating permission sets for user accounts

use this procedure to create a permission set.

1. From the 4.0 ePO console, select **Configuration | Permission Sets**. From the 4.5 ePO console, select **Menu | User Management | Permission Sets**, and then click **New Permission Set**.
2. Type a name for the permission set and then select the users to which the set is assigned.
3. Select a server name from the drop-down list, or click **Add** if the server name you need does not appear in the server list.
4. Click **Save**. The Permission Sets page appears.
5. Select the new permission set from the Permission Sets list. Its details appear to the right.
6. Click **Edit** next to the Solidcore General section.
7. On the Edit Permission Set page that appears, select the appropriate options, then click **Save**.
8. Click **Edit** next to the Solidcore Policy Permissions section.
9. On the Edit Permission Set page that appears, select the appropriate options, then click **Save**.

Deleting permission sets

Use this procedure to delete a permission set.

1. From the 4.0 ePO console, select **Configuration | Permission Sets**. From the 4.5 ePO console, select **Menu | User Management | Permission Sets**, and then select the permission set you want to delete in the Permission Sets list. Its details appear to the right.

2 Click **Actions | Delete**, and then click **OK** in the Action pane. The permission set no longer appears in the Permission Sets list.

Configuring user accounts

User accounts provide a means for users to access and use the software. They are associated with permission sets, which define what users, are allowed to do with the software.

You must create user accounts and permission sets to accommodate the needs of each user that logs on to the ePO server. You can create accounts for individual users, or you can create permission sets that map to users or groups.

Creating user accounts

Use this procedure to create a user account. You must be a global administrator to add, edit, or delete user accounts.

1 From the 4.0 ePo console, select **Configuration | Users** . from the 4.5 ePO console, select **Menu | User Management | Users**, and then click **New Users**.

2 Type a user name.

3 Select whether to enable or disable the logon status of this account. If this account is for someone who is not yet a part of the organization, you might want to disable it.

4 Select whether the new account uses **ePO authentication** or **Windows authentication**, and provide the required credentials.

5 Optionally, provide the user's full name, email address, phone number, and a description in the **Notes** text box.

6 Select the appropriate permission sets for the user. (Valid selections are **Solidcore General** or **Solidcore Policy permissions**)

7 Click **Save** to save the current entries and return to the Users tab. The new user should appear in the Users list.

Deleting user accounts

Use this procedure to delete a user account

NOTE: McAfee recommends disabling the Login status of an account instead of deleting it, until you are sure all valuable information associated with the account has been moved to other users.

1 From the 4.0 ePo console, select **Configuration | Users** Sets. from the 4.5 ePO console, select **Menu | User Management | Users**.

2 From the Users list, select the user you want to delete, and then select **Actions | Delete**.

3 Click **OK**.

Configuring server settings for Solidcore

You must provide valid license keys to activate corresponding Solidcore features. Edit ePolicy Orchestrator Server Settings to add license keys for the required Solidcore features. This

procedure can also be used to enter a valid McAfee Analytic Server URL and Network Control URL.

1 From the 4.0 ePolicy Orchestrator console, select **Configuration | Server Settings**. From the 4.5 ePO console, select **Menu | Configuration | Server Settings**, then from the **Settings Categories** select **Solidcore**.

2 Click **Edit**. The Edit Server Settings page appears.

3 Type valid license keys for corresponding Solidcore features.

4 Type valid **Analytics Server URL**. This is optional and required only if you want to access the Analytics Server from ePolicy Orchestrator. Refer to *When Should You Implement the Analytics Server Guide* for more information.

5 Type the URL of the **Integrity Monitor for Network Devices Application**. Refer to the documentation on Integrity Monitor for Network Devices for details.

6 Click **Save**.

Managing rule groups

McAfee includes a set of default group filter rules for Integrity Monitor and Application Control. The default filter rules can not be edited; however users can:

- Create a duplicate of a predefined rule group
- Edit the duplicate rule group
- Apply a rule group filter rule
- Search for rule groups by their **Group Name**
- Import or export rule groups

Creating a Change Control Rule Group

Use this task to create a new Change Control Rule Group.

Task

For option definitions, click **?** in the interface.

1 From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Rule Groups**, then select the Filter Type as **Change Control**. All the default and user created rule groups for the selected category are displayed.

2 Add a new rule group or edit an existing rule group as required.

3 To read protect a file select **Read Protect** and then click **Add**.

- In the Add File dialog box enter the file path.
- To enforce read-protect select **Include**.
- Click **OK**.

  NOTE: For optimal system performance the read protect feature is disabled by default on the client. To enable this feature use the **SC: Run Commands (Solidcore 5.1.0)** client task.

You can read-protect critical files, directories to protect them from unauthorized access. When a directory is specified for read protection, all files in that directory are scanned and

added to the read protection list. Any unauthorized attempt made to read data from these files is stopped and an event is generated.

4 To write protect a file select **Write Protect File** and then click **Add**.

- In the Add File dialog box enter either a **file** or a **directory**. The longest pathname takes precedence, e.g. If C:\temp is excluded, and C:\temp\foo.cfg is included, the changes to foo.cfg will be tracked.
- To enforce write protection select **Include**.
- Click **OK**.

You can enforce write protection rules on a file or directory in order to protect them from unauthorized modifications. You should only protect files that are not routinely being updated by programs e.g. log files, etc. The write protection rules applied on the specified files render them as read only thereby protecting your data. When a directory is specified for write protection, all files in that directory are scanned and added to the write protection list.

5 To write protect a registry select **Write Protect Registry** and then click **Add**.

- Enter a **registry key** — the longest key takes precedence, e.g. If HKEY_LOCAL_MACHINE is excluded, and HKEY_LOCAL_MACHINE\\System is included, the changes to HKEY_LOCAL_MACHINE\\System will be tracked.
- To enforce write-protection select **Include**.
- Click **OK**.

Critical registry keys can be protected against change using the deny-write feature. All enforcement rules to control modifications to registry keys can be applied using this feature.

6 To add an updater select **Updaters** and then click **Add**. Configure these options as required then click **OK**.

- Binary - type the location of an executable binary.
- Updater Label - type an identification label (For example, if you type **Adobe Updater changes**, then changes done by Adobe_Updater.exe will be tagged with this label.)
- Condition - select one of these options as required:
  - None - to allow the binary to run as updater without any conditions.
  - Parent - to allow the binary to run as updater only if it is launched by the specified parent process.
  - Library - to allow the binary to run as updater only when it has loaded the specified library.
- Disable Inheritance - disables inheritance of the updater. For example if process A is an updater and launches process B, process B will not become an updater.
- Suppress Events - select this option to suppress events created actions performed by the updater.

7 On the **Trusted User** tab, perform these actions as required.

- To add a trusted user to a policy (Windows only), click **Add**. On the Add User dialog box, configure these options as required then click **OK**.
  - Domain\User - type the domain name and the logon name of the user.
  - User Label - type an identification label (for example, if you type **John Doe changes**, then changes done by John Doe will be tagged with this label).
  - Name - type the name of the user.

- To import users from a registered Active Directory, click **AD Import**. On the Import from Active Directory dialog box, configure the search options as required, then select the required user or group from the search result.
  - Active Directory Server — Select the required registered Active Directory.
  - Global Catalog Search — Select this to search for users in Global Catalog.
  - Search for — Select whether to search for users or groups.
    - For searching Users:
      - Search By — Select whether to search for Users by UPN (User Principal Name) or SAM account name

        NOTE:

        - In case, search is done by UPN/Common name, the user will be trusted with the UPN.
        - In case, search is done by SAM Account Name, the user will be trusted with the SAM Account Name.

      - User Name - Type the user name search string.
      - Group Name - In case, search for Users is to be restricted to a group, type the complete group name here.

        NOTE:

        - The search criteria is **Contains** for the specified user name or group name search string.

    - For searching Groups:
      - Group Name — Type the group name search string.

        NOTE: The search criteria is Contains for the specified user name or group name search string.

  - Find — Click to search the specified user or group name.

8 Click **Save Rule Group**.

Creating a Integrity Monitor Rule Group

Use this task to create a new Integrity Monitor Rule Group.

Task

For option definitions, click **?** in the interface.

1 From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Rule Groups**, then select the **Filter Type** as **Integrity Monitor**. All the default and user created rule groups for the selected category are displayed.

2 Add a new rule group or edit an existing rule group as required.

3 To add files or directories to be included or excluded from being monitored for, on the **File** tab click **Add**. In the Add File dialog box, type the file or directory to include or exclude then click **OK**.

The longest pathname takes precedence, e.g. if C:\temp is excluded, and C:\temp\foo.cfg is included, the changes to foo.cfg will be tracked.

4 To add registry keys to be included or excluded from being monitored for changes, on the **Registry** tab click **Add**. In the Registry Filters dialog box, type the registry filters to be excluded or included, then click **OK**.

   The longest pathname takes precedence, for example if HKEY_LOCAL_MACHINE is excluded, and HKEY_LOCAL_MACHINE\System is included, the changes to HKEY_LOCAL_MACHINE\System will be tracked.

5 To add file extension(s) to be included or excluded from being monitored for changes, on the **Extension** tab click **Add**. Type the file extension without the dot, for example log. Select whether to **Include** or **Exclude** the extension, then click **OK**.

6 To add processes or programs to be included or excluded from being monitored for changes, on the **Program** tab click **Add**. In the Add Program dialog box, type the program to be excluded or included then click **OK**.

   Enter the full path of the program or just the name, for example notepad.exe. It is recommended to exclude background processes such as lsass.exe.

7 To exclude users from monitoring, on the **User** tab click **Add**. Configure these options as required then click **OK**.

   - User — type the name of the user to exclude from being monitored.
   - Exclude — excludes specific users from being monitored.

8 To create an advanced filter (if changes are to be excluded using a combination of conditions), on the **Advanced** tab click **Add Rule**, then edit the settings as required.

   NOTE: When configuring Advanced exclude filters use the full path when performing an **equals** match or use {name}.exe with an **ends with** match.

9 Click **Save Rule Group**.

Creating a Application Control Rule Group

Use this task to create a new Application Control Rule Group.

Task

For option definitions, click **?** in the interface.

1 From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Rule Groups**, then select the **Filter Type** as **Application Control**. All the default and user created rule groups for the selected category are displayed.

2 Add a new rule group or edit an existing rule group as required.

3 On the **Updaters** tab, click **Add** to add an updater. Configure these options as required then click **OK**.

   - Binary - type the location of an executable binary.
   - Updater Label - type an identification label (For example, if you type **Adobe Updater changes**, then changes done by Adobe_Updater.exe will be tagged with this label.)
   - Condition - select one of these options as required:
     - None - to allow the binary to run as updater without any conditions.
     - Parent - to allow the binary to run as updater only if it is launched by the specified parent.
     - Library - to allow the binary to run as updater only when it has loaded the library.

- Disable Inheritance - disables inheritance of the updater. For example if process A is an updater and launches process B, process B will not become an updater.
- Suppress Events - select this option to suppress events created actions performed by the updater.

4 On the **Binary** tab, perform these actions as required.

- To add a binary, click **Add**. The Add Binary dialog box appears. Configure these options as required, then click **OK**.
  - Rule name - type the name of a program.
  - Allow/Ban - if program is trusted select **Allow** otherwise select **Ban**.
  - Rule Type - Select one of these options.
    - File — to allow/ban by binary file name.
    - Checksum — to allow/ban by the checksum of the binary.
  - Name/SHA1: This field will be either Name or SHA1 depending on the **Rule Type**.
- To add binary from inventory, click **Add from Inventory**. On the Add from Inventory dialog box, configure these options as required then select the required binary file from the search result.
  - Rule name — type the name of a program.
  - Allow/Ban — If program is trusted select **Allow** otherwise select **Ban**.
  - Rule Type — Select one of these options.
    - File — to allow/ban by binary file name.
    - Checksum — to allow/ban by the checksum of the binary.
  - File Name — Search for binaries already present on client system(s) in your network to fill this field. This search looks for matching file names in the Inventory data pulled into ePolicy Orchestrator from client systems.

5 On the **Trusted User** tab, perform these actions as required.

- To add a trusted user to a policy (Windows only), click **Add**. On the Add User dialog box, configure these options as required then click **OK**.
  - Domain\User — type the domain name and the logon name of the user.
  - User Label - type an identification label (for example if you enter **John Doe changes**, then changes done by John Doe will be tagged with this label).
  - Name - Type the name of the user.
- To import users from a registered Active Directory, click **AD Import**. On the Import from Active Directory dialog box, configure the search options as required, then select the required user or group from the search result.
  - Active Directory Server — Select the required registered Active Directory.
  - Global Catalog Search — Select this to search for users in Global Catalog.
  - Search for — Select whether to search for users or groups.
    - For searching Users:
      - Search By — Select whether to search for Users by UPN (User Principal Name) or SAM account name

        NOTE:

- In case, search is done by UPN/Common name, the user will be trusted with the UPN.
- In case, search is done by SAM Account Name, the user will be trusted with the SAM Account Name.

- User Name - Type the user name search string.
- Group Name - In case, search for Users is to be restricted to a group, type the complete group name here.

  NOTE:

  - The search criteria is **Contains** for the specified user name or group name search string.

- For searching Groups:
  - Group Name — Type the group name search string.

    NOTE: The search criteria is Contains for the specified user name or group name search string.

- Find — Click to search the specified user or group name.

6 To add a publisher to the policy (Windows only), select **Publishers** then click **Add**. Search for the required publishers based on their category, then add the publisher. Executable signed by trusted publisher will be allowed to run (example, Internet Explorer).

Select **Add Publisher(s) as Updater** and type the **Updater Label** if you want to allow the applications signed by the selected publishers to make changes to the executables or launch any new application on the client system. Changes done by the executables signed by selected publisher will be tagged with this Updater label.

7 To add an installer (Windows only) allowed to run on your system, select **Installers** then click **Add**. Search for the required installer based on the installer name or vendor name, then type the **Installer Label** and click **OK**.

NOTE: Changes done by the installer will be tagged with Installer Label.

8 To add a trusted directory such as a shared network drive select **Trusted Directories** and click **Add**. Configure these options as required then click **OK**.

- Path - enter the location of your trusted directory.
- Include/Exclude - select Include.
- Select **Make programs executed from this directory updaters** if you want to allow the applications launched from the specified directory to make changes to the executables or launch a new application on the client system.

9 Click **Save Rule Group**.

Viewing predefined rule group

Use procedure to view predefined rule groups.

1 From the 4.0 ePO console, select **Configuration | Solidcore | Rule Group**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Rule Groups**.

2 From the **Type** menu options select from **Change Control**, **Integrity Monitor** or **Application Control**.

3 Select the platform. The predefined list of rule groups will be displayed.

NOTE: You can also search for a rule group based on their **Group Name**.

Adding a new rule group

Use this procedure to add a new rule group.

1 From the 4.0 ePO console, select **Configuration | Solidcore | Rule Groups**. From the 4.5 ePO console, select **Menu | Configuration | Solidcore |Rule Groups**.

2 Click **Add Rule Group**. The Add Rule Group dialog box appears.

3 Enter a name for the new group rule and click **OK**.

4 Locate the group you just created and select **Edit**. Edit the saved group and assign or edit existing rule.

5 Click **Save Group**. This group can now be added to policy which can applied to a client system.

Applying a rule group

Use this procedure to add a new rule group.

1 From the 4.0 ePO console, select **Systems | Policy Catalog**. From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select the desired policy from Change Control, Integrity Monitor, or Application Control.

2 Click **Add Group**. The Select Group dialog box appears.

3 Select the group you previously created and click **OK**.

Importing or exporting rule groups

Use procedure to import or export rule groups.

1 From the 4.0 ePO console, select **Configuration | Solidcore | Rule Group**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Rule Groups**.

2 Do one of these:

- Click **Import**, then browse to select the rule groups file and click **OK**.
- Select the rule groups to export, then click **Export**. Save the xml file in the desired location.

Viewing policy assignment for a rule group

Use this task to view policy assignment for a rule group.

Task

For option definitions, click **?** in the interface.

1 From the 4.0 ePO console, select **Configuration | Solidcore | Rule Group**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Rule Groups**.

2 Click **Assignments** next to the desired rule group to view the policies to which it is assigned.

Managing Publishers

There are three ways to import certificates:

- Upload button - This allows you to upload or import a valid certificate. From the 4.0 ePO console, select **Configuration | Solidcore | Publishers**. From the 4.5 ePO console, select **Menu |Configuration | Solidcore | Publishers**.
- Extract certificate from a binary - This allows you to extract the certificate from the binary file. Specify the path of the binary file accessible from the ePO server. From the 4.0 ePO console, select **Configuration | Solidcore | Publishers**. From the 4.5 ePO console, select **Menu |Configuration | Solidcore | Publishers**.
- Use the scan software repository server task to scan repositories and collect publisher certificates. From the 4.0 ePO console, select **Automation | Server Tasks**. From the 4.5 ePO console, select **Menu |Configuration | Server Tasks**.

Uploading a certificate

Use procedure to upload a valid certificate.

1. From the 4.0 ePo console, select **Configuration | Solidcore | Publishers**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Publishers**.
2. Click **Upload**. The Upload Certificate dialog box appears.
3. Browse to and select a valid file to import. Click **OK**.

Assigning a certificate to a policy

Use this procedure to apply a certificate or publisher to a policy. Refer to *Creating an Application Control policy* for more details.

Assigning a certificate to a rule group

Use this task to apply a certificate or publisher to a rule group.

Task

For option definitions, click **?** in the interface.

1. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Publishers**.
2. Select the publishers to apply to a rule group, then click **Actions | Add to Rule Group**. The Add to Rule Group dialog box appears.
3. Select the required user-defined rule group, then click **OK**.

Alternatively, you can apply a certificate or publisher to a rule group using **Menu | Configuration| Solidcore | Rule Group** tab. Refer to *Creating a Application Control Rule Group* section for more details.

Extracting a certificate

Use this procedure to extract a certificate from a binary file.

1. From the 4.0 ePO console, select **Configuration | Solidcore | Publishers**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Publishers**.

2 Click **Actions | Extract Certificates**. The Extract certificate from binary page appears.

3 Type the path of the binary file accessible from the ePO server.

4 Type the **Domain**, **User Name**, and **Password** to access the specified network location, then click **OK**.

Searching for a publisher

Use this task to search for a publisher based on their information.

Task

For option definitions, click **?** in the interface.

1 From the 4.0 ePO console, select **Configuration | Solidcore | Publishers**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Publishers**.

2 Select one of these categories based on which you want to search for publishers.

- Issued to — Name of the organization which publishes the certificate
- Issued by — Name of the signing authority
- Extracted From — Path of the binary file from which the certificate was extracted
- Friendly Name — Friendly name of the certificate

3 Type the publisher information to search for, then click **Search**.

Viewing assignments for a publisher

Publishers can be assigned to Policy and Rule Group. Use this task to view assignments for a publisher.

Task

For option definitions, click **?** in the interface.

1 From the 4.0 ePO console, select **Configuration | Solidcore | Publishers**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Publishers**.

2 Select the required publisher, then click **Actions | Check Assignments**. The Publisher Assignments dialog box appears with the Rule Group and the Policy names to which the publisher is assigned.

Managing Installers

The Installer settings allow you to define installers that are allowed to install software on your system. You can declare any installers (executables, installers, or batch files) as a whitelist application.

Adding installers

Use this procedure to add an installer to your application whitelist.

1 From the 4.0 ePolicy Orchestrator console, select **Configuration | Solidcore | Installers** then click **Add**. From the 4.5 ePolicy Orchestrator console, select **Menu | Configuration| Solidcore | Installers** then click **Actions | Add Installer**.
2 In the Add Installer page, provide these installer details:
   - **Installer Name** — Type the name of the installer.
   - **Binary Path** — Type the path of the installer file.
   - **Version** — Type the version of the installer. This field is optional.
   - **Vendor** — Type the name of the vendor who publishes the installer.
   - **Checksum (SHA1)** — Type the checksum (SHA1) of the installer file.
3 Click **Add**.

Assigning an installer to a policy

Use this task to assign an installer to a policy. Refer to *Creating an Application Control policy* for more details.

Assigning an installer to a rule group

Use this task to apply a installer to a rule group.

Task

For option definitions, click **?** in the interface.

1 From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Installer**.
2 Select the installers to apply to a rule group, then click **Actions | Add to Rule Group**. The Add to Rule Group dialog box appears.
3 Select the required user-defined rule group, then click **OK**.

Alternatively, you can apply an installer to a rule group using **Menu | Configuration| Solidcore | Rule Group** tab. Refer to *Creating a Application Control Rule Group* section for more details.

Searching for an installer

Use this task to search for an installer based on the name or vendor.

Task

For option definitions, click **?** in the interface.

1 From the 4.0 ePO console, select **Configuration | Solidcore | Installers**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Installers**.
2 Select one of these categories based on which you want to search for installers.
   - Installer Name — Name of the installer.
   - Vendor — Name of the vendor who has published the installer.
3 Type the installer name or vendor name to search for, then click **Search**.

Viewing assignments for an installer

Installers can be assigned to Policy and Rule Group. Use this task to view assignments for an installer.

Task

For option definitions, click **?** in the interface.

1. From the 4.0 ePO console, select **Configuration | Solidcore | Installers**. From the 4.5 ePO console, select **Menu | Configuration| Solidcore | Installers**.
2. Select the required installer, then click **Actions | Check Assignments**. The Installer Assignments dialog box appears with the Rule Group and the Policy names to which the installer is assigned.

Working with the agent from the ePO server

The ePO console includes pages where agent tasks and policies can be configured, and where agent properties can be viewed.

Use the following procedures when working with the agent from the ePO server.

- Viewing agent and product properties
- Viewing system information
- Accessing settings to retrieve properties
- Windows system and product properties reported by the agent
- Sending manual wake-up calls to the system
- Sending manual wake-up calls to a group
- Making the system tray icon visible
- Locating inactive agents.

For more information on these procedures refer to the *McAfee ePolicy Orchestrator 4.0 Product Guide* or the *McAfee ePolicy Orchestrator 4.5 Product Guide*.

Configuring Policies

The ePolicy Orchestrator console allows you to configure policy settings for Solidcore features from a central location. A policy is a collection of settings that you create, configure, and enforce. Policies ensure that Solidcore features are configured correctly.

The following policies can be created:

- Change Control polices
- Integrity Monitor policies
- Application Control policies
- General policies

NOTE: Policies can only be viewed, created or edited if the appropriate license is installed.

Windows path definitions in Solidcore policies

Solidcore policies permit the use of system environment variables to define monitoring policies. The following table provides details on the available variables.

Variable	Windows default values
%ALLUSERSPROFILE%	C:|Documents and Settings\All Users
%APPDATA%	C:|Documents and Settings\{username}\Application
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES (x86)%	C:\Program Files (x86)\Common Files
%HOMEDRIVE%	C;
%HOMEPATH%	C:|Documents and Settings\{username}(\on earlier Windows)
%PROGRAMFILES%	C:\Program Files
%PROGRAMFILES (x*86)%	C:\Program Files (x86) (only in 64-bit version)
%SYSTEMDRIVE%	C;
%SYSTEMROOT%	C:\windows (C:\WINNT on earlier Windows versions)
%TEMP% (system) %tmp% (user)	C:|Documents and Settings\{username}\local Settings\Temp C:\Temp
%USERPROFILE%	C:|Documents and Settings\{username} (C:WINNT\profiles|{username} for earlier versions)
%WINDIR%	C:\Windows

Contents

Viewing policies

Use this procedure to view the groups and systems where a policy is assigned. This list shows the assignment point's only, not each group or system that inherits the policy.

1. From the 4.0 ePO console, select **Systems | Policy Catalog**. From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select from:
   - Solidcore 5.1.0. Application Control
   - Solidcore 5.1.0 Change Control
   - Solidcore 5.1.0 Integrity Monitor
   - Solidcore 5.1.0 General
2. Select **Category**. All created policies for the selected category appear in the pane.
3. Under Assignments on the row of the desired policy, click the link that indicates the number of groups or systems the policy is assigned to (for example 2 assignments). On the Assignments page, each group or system where the policy is assigned appears with its **Node Name** and **Node Type**.

Viewing policy settings

Use this procedure to view the specific settings of a policy.

1. From the 4.0 ePO console, select **Systems | Policy Catalog**. From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, then select from:
   - Solidcore 5.1.0. Application Control
   - Solidcore 5.1.0 Change Control
   - Solidcore 5.1.0 Integrity Monitor
   - Solidcore 5.1.0 General
2. Select **Category**. All created policies for the selected category appear in the pane.
3. Click **View** or **Edit** next to the desired policy. The policy page and their settings appear.

Working with the Policy Catalog

Use these procedures to create and maintain policies from the Policy Catalog page.

Creating a Change Control policy

Change Control allows you to monitor change actions, use this procedure to create a new Change Control policy from the Policy Catalog. These are multi-slot policies; a user can assign multiple policies to a single node on the system tree.

1. From the 4.0 ePO console, select **Systems | Policy Catalog**. From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select **Solidcore 5.1.0 Change Control**.

2 Under Category select from **Change Control Rules (Windows)** or **Change Control Rules (Unix)**. All created policies for the selected category appear in the pane.

3 Click **New Policy**. The Create New Policy dialog box appears.

4 Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down.

5 Type a name for the new policy and click **OK**. The Policy Settings page opens.

6 You can read-protect critical files, directories to protect them from unauthorized access. When a directory is specified for read protect, all files in that directory are scanned and added to the read protection list. Any unauthorized attempt made to read data from these files is stopped and an event is generated. To read protect a file select **Read Protect** and then click **Add**.

- In the Add File dialog box enter the file path.
- To enforce read-protect select **Include**.
- Click **OK**.

NOTE: For optimal system performance the read protect feature is disabled by default on the client. To enable this feature use the **SC: Run Commands (Solidcore 5.1.0)** client task.

7 You can enforce write protection rules on a file or directory in order to protect them from unauthorized modifications. You should only protect files that are not routinely being updated by programs for example log files. The write protection rules applied on the specified files render them as read only thereby protecting your data. When a directory is specified for write protect, all files in that directory are scanned and added to the write protection list. To write protect a file select **Write Protect File** and then click **Add**.

- In the Add File dialog box enter either a file or a directory. The longest pathname takes precedence. For example, if C:\temp is excluded, and C:\temp\foo.cfg is included, the changes to foo.cfg will be tracked.
- To enforce write protection select **Include**.
- Click **OK**.

8 Critical registry keys can be protected against change using the deny write feature. All enforcement rules to control modifications to registry keys can be applied using this feature. To write protect a registry select **Write Protect Registry**, then click **Add**.

- Enter a **Registry key**. The longest key takes precedence. For example, if HKEY_LOCAL_MACHINE is excluded, and HKEY_LOCAL_MACHINE\\System is included, the changes to HKEY_LOCAL_MACHINE\\System will be tracked.
- To enforce write-protection select **Include**.
- Click **OK**.

9 To add an updater select **Updaters** and then click **Add**. Configure these options as required then click **OK**.

- Binary - type the location of an executable binary.
- Updater Label - type an identification label (For example, if you type **Adobe Updater changes**, then changes done by Adobe_Updater.exe will be tagged with this label.)
- Condition - select one of these options as required:
  - None - to allow the binary to run as updater without any conditions.

- Parent - to allow the binary to run as updater only if it is launched by the specified parent.
- Library - to allow the binary to run as updater only when it has loaded the library.

- Disable Inheritance - disables inheritance of the updater. For example if Process A is an updater and launches process B, process B will not become an updater.
- Suppress Events - select this option to suppress events created actions performed by the updater.

10 On the **Trusted User** tab, perform these actions as required.

- To add a trusted user to a policy (Windows only), click **Add**. On the Add User dialog box, configure these options as required then click **OK**.
  - Domain\User - type the domain name and the logon name of the user.
  - User Label - type an identification label (for example, if you type **John Doe changes**, then changes done by John Doe will be tagged with this label).
  - Name - type the name of the user.
- To import users from a registered Active Directory, click **AD Import**. On the Import from Active Directory dialog box, configure the search options as required, then select the required user from the search result.
  - Active Directory Server — Select the required registered Active Directory.
  - Global Catalog Search — Select this to search for users in Global Catalog.
  - Search for — Use this to search for users.
  - Search By — Select whether to search for Users by UPN (User Principal Name) or SAM account name

    NOTE:
    - In case, search is done by UPN/Common name, the user will be trusted with the UPN.
    - In case, search is done by SAM Account Name, the user will be trusted with the SAM Account Name.
  - User Name - Type the user name search string.
  - Group Name - In case, search for Users is to be restricted to a group, type the complete group name here.

    NOTE:
    - To add Groups, add them to a rule group and then, include the rule group into the policy.
    - The search criteria is **Contains** for the specified user name search string.
  - Find — Click to search the specified user name.

11 Click **Save**.

Creating an Integrity Monitor policy

File Integrity monitoring allows you to designate a set of files to monitor for changes. When a file is changed, an event is generated and sent to the ePO server. These are multi-slot policies; a user can assign multiple policies to a single node on the system tree.

Use this procedure to create a new Integrity Monitor policy from the Policy Catalog.

1. From the 4.0 ePO console, select **Systems | Policy Catalog**. From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select **Solidcore 5.1.0 Integrity Monitor**.
2. Under Category select from **Integrity Monitor Rules (Windows)**. All created policies for the selected category appear in the pane.
3. Click **New Policy**. The Create New Policy dialog box appears.
4. Select the policy you want to duplicate from **Create a policy based on this existing policy** drop-down menu.
5. Type a name for the new policy and click **OK**. The Policy Settings page opens.
6. To add files or directories to be included or excluded from being monitored for, on the **File** tab click **Add**. In the Add File dialog box, type the file or directory to include or exclude then click **OK**.

   The longest pathname takes precedence, e.g. if C:\temp is excluded, and C:\temp\foo.cfg is included, the changes to foo.cfg will be tracked.
7. To add registry keys to be included or excluded from being monitored for changes, on the **Registry** tab click **Add**. In the Registry Filters dialog box, type the registry filters to be excluded or included, then click **OK**.

   The longest pathname takes precedence, for example if HKEY_LOCAL_MACHINE is excluded, and HKEY_LOCAL_MACHINE\System is included, the changes to HKEY_LOCAL_MACHINE\System will be tracked.
8. To add file extension(s) to be included or excluded from being monitored for changes, on the **Extension** tab click **Add**. Type the file extension without the dot, for example log. Select whether to **Include** or **Exclude** the extension, then click **OK**.
9. To add processes or programs to be included or excluded from being monitored for changes, on the **Program** tab click **Add**. In the Add Program dialog box, type the program to be excluded or included then click **OK**.

   Enter the full path of the program or just the name, for example notepad.exe. It is recommended to exclude background processes such as lsass.exe.
10. To exclude users from monitoring, on the **User** tab click **Add**. Configure these options as required then click **OK**.
    - User — type the name of the user to exclude from being monitored.
    - Exclude — excludes specific users from being monitored.
11. To create an advanced filter (if changes are to be excluded using a combination of conditions), on the **Advanced** tab click **Add Rule**, then edit the settings as required.

    NOTE: When configuring Advanced exclude filters use the full path when performing an **equals** match or use {name}.exe with an **ends with** match.
12. Click **Save**.

Creating an Application Control policy

Application Control allows you to define applications that are allowed to run on your system. These are multi-slot policies; a user can assign multiple policies to a single client system on the system tree.

Applications that update the system (program code, exe, and dll) are referred as Updaters. When a program is configured as an updater it is able to install new software and update existing program code. It is not authorized automatically but has to be present in the inventory during the initial scan or through allowed updater in the Application Control policy.

When an installer is configured as an authorized installer it gets both the authorized and updater attributes. For example, irrespective of whether this installer was originally present on the system or not, it will be allowed to execute and install/update software on that system. Authorized installers are allowed on the basis of the checksum (SHA1) of the original installer. This ensures that irrespective of the source of the installer if the checksum remains the same it will be authorized and work as updater.

Use this procedure to create a new Application Control policy from the Policy Catalog.

1. From the 4.0 ePO console, select **Systems | Policy Catalog**. From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select **Solidcore 5.1.0 Application Control**.
2. Under Category select from **Application Control Rules (Windows)** or **Application Control Rules (Unix)**. All created policies for the selected category appear in the pane.
3. Click **New Policy**. The Create New Policy dialog box appears.
4. Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down menu.
5. Type a name for the new policy and click **OK**. The Policy Settings page opens.
6. On the **Updaters** tab, click **Add** to add an updater. Configure these options as required, then click **OK**.
   - Binary - type the location of an executable binary.
   - Updater Label - type an identification label (For example, if you type **Adobe Updater changes**, then changes done by Adobe_Updater.exe will be tagged with this label.)
   - Condition - select one of these options as required:
     - None - to allow the binary to run as updater without any conditions.
     - Parent - to allow the binary to run as updater only if it is launched by the specified parent.
     - Library - to allow the binary to run as updater only when it has loaded the library.
   - Disable Inheritance - disables inheritance of the updater. For example if process A is an updater and launches process B, process B will not become an updater.
   - Suppress Events - select this option to suppress events created actions performed by the updater.
7. On the **Binary** tab, perform these actions as required.
   - To add a binary, click **Add**. The Add Binary dialog box appears. Configure these options as required, then click **OK**.
     - Rule name - type the name of a program.
     - Allow/Ban - if program is trusted select **Allow** otherwise select **Ban**.
     - Rule Type - Select one of these options.
       - File — to allow/ban by binary file name.
       - Checksum — to allow/ban by the checksum of the binary.
     - Name/SHA1: This field will be either Name or SHA1 depending on the **Rule Type**.

- To add binary from inventory, click **Add from Inventory**. On the Add from Inventory dialog box, configure these options as required then select the required binary file from the search result.
  - Rule name — type the name of a program.
  - Allow/Ban — If program is trusted select **Allow** otherwise select **Ban**.
  - Rule Type — Select one of these options.
    - File — to allow/ban by binary file name.
    - Checksum — to allow/ban by the checksum of the binary.
  - File Name — Search for binaries already present on client system(s) in your network to fill this field. This search looks for matching file names in the Inventory data pulled into ePolicy Orchestrator from client systems.

8 On the **Trusted User** tab, perform these actions as required.

- To add a trusted user to a policy (Windows only), click **Add**. On the Add User dialog box, configure these options as required then click **OK**.
  - Domain\User — type the domain name and the logon name of the user.
  - User Label - type an identification label (for example if you enter **John Doe changes**, then changes done by John Doe will be tagged with this label).
  - Name - Type the name of the user.
- To import users from a registered Active Directory, click **AD Import**. On the Import from Active Directory dialog box, configure the search options as required, then select the required user or group from the search result.
  - Active Directory Server — Select the required registered Active Directory.
  - Global Catalog Search — Select this to search for users in Global Catalog.
  - Search for — Use this to search for users.
  - Search By — Select whether to search for Users by UPN (User Principal Name) or SAM account name

    NOTE:
    - In case, search is done by UPN/Common name, the user will be trusted with the UPN.
    - In case, search is done by SAM Account Name, the user will be trusted with the SAM Account Name.
  - User Name - Type the user name search string.
  - Group Name - In case, search for Users is to be restricted to a group, type the complete group name here.

    NOTE:
    - To add Groups, add them to a rule group and then, include the rule group into the policy.
    - The search criteria is **Contains** for the specified user name search string.
  - Find — Click to search the specified user name.

9 To add a publisher to the policy (Windows only), select **Publishers** then click **Add**. Search for the required publishers based on their category, then add the publisher. The executables signed by a trusted publisher will be allowed to run (example, Internet Explorer).

Select **Add Publisher(s) as Updater** and type the **Updater Label** if you want to allow the applications signed by the selected publishers to make changes to the executables or launch any new application on the client system. Changes done by the executables signed by selected publisher will be tagged with this Updater label.

10 To add an installer (Windows only) allowed to run on your system, select **Installers** then click **Add**. Search for the required installer based on the installer name or vendor name, then type the **Installer Label** and click **OK**.

NOTE: Changes done by the installer will be tagged with Installer Label.

11 To add a trusted directory such as a shared network drive, select **Trusted Directories** and click **Add**. Configure these options as required, then click **OK**.

- Path - enter the location of your trusted directory.
- Include/Exclude - select Include.
- Select **Make programs executed from this directory updaters** if you want to allow the applications saved in the specified directory to make changes to the executables or launch a new application on the client system.

12 Click **Save**.

Creating a General policy with exception rules

Use this procedure to create a general policy with exception rules from the Policy Catalog.

1 From the 4.0 ePO console, select **Systems | Policy Catalog**. From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select **Solidcore 5.1.0 General**.

2 Under Category select from **Exception Rules (Windows), or Exception Rules (UNIX)**. All created policies for the selected category appear in the pane.

3 Click **New Policy**. The Create New Policy dialog box appears.

4 Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down menu.

5 Type a name for the new policy and click **OK**. The Policy Settings page opens.

6 Click Add. The Add attribute dialog box appears. Edit the settings as needed. Click **OK**.

7 Click **Save**.

Creating a General policy with lockdown rules

NOTE: Users are encouraged to change the default local CLI recovery password using the General Lockdown Rules policy.

Use this password to unlock CLI and troubleshoot client systems.

Use this procedure to create a general policy with lockdown rules from the Policy Catalog.

1 From the 4.0 ePO console, select **Systems | Policy Catalog**. From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select **Solidcore 5.1.0 General**.

2 Under Category select from **Lockdown Rules**. All created policies for the selected category appear in the pane.

3 Click **New Policy**. The Create New Policy dialog box appears.

4 Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down menu.

5 Type a local **CLI Access Password**.

6 Confirm the password.

7 Click **Save**.

Editing a policy's settings from the Policy Catalog

Use this procedure to modify the settings of a policy. Your user account must have the appropriate permissions to edit policy settings for the desired product.

1 From the 4.0 ePO console, select **Systems | Policy Catalog** . From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select one of the **Solidcore 5.1.0 products** and **Category** from the drop-down menu. All created policies for the selected category appear in the pane.

2 Locate the desired policy, and then click **Edit Settings** next to it.

3 Edit the settings as needed, then click **Save**.

Deleting a policy from the Policy Catalog

Use this procedure to delete a policy from the Policy Catalog. When you delete a policy, all groups and systems where it is currently applied inherit the policy of their parent group. Before deleting a policy, review the groups and systems where it is assigned. If you don’t want the group or system to inherit the policy from the parent group, assign a different policy. If you delete a policy that is applied to the My Organization group, the McAfee Default policy of this category is assigned.

1 From the 4.0 ePO console, select **Systems | Policy Catalog** . From the 4.5 ePO console, select **Menu | Policy | Policy Catalog**, and then select one of the **Solidcore 5.1.0 products** and **Category** from the drop-down menu. All created policies for the selected category appear in the pane.

2 Locate the desired policy, and then click **Delete** in the policy's row.

3 Click **OK** when prompted.

Assigning policies

Use the following procedure to assign your policies.

1 From the 4.0 ePO console, select **Systems | System Tree | Policies**.

2 From the 4.5 ePO console, select **Menu | Systems | System Tree | Assigned Policies**. Select a Product.

3 Next to the **McAfee Default** policy select **Edit assignments**. The Policy Assignments page opens.

4 Create a new policy instance by clicking **New Policy Instance**. Select the policy you have created earlier from the **Assign Policy** drop-down list.

5 Click **Save.**

6 To apply the new policy immediately, perform an agent wake-up call.

Enforcing Polices

Use this procedure to enable or disable policy enforcement for a Solidcore product on a System Tree group.

Policy enforcement is enabled by default and is inherited in the System tree.

1. From the 4.0 ePO console select **Systems | System Tree**.

   From the 4.5 ePO console select **Menu | Systems | System Tree** and then select the desired group in the System Tree.
2. In the Policies tab select the desired Solidcore Product, and then click the link next to **Enforcement Status**. The Enforcement page appears.
3. To change the enforcement status you must first select **Break** inheritance and assign the policy and settings below.
4. Next to Enforcement status, select **Enforcing** or **Not** enforcing accordingly.
5. Choose whether to lock policy inheritance. Locking inheritance for policy enforcement prevents breaking enforcement for groups and systems that inherit this policy.
6. Click **Save**.

More about policies

In the Policy Catalog page, policies are displayed by product and category. For each Solidcore feature you can view policy assignments, where they are applied, and if they are enforced.

NOTE: A McAfee Default policy exists for each category. You cannot delete, edit, export or rename these policies, but you can copy them and edit the copy.

When you reconfigure policy settings, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication. The frequency of this communication is determined by the Agent-to-server-communication interval settings on the General tab of the McAfee Agent policy pages, or the McAfee Agent Wake up client task schedule (depending on how you implement agent-server communication). This interval is set to occur once every 60 minutes by default.

Once the policy settings are in effect on the managed system, the agent continues to enforce policy settings locally at a regular interval. This enforcement interval is determined by the Policy enforcement interval setting on the General tab of the McAfee Agent policy pages. This interval is set to occur every five minutes by default.

Policies are applied to a system by one of two methods:

- Inheritance —Inheritance determines whether the policy settings for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree.
- Assignment — You can assign any policy in the Policy Catalog to any group or system, provided you have the appropriate permissions.

For more information about working with policies refer to the *McAfee ePolicy Orchestrator Product Guide*.

Policy categories

Policy settings for most products are grouped by category. Each policy category refers to a specific subset of policy settings. Policies are created by category. In the Policy Catalog page, policies are displayed by product and category. When you open an existing policy or create a new policy, the policy settings are organized across tabs.

How policy enforcement is set

For each managed product or component, choose whether the agent enforces all or none of its policy selections for that product or component.

From the Assigned Policies page, choose whether to enforce policies for products or components on the selected group.

In the Policy Catalog page, you can view policy assignments, where they are applied, and if they are enforced. You can also lock policy enforcement to prevent changes to enforcement below the locked node.

When policies are enforced

When you reconfigure policy settings, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication. The frequency of this communication is determined by the Agent-to-server-communication interval (ASCI) settings on the General tab of the McAfee Agent policy pages, or the McAfee Agent Wake-up client task schedule (depending on how you implement agent-server communication). This interval is set to occur once every 60 minutes by default.

Once the policy settings are in effect on the managed system, the agent continues to enforce policy settings locally at a regular interval. This enforcement interval is determined by the Policy enforcement interval setting on the General tab of the McAfee Agent policy pages. This interval is set to occur every five minutes by default.

Policy settings for McAfee products are enforced immediately at the policy enforcement interval and at each agent-server communication if policy settings have changed.

Exporting and importing policies

If you have multiple servers, you can export and import policies between them via XML files. In such an environment, you only need to create a policy once. You can export and import individual policies, or all policies for a given product. This feature can also be used to back up policies if you need to reinstall the server.

Policy application

Policies are applied to any system by one of two methods, inheritance or assignment.

Inheritance

When you reconfigure policy settings, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication. The frequency of this communication is determined by the Agent-to-server-communication interval (ASCI) settings on the General tab of the McAfee Agent policy pages, or the McAfee Agent Wake-up client task schedule (depending on how you implement agent-server communication). This interval is set to occur once every 60 minutes by default.

Inheritance determines whether the policy settings and client tasks for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree.

When you break this inheritance by assigning a new policy anywhere in the System Tree, all child groups and systems that are set to inherit the policy from this assignment point do so.

Assignment

You can assign any policy in the Policy Catalog to any group or system, provided you have the appropriate permissions. Assignment allows you to define policy settings once for a specific need, and then apply the policy to multiple locations.

When you assign a new policy to a particular group of the System Tree, all child groups and systems that are set to inherit the policy from this assignment point do so.

Assignment locking

You can lock the assignment of a policy on any group or system, provided you have the appropriate permissions. Assignment locking prevents other users:

- With appropriate permissions at the same level of the System Tree from inadvertently replacing a policy.
- With lesser permissions (or the same permissions but at a lower level of the System Tree) from replacing the policy.

Assignment locking is inherited with the policy settings.

Assignment locking is valuable when you want to assign a certain policy at the top of the System Tree and ensure that no other users replace it anywhere in the System Tree.

Assignment locking only locks the assignment of the policy, but does not prevent the policy owner from making changes to its settings. Therefore, if you intend to lock a policy assignment, make sure that you are the owner of the policy.

For more information refer to the *ePolicy Orchestrator Product Guide*.

Configuring Tasks

The ePolicy Orchestrator allows you to create and schedule client tasks that run on managed systems. You can define tasks for the entire System Tree, for a specific group, or for an individual system.

Like policy settings, client tasks are inherited from parent groups in the System Tree.

NOTE: All tasks are visible but you will get an error message when you try to view, edit, or create an unsupported client task.

Client tasks are commonly used for:

- Product deployment
- Product functionality
- Upgrades and updates

For more information refer to the *ePolicy Orchestrator Product Guide*.

Contents

Working with client tasks

Use these procedures to create and maintain your Solidcore client tasks.

Creating a SC: Begin Update Mode client task

When enforcement is on no changes are allowed on the client. To authorize approved changes to the client, a change window can be defined where the user or program can make changes to the system. Use this procedure to allow authorized or approved changes to the client computers.

NOTE: When creating a SC: Begin Update mode task users should also create an SC: End Update Mode task.

1. From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.
2. Select the desired group in the System Tree, and then click **New Task**. The New Client Task Builder page appears .
3. Type the name of the task and add any descriptive information to the **Notes** field.
4. Select **SC: Begin Update Mode (Solidcore 5.1.0)** from the Type drop-down menu.
5. Click **Next**. The Configuration page appears.

6 Type the Workflow_id and any comments. The workflow_id can be a meaningful description for the update window.

7 Click **Next**. The Schedule page appears.

8 Enable the task, then schedule the task as needed, and then click **Next**. The Summary page appears.

9 Review and verify the details, then click **Save**.

10 To apply your task immediately wake-up the agent.

Creating a SC: Change Local CLI Access client task

Use this procedure to allow or restrict the McAfee Solidcore Agent CLI console access on the client systems. If the local CLI is in the recovered state, enforcement of policies and the execution of tasks will be suspended on the agent. Enforcement of policies and the execution of tasks will resume once the local CLI is in lockdown.

1 From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task**. The New Client Task Builder page appears.

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: Change Local CLI Access (Solidcore 5.1.0)** from the Type drop-down menu.

5 Click **Next**. The Configuration page appears.

6 Configure the **Change Local CLI Access** settings to **Allow** or **Restrict**, then click **Next**. The Schedule page appears.

7 Enable the task, then schedule the task as needed.

8 Click **Next**. The Summary page appears.

9 Review and verify the details, then click **Save**.

10 To apply your task immediately wake-up the agent.

NOTE: Recovering the local CLI access stops enforcement of policies and tasks.

It is recommended that the local CLI recovery password be changed via the General Lockdown Rules policy.

Creating a SC: Collect Debug Info client task

Use this procedure to create a file archive with system information and Solidcore Agent log files for debugging. The location of generated ZIP file is available in the corresponding Client Task Log.

1 From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task**. The New Client Task Builder page appears.

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: Collect Debug Info (Solidcore 5.1.0)** from the Type drop-down menu.

5 No additional configuration is required click **Next**. The Schedule page appears.

6 Enable the task, then schedule the task as needed.

7 Click **Next**. The Summary page appears.

8 Review and verify the details, then click **Save**.

9 To apply your task immediately wake-up the agent.

Creating a SC: Disable Solidcore Agent task

Use this procedure to disable Solidcore Agent on the client computers.

1 From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task**. The New Client Task Builder page appear.

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: Disable (Solidcore 5.1.0)** from the Type drop-down menu.

5 Click **Next**. The Configuration page appears.

6 Select **Force Reboot with the Task** to restart the client system immediately after running the task, then click **Next**. The Schedule page appears.

NOTE: A restart of the client system is necessary to bring the changes into effect.

7 Enable the task, then schedule the task as needed.

8 Click **Next**. The Summary page appears.

9 Review and verify the details, then click **Save**.

10 To apply your task immediately wake-up the agent.

Creating an SC: Enable Solidcore Agent task

Use this procedure to enable Solidcore Agent on the client computers.

1 From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task** . The New Client Task Builder page appears.

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: Enable (Solidcore 5.1.0)** from the Type drop-down menu.

5 Click **Next**. The Configuration page appears.

6 Next to **Enable**, select the required features to enable **Change Control**, **Integrity Monitor**, or **Application Control** .

NOTE:

- Features available depends on the licenses installed.
- When enabling Application Control, there is an option to **Perform Initial Scan to create whitelist**. Activating Application Control requires a one-time system scan to populate a list of trusted executable files present on the client system (called solidification). Select this option to perform the initial scan of the client system while enabling the Solidcore agent. You can deselect this option to defer initial scan to later. If this option is not selected, run SC: Initial Scan to create whitelist client task after the SC: Enable client task is applied and the system is restarted to complete Application Control activation.

7 Select **Force Reboot with the Task** to restart the client system immediately after running the task, then click **Next**. The Schedule page appears.

   NOTE: A restart of the client system is necessary to bring the changes into effect.

8 Enable the task, then schedule the task as needed.

9 Click **Next**. The Summary page appears.

10 Review and verify the details, then click **Save**.

11 To apply your task immediately wake-up the agent.

Creating an SC: End Update Mode client task

Use this procedure to close the update mode window on the desired client systems.

1 From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task** . The New Client Task Builder page appears.

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: End Update Mode (Solidcore 5.1.0)** from the Type drop-down menu.

5 Click **Next**. The Configuration page appears.

6 No additional settings are required for this page.

7 Click **Next**. The Schedule page appears.

8 Enable the task, then schedule the task as needed.

9 Click **Next**. The Summary page appears.

10 Review and verify the details, then click **Save**.

11 To apply your task immediately wake-up the agent.

Creating a SC: Get Diagnostics for programs client task

Use this procedure to retrieve a list of potential updaters tha tcan be added in the Application Policy Catalog to apply on client systems

1 From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task** . The New Client Task Builder page appears.

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: Get Diagnostics for programs (Solidcore 5.1.0)** from the Type drop-down menu.

5 Click **Next**. The Configuration page appears.

6 No additional settings are required on this page.

7 Click **Next**. The Schedule page appears.

8 Enable the task, then schedule the task as needed.

9 Click **Next**. The Summary page appears.

10 Review and verify the details, then click **Save**.

11 To apply your task immediately wake-up the agent.

Creating a SC: Initial Scan to create whitelist client task

Activating Application Control requires one-time system scan to populate the list of executable files present on the client system. Schedule and run this task after SC: Enable client task.

NOTE: This client task is required only if you deselected **Perform Initial Scan to create whitelist** in SC: Enable client task.

1 From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task**. The New Client Task Builder page appears.

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: Initial Scan to create whitelist (Solidcore 5.1.0)** from the **Type** drop-down menu, then click **Next**. The Configuration page appears.

5 Click **Next**. The Schedule page appears.

6 Enable the task, then schedule the task as needed.

NOTE: This task needs to be performed only once on an agent. Select **Schedule type** as **Run Immediately** or **Once**.

7 Click **Next**. The Summary page appears.

8 Review and verify the details, then click **Save**.

9 To apply the task immediately wake-up the agent.

NOTE: This task can take time depending on the number of files present in the client system. A pop-up message is displayed on the client system after the task is completed.

Creating a SC: Pull Inventory client task

Use this procedure to collect the list of executable files and their details (whether they are authorized or unauthorized) from the client system. These details can be accessed from **Reporting | Solidcore | Inventory** tab for analysis and defining new policies.

1 From the 4.0 ePO console, select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task**. The New Client Task Builder page appears.

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: Pull Inventory (Solidcore 5.1.0)** from the Type drop-down menu.

5 Click **Next**. The Configuration page appears.

6 Click **Next**. The Schedule page appears.

7 Enable the task, then schedule the task as needed.

8 Click **Next**. The Summary page appears.

9 Review and verify the details, then click **Save**.

NOTE: To see inventory immediately wake-up should be invoked for the agent to get the task and compute the inventory. A second wake up should be invoked for the client to send the inventory back to ePO.

To make these inventory items searchable you will need to create an SC: Update Inventory Search Indexes server task.

Creating a SC: Run Commands client task

Use this procedure to run a sadmin command remotely on the client to perform tasks such as enabling read protection. Users can enter multiple commands using "+".

1 From the 4.0 ePO console , select **Systems | System Tree | Client Tasks**. From the 4.5 ePO console, select **Menu | Systems | System Tree | Client Tasks**.

2 Select the desired group in the System Tree, and then click **New Task**. The New Client Task Builder page appears .

3 Type the name of the task and add any descriptive information to the **Notes** field.

4 Select **SC: Run Commands (Solidcore 5.1.0)** from the Type drop-down menu.

5 Click **Next**. The Configuration page appears.

6 Type the required command without sadmin prefix.

For example, type features enable deny-read to enable read protection.

7 Select **Requires Response** if you want to view the status of the commands in **Reporting | Solidcore| Client Task Log** tab.

8 Click **Next**. The Schedule page appears.

9 Enable the task, then schedule the task as needed.

10 Click **Next**. The Summary page appears.

11 Review and verify the details, then click **Save**.

12 To apply your task immediately wake-up the agent.

The read protection feature is disabled by defaults on clients. To enable this feature use this task with the following command features enable deny-read.

Working with server tasks

Use these procedures to create and maintain your Solidcore server tasks.

Creating a Solidcore: Purge server task

Use this procedure to purge Solidcore reporting features. You can purge Solidcore reporting features by age. When you purge results, the records are deleted permanently.

1 From the 4.0 ePO console, select **Automation | Server Tasks**. From the 4.5 ePO console, select **Menu | Automation | Server Tasks** and then click **New Task**. The Server Task Builder page opens.

2 Enter a **Name** describe the task, and click **Enabled** after Schedule status.

3 Click **Next**. The Actions page appears.

4 Select **Solidcore: Purge Task** from the **Actions** drop-down menu.

5 Configure these options as required then click **Next**. The Schedule page appears.

- Choose Feature - Select the Solidcore reporting feature for which you want to purge records.
- Purge records older than - Select this option to purge the selected feature record entries older than the specified age. This option is not applicable for features that do not have ageing criteria (For example, Inventory records).
- Purge by query - This option is only applicable to Solidcore reporting features that support queries in ePO. Purges the selected feature record entries meeting the query criteria.

  NOTE:

  - To purge records by queries, create the required query from **Menu | Reporting | Queries** (in ePO 4.5 console) or **Reporting | Queries** (in ePO 4.0 console).
  - This option is supported only for tabular query results.

6 Schedule the task as needed, and then click **Next**. The Summary page appears.

7 Review and verify the details, then click **Save**.

Creating a Solidcore: Run Image Deviation server task

Image deviation is used to compare the inventory of a system with the inventory fetched from a designated gold system. This helps users to track inventory present on a client system, if any changes occur they can be brought to attention immediately.

NOTE: Run Image Deviation will only work when the Inventory has been pulled for that system.

Use this procedure to choose a gold system and compare other systems to it.

1 From the 4.0 ePO console, select **Automation | Server Tasks**. From the 4.5 ePO console, select **Menu | Automation | Server Tasks** and then click **New Task**. The Server Task Builder page appears.

2 Enter a **Name** describe the task, and click **Enabled** after Schedule status.

3 Click **Next**. The Actions page appears.

4 Select **Solidcore: Run Image Deviation** from the drop-down menu.

5 Select the system to use as the gold system.

6 Configure these options as required, then click **OK**.

- **System to compare with Gold System** — Click **Add** to search for the system that you want to compare with the gold system. Type the name of the system in the Search for systems available on ePO dialog box, then click **Search**.
- **Groups to compare with Gold System** — Click **Add** to search for the system group that you want to compare with the gold system. Type the name of the system group in the Search for Groups available on ePO dialog box, then click **Search**.
- **Include Systems with Tags** — Click **Add** to search for systems based on their tag names. Type the name of the tag in the Search for Tags available on ePO dialog box, then click **Search**.
- **Exclude Systems with Tags** — Click **Add** to search for the system based on their tag names. Type the name of the tag in the Search for Tags available on ePO dialog

box, then click **Search**. Select the required tag from the search result. The client systems with the selected tag(s) are excluded from comparison with the gold system.

7 Click **Next**. The Schedule page appears.

8 Schedule the task as needed, and then click **Next**. The Summary page appears.

9 Review and verify the details, then click **Save**.

The result of the comparisons would show the deviations from the gold image. Users can view the results of their comparison of inventories in **Reporting | Solidcore | Image Deviation**.

Creating a Solidcore: Scan a Software Repository server task

This task scans the repository to find installers and publishers.

1 From the 4.0 ePO console, select **Automation | Server Tasks**. From the 4.5 ePO console, select **Menu | Automation | Server Tasks** and click **New Task**. The Server Task Builder page opens.

2 Enter a **Name** describe the task, and click **Enabled** after Schedule status.

3 Click **Next**. The Actions page appears.

4 Select **Solidcore: Scan a Software Repository** from the drop-down list.

5 Specify the path of the repository that is accessible from the ePO server.

NOTE: The subfolders in the repository are also scanned for installers and publishers.

6 Type the **Domain**, **User Name**, and **Password** to access the specified network location.

7 Click **Test Connection** to ensure that the connection to the specified network location works.

8 Select **Add extracted certificates and installers to Rule Group** if you want to add the certificates and installers extracted by the task to user-defined rule group, then select the user-defined rule group from the drop-down list.

NOTE:

- You can add extracted certificates and installers only to user-defined rule groups.
- If the selected rule-group is added to a policy, extracted certificates and installers will be automatically added to the Policy.

9 Click **Next**. The Schedule page appears.

10 Schedule the task as needed, and then click **Next**. The Summary page appears.

11 Review and verify the details, then click **Save**.

Create a Solidcore: Update Inventory Search Indexes server task

Use this procedure to update inventory search indexes with a scheduled server task.

1 From the 4.0 ePO console, select **Automation |Server Tasks**. From the 4.5 ePO console, select **Menu | Automation | Server Tasks** and then click **New Task**. The Server Task Builder page.

2 Enter a **Name**, describe the task, and click **Enabled** after the Schedule Status.

3 Click **Next**. The Actions page appears.

4 Select **Solidcore: Update Inventory Search Indexes** from the drop-down menu.

5 Click **Next**. The Schedule page appears.

6 Schedule the task as needed, and then click **Next**. The Summary page appears.

7 Review and verify the details, then click **Save**.

NOTE:

- To get data to display on the UI immediately, run the **Update Inventory search indexes** server task immediately.
- Set this up to run as a scheduled task daily so that inventory data is updated periodically.

Reports and Queries

From the ePolicy Orchestrator console, you can view reports which show the status of the Solidcore client computers. You can also create reports using data sent by the Agent in the selected ePolicy Orchestrator database. You can save the selections you make in the Enter Report Inputs and Report Data Filter dialog boxes for future use.

ePolicy Orchestrator reports allow you to:

Set a directory filter to gather only the information that you want to view. When setting this filter, you can choose which part of the ePolicy Orchestrator console tree is included in the report.

- Set a data filter, by using logical operators, to define precise filters on the data returned by the report.
- Generate graphical reports from the information in the database, and filter the reports as desired. You can print the reports and export them for use in other software.
- Conduct queries of computers, events, and installations.

Contents

Managing Alerts

Alerts can be created based on events generated by the Solidcore products.

Defining an alert

Use this task to define an alert.

1. From the 4.0 ePO console, select **Automation | Responses**. From the 4.5 ePO console, select **Menu | Automation |Automatic Response**s.
2. Click **New Response**. The Response Builder page opens to the Description page.
3. Enter a Name, select **Solidcore Events** as **Event Groups**, **All Events** as **Event Type** then select **Enabled**.
4. Click **Next**. The Filter page appears.

5 Select from one or more **Available Properties** options, then click **Next**. The Aggregation page appears.

NOTE: When configuring Alerts use the full path to perform an **equals** match or use **{name}.exe** with an **ends with** match.

6 Select one of these options as required, then click **Next**. The Actions page appears.

- **Trigger this response for every event** — Triggers response for each events that matches filter criteria.
- **Trigger this response if multiple events occur within** — Triggers response for a groups of events that meet filter criteria and aggregation criteria

7 Select **Show Alert in Reporting** from the drop-down menu.

8 Select from one of available actions and enter:

- Severity — Set the severity level of the alert from the drop-down list.
- Insert variable — Select the required variable from the drop-down list.
- Insert — Click this to insert the selected variable in **Message**.
- Message — Type or insert the variable to be added in the alert.

9 Click **Next**. The Summary page appears.

10 Review the alert detail's then click **Save**.

Viewing an alert

Alerts can only be viewed if the user has selected **Show Alert in Reporting** while configuring the alert. Use this task to view alerts.

1 From the 4.0 ePO console, select **Reporting | Solidcore**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore**.

2 Select the **Alerts** tab, the alerts page opens.

Dismissing an alert

Use the following procedure to dismiss alerts.

1 From the 4.0 ePO console, select **Reporting | Solidcore | Alerts**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore | Alerts**.

2 Select the alert, then click **Actions | Dismiss**.

Default Solidcore queries

The Queries page provides a set of queries that provide high-level reports checks rules, and file integrity. The solidcore queries are:

Solidcore: Alerts

This report displays all Solidcore alerts by severity in the last three months.

Solidcore: Application Control Agent Status

This report displays the status of Solidcore Application Control Agents managed by the ePolicy Orchestrator.

Solidcore: Attempted Violations Detected in the last 24 Hours

This report displays the attempted violation events detected during the last 24 hours.

Solidcore: Attempted Violations Detected in the last 7 Days

This report displays the attempted violation events detected during the last seven days.

Solidcore: Change Events grouped by Reconciliation Status in the Last 1 Month

This report displays a pie chart of events that occurred in the last one month organized by whether the change event has been reconciled against a change ticket or not. Reconciled changes are shown as authorized and un-reconciled events are shown as unauthorized.

Solidcore: Change Events grouped by Reconciliation Status in the Last 7 Days

This report displays a pie chart of events that occurred in the last seven days organized by whether the change event has been reconciled against a change ticket or not. Reconciled changes are shown as authorized and un-reconciled events are shown as unauthorized.

Solidcore: Integrity Monitor Events Detected in the Last 24 Hours

This report displays all the Integrity Monitor events that were detected during the last 24 hours on a per hour basis.

Solidcore: Integrity Monitor Events Detected in the Last 7 Days

This report displays all the Integrity Monitor events that were detected during the last week on a per day basis.

Solidcore: Integrity Monitor Agent Status

This report displays the status of all Integrity Monitor agents being managed by the ePolicy Orchestrator.

Solidcore: Out of Band Change Events Detected in the Last 24 Hours

This report displays change events which are not done as per update policy in the last 24 hours.

Solidcore: Out of Band Change Events Detected in the Last 7 Days

This report displays change events which are not done as per update policy in the last 7 days.

Solidcore: Policies Applied on Host

This report displays a list of all policies applied on hosts.

Solidcore: Reconciled Change Events grouped by Tickets in the Last 1 Month

This report displays change tickets against which events have been reconciled in the last one month.

Solidcore: Reconciled Change Events grouped by Tickets in the Last 7 Days

This report displays change tickets against which events have been reconciled in the last seven days.

Solidcore: Solidcore Agent License Report

This report displays the number of Solidcore Agents being managed by the server, grouped by license type.

Solidcore: Solidcore Agent Status Report

This report displays the status of all Solidcore Agents being managed by the ePolicy Orchestrator.

Solidcore: Top 10 Change Events in the Last 7 Days

This report displays the top 10 change events that occurred during the last seven days.

Solidcore: Top 10 Programs with Most Change Events in the Last 7 Days

This report displays the top 10 programs with most changes during the last seven days

Solidcore: Top 10 Systems with Most Violations in the Last 24 Hours

This report displays the top 10 systems with the most violations during the last 24 hours.

Solidcore: Top 10 Systems with Most Violations in the Last 7 Days

This report displays the top 10 systems with the most violations during the last seven days.

Solidcore: Top 10 Users with Most Change Events in the Last 7 Days

This report displays the top 10 users with the most changes during the last seven days.

Solidcore: Top 10 Users with Most Change Events in the Last 24 Hours

This report displays the top 10 users with the most changes during the last 24 hours.

Solidcore: Top 10 Users with most Violations Detected in the Last 24 Hours

This report displays the top 10 users with the most policy violation attempts detected in the last 24 hours.

Solidcore: Top 10 Users with Most Violations Detected in the Last 7 Days

This report displays the top 10 users with the most policy violation attempts detected in the last seven days.

Solidcore: Non Compliant Solidcore Agents

This report lists Solidcore Agents which are either Disabled or where local CLI access is recovered. Disabled agents do not provide and Integrity Monitor or Application Control functionality on the client. The ePO policy and task enforcement is suspended.

Viewing Reports

To view the reports:

1. From the 4.0 ePO console, select **Reporting | Queries**. Then select the appropriate report from the Queries list.
2. From the 4.5 ePO console, select **Menu | Reporting | Queries**. From **Groups** select **Solidcore** and then select the appropriate report from the Queries list.
3. Click **Run**. The report will be displayed.
4. Click **More Actions** to view further actions that you can take.

Queries

Queries are configurable objects that retrieve and display data from the database. The results of queries are displayed in charts and tables. Most queries can be used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).

Exported results

Query results can be exported to four different formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Unlike query results in the console, data in exported reports is not actionable.

Reports are available in several formats:

- CSV - use the data in a spreadsheet application (for example Microsoft Excel)
- XML - transform the data for other purposes
- HTML - view the exported results as a web page
- PDF -print the results as a PDF

Working with queries

Use these procedures to create, use and manage queries.

- Creating custom queries
- Running an existing query
- Making a query public

Creating custom queries

Use this procedure to create custom queries with the Query Builder wizard. You can query on system properties, product properties, many of the log files, repositories, and more.

1. From the 4.0 ePO console, select **Reporting | Queries**. From the 4.5 ePO console, select **Menu | Reporting | Queries**, and then select **Actions | New Query**. The Query Builder page opens.

2 On the Result Type page, select from the list of available queries for example, solidcore Events, Non compliant Solidcore Agents, Solidcore Alerts, Solidcore Inventory and Solidcore Change Management Compliance. The Chart page appears.

NOTE: This choice determines the options available on subsequent pages of the wizard.

3 Select the type of chart or table to display the primary results of the query, and then click **Next**. The Columns page appears.

NOTE: If you select Boolean Pie Chart, you must configure the criteria to include in the query.

4 Select the columns to be included in the query and then click **Next**. The Filter page appears.

NOTE: If you selected Table on the Chart page, the columns you select here are the columns for the table. Otherwise these are the columns that make up the query details table.

5 Select properties to narrow the search results, and then click **Run**. The Unsaved Query page displays the results of the query, which is actionable, so you can take any available actions on items in any tables or drill down tables.

- If you do not need to save the query, click **Close**.
- If this a query you want to use again, click **Save** and continue to the next step.
- The Save Query page appears. Type a name for the query, add any notes.

6 Click **Save**.

Running an existing query

Use this procedure to run an existing query from the Queries page.

1 From the 4.0 ePO console, select **Reporting | Queries**. From the 4.5 ePO console, select **Menu | Reporting | Queries**, and then select a query from the Queries list.

2 Click **Run**. The query results page appears. Drill down into the report and take actions on items as necessary. Available actions depend on the permissions of the user.

3 Click **Close** when finished.

Solidcore reporting tabs

Solidcore activity can be viewed from **Reporting | Solidcore**. The following Solidcore tabs are available:

- **Events** — All Integrity Monitor and Application Control events generated from the client computers can be viewed from this tab.
- **Alerts** — Use this tab to view Solidcore related alerts.
- **DB Audit** — This is only available from the McAfee Analytics Server. If you have configured an Analytics Server URL in the ePO you will be able to access it from this tab and login as DB admin user to view DB Audit.
- **Network Control** — This is only available from the McAfee Analytics Server. If you have configured an Analytics Server URL in the ePO you will be able to access it from this tab and then go in a view Network Control.
- **Reconciliation** — Has two tabs

Reconciliation Summary — Use this to view a comprehensive inventory of the changes carried out on all systems, grouping and matching them with change tickets and approvals.

Configure Reconciliation — If you have configured an Analytics Server URL in the ePO you will be able to access it from this tab and then configure reconciliation.

- **Inventory** — Allows you to search by Binary, Name, SHA1, Product Name and Vendor.
- **Image Deviation** — Any changes such as modifications, deletions or additions in the system inventory to a golden inventory can be viewed via this tab.
- **Client Task Log** — Client task responses are displayed.

Filtering Solidcore events

Use this task to filter Solidcore events based on their age and system tree group level.

Task

For option definitions, click **?** in the interface.

1. From the 4.0 ePO console, select **Reporting | Solidcore | Inventory**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore | Events**.
2. Configure these filter options as required.
   - Time Filter — Use this option to filter events recorded within the specified time period.
   - System Tree Filter — Use this option to filter events recorded from the specified system group or subgroup.
   - Advanced Filters — Opens the Edit Filter Criteria page. Use this to select from a list of available properties to filter the content displayed in the Solidcore Events tab.

Searching for an Inventory

Use this task to search for an Inventory based on the name of the binary file, checksum of the binary, name of the product, name of the vendor, name of the system from which it was collected.

Task

For option definitions, click **?** in the interface.

1. From the 4.0 ePO console, select **Reporting | Solidcore | Inventory**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore | Inventory**.
2. Configure these filter options as required, then click **Search**.
   - Binary Name — Use this option to search inventory data by their binary names.
   - Checksum (SHA1) — Use this option to search inventory data by their checksum (SHA1) details.
   - Product — Use this option to search inventory data by their product names.
   - Vendor — Use this option to search inventory data by their vendor names.
   - System Name — Use this option to search inventory data by the system names.

Viewing details of an inventory

Use this task to view the system details of the selected inventory.

Task

For option definitions, click **?** in the interface.

1. From the 4.0 ePO console, select **Reporting | Solidcore | Inventory**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore | Inventory**.
2. Search for the required inventory, then click **System-Details** next to it. The System Details page appears.

The inventory system details page displays the binary name, checksum (SHA1), system name, and the path of the binary file to which the inventory belongs to. The field Execution Allowed displays if the binary is allowed or banned for execution on the client system.

Click on the row to know more details on **Execution Allowed** status. The Inventory details page appears. The **Execution Permissions** section on the page explains the rules governing **Execution Allowed** status. The order of listing of rules reflects the priority. For example, if for an executable, the **Allow by Checksum** permission is **No** and **Allow by Name** is **Yes**, then **Execution Allowed** will be **No** for the executable because **Allow by Checksum** permission has higher priority.

This page also provides the link to access the events generated for a particular inventory item. Click on Event History link for an inventory item and the Change History page appears. This displays details of change events associated with the inventory item e.g., event timestamp, Event Display Name, File, and User name.

Filtering Client Task Logs

Use this task to search for Client Task Logs based on the client system to which they were assigned, time when they were executed, command status after execution, name of the task, and status of the task.

Task

For option definitions, click **?** in the interface.

1. From the 4.0 ePO console, select **Reporting | Solidcore | Client Task Log**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore | Client Task Log**.
2. Configure these filter options as required, then click **Search**.
   - System Name — Type the name of the system based on which you want to filter the client task log.
   - Time — Specify the time period within which the client task was executed.

     NOTE: Client Task Logs for time-based filtering considers the start time of the client task.

   - Task Name — Type the name of the task based on which you want to filter the client task log.
   - Task Status — Select the status of the client task based on which you want to filter the client task log.
   - Command Status — Select the status of the command executed through client task based on which you want to filter the client task log.

Searching for an Image Deviation result

Use this task to search for an Image Deviation result based on the target system.

Task

For option definitions, click **?** in the interface.

1. From the 4.0 ePO console, select **Reporting | Solidcore | Image Deviation**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore | Image Deviation**. The Image Deviation Summary Listing page appears.
2. Type the name of the target system, then click **Search**.
   The Image Deviation Summary Listing page displays the filtered Image Deviation results with the following details.
   - Compared at — Displays the date and time when the Image Deviation task was run.
   - Target System Agent GUID — Displays the Agent GUID of the target system.
   - Target System — Displays the name of the client system which was compared with the gold system.
   - Gold System — Displays the name of the gold system with which the client system was compared
   - Files Added — Displays the number of files added on the client system.
   - Files Missing — Displays the number of files deleted from the client system.
   - Files Modified — Displays the number of files modified on the client system.

Filtering Image Deviation results

Use this task to filter Image Deviation results by the deviation type or the file path.

Task

For option definitions, click **?** in the interface.

1. From the 4.0 ePO console, select **Reporting | Solidcore | Image Deviation**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore | Image Deviation**. The Image Deviation Summary Listing page appears.
2. Click **View** on the required Image Deviation result row. The Image Deviation Details page appears.
3. Configure these filter options as required, then click **Search**.
   - Filter by Deviation Type — Filters the image deviation details based on the selected the deviation type.
   - Filter by Path — Filters the image deviation details based on the comparison operator and the file path.

Reconciliation

McAfee Change Reconciliation creates a comprehensive inventory of the changes carried out on all systems, grouping and matching them with change tickets and approvals. It flags ad-hoc changes made without approvals, and documents emergency changes that were made with improper documentation.

Change Reconciliation operating in concert with Change Control, integrates with popular change management systems such as HP Service Manager and BMC Remedy.

Change Reconciliation verifies that approved changes have been deployed and identifies unapproved or unticketed changes (for example, emergency changes) with a high degree of accuracy.

Change Reconciliation automatically validates changes corresponding to an approved and implemented request for change (RFC) based on the identifying hostname or configuration item (CI), actual start time, actual end time, and username. After reconciliation, the RFC is updated with detailed information about the change, including the name of the user who made the change, the CI/hostname that changed, and a link to a detailed report of changes.

NOTE: Reconciliation is only available for Change Control.

Contents

Configuring the McAfee Analytics Server URL

Use this procedure to configure the Analytics Server URL from the ePolicy Orchestrator.

1. From the 4.0 ePO console, select **Configuration | Server**. From the 4.5 ePO console, select **Menu | Configuration | Server Settings**.
2. From the Settings Categories List select **Solidcore**.
3. Select **Edit**.
4. Enter your **Analytics Server URL**.
5. Click **Save**.

Accessing Reconciliation from the ePO

The McAfee Analytics Server reconciliation correlates the changes made on servers to change tickets documented in existing ticketing systems and integrates with popular ticketing systems such as BMC Remedy. To access the Analytics Server from the ePolicy Orchestrator:

1 From the 4.0 ePo console, select **Reporting | Solidcore |Reconciliation**. From the 4.5 ePO console, select **Menu | Reporting | Solidcore | Reconciliation**. The Reconciliation summary page appears and provides details of the last reconciliation.

2 Select **Configure Reconciliation**. The Analytics Server Login screen appears.

NOTE: Users are required to have db_datareader and db_datawriter rights on the ePO database tables for reconciliation to run when connecting to the ePO SQL server.

3 Login to the Analytics Server.

For more information refer to the *McAfee Analytics Server Deployment Guide (MFE_AS_ALL_DG.pdf)*.

Viewing Reconciled events

Reconciled events are change events on the hosts or groups monitored by the solidified server that are reconciled or matched to change event tickets in the Change Management System.

Use this task to view reconciled events.

Task

For option definitions, click **?** in the interface.

1 At the bottom of the screen under **Reconciliation Actions** select the **Reconciled Tickets** link. The Reconciled tickets Summary page appears.

2 To view details for a particular ticket select the **View Reconciled Changes** link.

Viewing unauthorized events

Unauthorized change events on the hosts or groups are events that could not be matched to any change tickets in the Change Management System.

Use this task to view Unauthorized events.

Task

For option definitions, click **?** in the interface.

1 At the bottom of the screen under **Reconciliation Actions** select the **Systems with Unauthorized Changes** link. The Unauthorized Changes Summary page that lists all the unauthorized change events appears.

2 Click the **View changes** link next to a system to view the corresponding unauthorized event count for the system.

3 Do one of these:

- To create a ticket for an unauthorized event, click the checkbox corresponding to the event and click **Actions | Document**.

- To create tickets for all the unauthorized events, click the checkbox in the table heading and click **Actions | Document**.

4 In the Document Unreconciled Change dialog box, type the **Ticket Summary** and **Description**, then click **Save**.
An informational dialog box appears stating that the Ticket ID is created for the server. These changes will be shown in the Reconciled Changes summary page.

Authorizing changes that match multiple tickets

Unresolved events are those change events on the hosts or groups that match with multiple tickets in the Change Management System.

Use this task to view Authorized Unresolved events.

Task

For option definitions, click **?** in the interface.

1 At the bottom of the screen under **Reconciliation Actions** select the **Systems with changes that match multiple Tickets** link. The Changes that match multiple Tickets Summary page appears.

2 To resolve event(s), click the checkbox corresponding to the event and click **Actions | Resolve**.

3 In the Actions Resolved dialog box, select the ticket you want to map the change to. All the ticket IDs which can be mapped to this change are displayed. You can select the required ticket ID to associate this change to. After resolving, the resolved event(s) will be displayed in the Reconciled Changes summary page. The Summary page will update after 60 minutes.

NOTE: Only ticket IDs that matched the change will be displayed.

Dashboards

The ePolicy Orchestrator and Solidcore integration provides a dashboard showing commonly viewed information.

Dashboards allow you to keep constant watch on your Solidcore environment and are a collection of monitors, or reports. Users must have the appropriate permissions to use and create dashboards. The Solidcore dashboard provides an overview of access-related activities occurring on your ePO server.

Change dashboards provide at a glance reporting of key parameters such as change policy compliance, changes on critical systems by user applications, by host etc.

Queries as dashboard monitors

Dashboards are collections of user-selected and configured monitors that provide current data about your environment. You can create your own dashboards from query results or use Solidcore default dashboards.

Solidcore Dashboards

The Solidcore extension provides the following three dashboards:

- Change Control dashboard
- Integrity Monitor dashboard
- Application Control dashboard

Contents

Setting up dashboards for the first time

When setting up dashboards for the first time:

- Decide which default dashboards and default monitors you want to use.
- Create any needed dashboards and their monitors and be sure to make active any you want available as tabs from the navigation bar.

Refer to the ePolicy Orchestrator documentation for detailed information on how to build query reports that can be added to a dashboard.

Viewing the Solidcore dashboards

The ePO and Solidcore integration provides a dashboard showing commonly viewed information.

Use this procedure to view the Solidcore Dashboard provided by the ePO.

1 to add the Solidcore:Dashboard to your active dashboards (this only needs to be done once):
   - From the 4.0 ePO console, select **Dashboards | Options | Manage Dashboards |**select a **Solidcore Dashboard**. From the 4.5 ePO console, select **Menu | Dashboards | Options | Manage Dashboards |** select a **Solidcore Dashboard**.
   - Click **Make Active**.
   - When prompted, click **OK** to make the selected dashboard active.
2 To view the dashboard select **Dashboards | Solidcore Dashboard**.

Creating a dashboard

Use this procedure to view the Solidcore Dashboard provided by the ePO.

1 From the 4.0 ePO console, select **Dashboards**. From the 4.5 ePO console, select **Menu | Dashboards** and then click **Options | New Dashboards**.
2 Type a name and select a size for the dashboard.
3 For each monitor, click **New Monitor**, select the monitor category as Queries.
4 Select from one of the available Solidcore monitor options and then click **OK**.
5 Click **Save**, then select whether to make this dashboard active. Active dashboards are displayed on the tab bar of Dashboards.
6 Optionally, you can make this dashboard public from the Managed Dashboards page by clicking **Make Public**.

   NOTE: All new dashboards are saved to the private My Dashboard category.

Making a dashboard active

Use this procedure to ,make a dashboard part of your active set.

1 From the 4.0 ePO console, select **Dashboards**. From the 4.5 ePO console, select **Menu | Dashboards** and then click **Options | Select Active Dashboards**. The Select Active Dashboards page appears.
2 Select the dashboards you want to activate from the **My Dashboard** list, and then click **OK**.

Selecting all active dashboards

Use this procedure to select all dashboards that make up your active set. Active dashboards are accessible on the tab bar under Dashboards.

1 From the 4.0 ePO console, select **Dashboards**. From the 4.5 ePO console select **Menu | Dashboards**, and then select **Options | Select Active Dashboards**. The Select Active Dashboards page appears.

2 Click the desired dashboards from the Available Dashboards list. They are added to the content pane.

3 Repeat the above step until all dashboards are selected.

4 Arrange the selected dashboards in the order you want them to appear on the tab bar.

5 Click **OK**. The selected dashboards appear on the tab bar whenever you open the Dashboards page of the product.

Making the Solidcore dashboard public

Use this procedure to make a private dashboard public. Public dashboards can be used by any user with permissions to public dashboards.

1 From the 4.0 ePO console, select **Dashboards**. From the 4.5 ePO console, select **Menu | Dashboards** and then select **Options | Manage Dashboards**.

2 Select the **Solidcore** dashboard from the Available Dashboards list, click **Make Public**.

3 Click **OK** when prompted.

4 Click **Close**.

The Solidcore dashboard appears in the Public Dashboards list on the Manage Dashboards page.

FAQs

How do I identify which files to monitor and create a policy?

This is a real-world use case scenario where several steps lie outside the scope of the product.

- Identify key applications installed on a client.
- Identify their installation directories, configuration files, registry keys and process names.
- Solidcore ships with pre-defined filters for certain applications. Please use one if it has already been provided. Otherwise, create your own policy as outlined below.
- Create a policy to monitor each application (file, registry key, extension, process, user and advanced rules). A typical way to do this could be:
  - Include the install directory, registry keys and configuration files
  - Monitor log files for tampering
  - Exclude the process of the application
- Assign this policy and apply to the client / group of clients.
- Check for events periodically and test and refine the policy. Any events that are generated regularly during the normal operation of an application should be filtered out using the available filtering mechanisms.

After applying a write-protection policy, my application is not working as before. how do I proceed?

It is likely that the application has a legitimate need to write to the protected file that but is prevented from doing so, hence it fails.

1. Check whether there are any "events which end with Denied for the client under the Events tab or run the Attempted Violations report.
2. If you find such events, verify whether any of the Denied events are reported for the failing application.
3. If so, make the application a trusted program for that write-protected file so that it can update it when it runs and the failures are avoided.

How do I run the AD group sync from the cmd line?

To execute AD sync immediately via the cmd line complete the following steps:

1. Start the shell-client.bat from the ePO remote client.
2. In interactive mode enter shell-client.bat [:port] user password [http | https] [post | soap].
3. When prompted type the following scor.cmd.syncADgroups cmdType=syncADgroups.
4. Press **Enter**.

How can I configure Reconciliation from a legacy Analytics Server using Windows Authentication?

Installation of the ePO with default SQL Express installs SQL Express with windows authentication only. To configure reconciliation from legacy Analytics Server on this database do one of the following:

- Both the ePO database and the legacy Analytics Server have to be on domain. The Analytics Server domain user login has to be created on SQL Express first and then reconciliation can be configured using windows authentication.
- Configure SQL Express as both SQL Server and Windows authentication mode. Then enable the "sa user" and configure reconciliation using "sa user".

If the ePO SQL Server is running in Windows Authentication mode, do the following:

- Legacy Analytics Server, ePO and SQL Server should be installed in the same domain.
- Legacy Analytics Server service should be run as a Domain User.
- The above Domain user should be added to SQL Server and should have same permissions as the ePO User.

Why am I getting so many Command Execute events from my Agent machine?

Events with commands such as sadmin status - sx, sadmin license list-x, sadmin mon list-x, sadmin updaters list -x, sadmin aef list-x generate Command Executed events.

These commands are executed locally on the client machine by the MA 'plugin' DLL for the Solidcore Agent, while enforcing the policies that verify the local configuration rules match with the ones specified by the (remote) ePO policy rules. In order to filter the events generated because of 'Command Execution' for these commands, the default installation has been configured with "Advanced exclude filters" (aef). The McAfee Default Policy (Minimal System Monitoring) has also been configured with 'Advanced exclude filters' (McAfee Agent 4.0 Windows Base Filters). This was based on the assumption that users would either apply the 'Minimal System Monitoring' and then define a new policy for their monitored set (Integrity Monitoring Rules are multi-slot) or if they choose to define a policy completely from blank, they would add 'McAfee Agent base filter' to remove extra events.

Users applying a new Integrity Monitor policy to the client, in order to filter out the unwanted events related to every policy enforcement interval, may either add 'Agent 4.0 Windows Base Filters' rule group to the new policy or just add the one rule explicitly to the policy for example:

How do I run a custom command on the Solidcore Agent and view the output on the ePO?

Use the following procedure to run any command on the Agent.

1. Create a new client task on the Agent machine and select **SC: Run Commands (Solidcore 5.1.0)** from the drop-down.
2. Enter the commands that you want to run but without the "sadmin" part of the command. For example, to run a "sadmin status", you type "status". Add as many commands as required by clicking **+** on the left of the check boxes.
3. To view the output for the commands you entered check the **Requires Response** check box.

4 On the Schedule page select **Run Immediately** or and other time you want this command to run.

5 **Save** this task. If you had selected "Run Immediately", it is a good idea to "Wake up Agents", as this will run the command(s) on the Agent machine.

6 To view the command response immediately in the Client Task log, run a wake-up agent again. Command responses can then be viewed from for **Reporting | Solidcore | Client Task Log** page where you can select to see the output of the command(s) that were executed.

What are the implications of recovering the local CLI access on the client?

Recovering the local CLI will stop the enforcement of policies from ePO to the client. This means once the CLI has been recovered on the client, no new policy, created on the ePO, will be applied to that client.

Can the same Solidcore Agent be used for Change Control, Integrity Monitor, and Application Control?

The license key determines which features will be enabled; any or all features can be used at the same time.

Do we have to add 8081 port in Firewall exception rules on client machines if the firewall is enabled on the client machine?

Once the McAfee Agent is deployed on a client machine, it adds the McAfee Framework Service to the firewall exception rules. Therefore it is not required to manually open 8081 port (the ePO uses this port to send wake-up agent calls to the client) on the client side.

Do the default FIM policies meet PCI requirements to monitor critical files?

The default FIM policies satisfy the PCI requirements, customers need only to add rules for payment applications.

Does Solidcore work in NATed environments?

If the ePO is able to communicate with the CMA in a NATed environment then there should not be any problem in Solidcore working with the ePO as Solidcore communicates with ePO through CMA.

How do I view Agent logs from the ePO browser?

By default the Agent log viewing is disabled on the 4.5 ePO. To enable agent log viewing enable following McAfee Agent policies:

- Accept connection only from the ePO server as unchecked (McAfee Agent policy pages, General tab).
- Enable remote access to log is checked (McAfee Agent policy pages, Logging tab) Send wake-up agent to host machine. Agent logs can only be viewed with Internet Explore.

Agent log viewing is enabled on the 4.0 ePO.

Can I start/stop/restart a Solidcore client product service from the ePO?

On Windows there is no way to start and stop a ser vice from the ePO.

On a UNIX platform this can be done from the ePO by creating a Solidcore Run Command task with the Sadmin Restart command. Then apply the task to the UNIX client machine with a wake-up agent.

How can I trust custom scripts and applications developed for usage within my organization?

This can be achieved by signing the scripts and applications with a self-generated certificate, then trusting this certificate.

1. Generate X.509 certificate pair using a tool like **makecert.exe**.

   For more information see http://msdn.microsoft.com/en-us/library/bfsktky3%28VS.80%29.aspx. You can skip this step if you already have a certificate.
2. Export the certificate in PEM (Base 64 Encoded DER) format.
3. Upload the Certificate to an Application Control Policy as a trusted publisher and apply the policy.
4. Use the certificate to sign and verify the binary. This can be done using a tool like **SignTool.exe**.

   NOTE: In case of scripts, convert the script into a self extracting executable file, then sign the fie. (To allow execution of a signed script wrapped into a self extracting exe, add the publisher as an updater in the Application Control policy.)
5. You can now copy the signed binary to a client and execute it.

How can I use Solidcore's Diagnostic feature to know which executables may be made updaters at the client?

This feature can be used to help identify updater rules in case certain applications do not function correctly after solidcore is enabled.

Solidcore Agent keeps track of attempts made by authorized executables to modify/run other executables / protected files which are denied by Solidcore. It is possible to use this data to configure such executables as updaters so that they are not denied by Solidcore the next time.

There are two main tasks to be done for using the Diagnostic feature Fetch the diagnostic recommendations from the client into ePO.

- Run the **SC: Get Diagnostics for Programs** client task to get diagnostic output from the client. Check if the task was successful from **Reporting | Solidcore | Client Task Log**. This task collects the diagnostic data at the end point which then sent to ePO as events at the next Agent communication interval.

  NOTE: To send the data immediately, open the McAfee Agent Status Monitor on the client system then click **Send Events** to upload events to ePO.

- Perform these steps to use the diagnostic recommendations in ePO for defining updaters in an Application Control policy.
  1. Click **Edit** next to the required Application Control policy.
  2. Click **Diagnostic Suggestions**. The Add Updater dialog box appears.
  3. Search for a list of executables/binaries that are suggested as updaters by diagnostics.
  4. Select the required executables/binaries, then click **OK**.
  5. Save the policy to add the rule to it.

When I enable Application Control, how can I ensure that I have the right updaters? Does Application Control have a "learning" mode?

Application Control has a learning mode called the **Update** mode. After enabling Application Control, run the SC: Begin Update Mode client task and use the client systems in update mode for one or two weeks. Run the SC: Get Diagnostics for programs client task to get updater recommendations and add the new updaters in the Application Control policy using **Diagnostic Suggestions**.

What is the significance of Updater label, User Label, or Installer Label in Application Control and Change Control policy tabs?

These labels help relating the events raised for the actions performed by the trusted resources. For example, executables marked as Updaters, Trusted Users, Publishers, or Installers User can specify Labels for the trusted resources. When an event is created for actions performed by a trusted resource, the event-attribute **Workflow ID** will be updated with the string specified in the Label of the trusted resource.

What is the best practice to enforce McAfee Application Control on Desktop System(s)?

1. Ensure that Application Control license is applied. (Check it in **Menu | Configuration | Server Settings | Solidcore**)
2. Ensure that Solidcore Agent is deployed on the system(s).
3. Create a **SC: Enable (Solidcore 5.1.0)** task, then select these Task settings:
   - Select **Application Control**.
   - Deselect **Perform Initial Scan to create whitelist**.
   - Deselect **Force Reboot with the task**.
   - Select Schedule status as **Enabled**.
   - Select Schedule type as **Run Immediately**.
   - Save the task.
4. Apply this task on the specified system(s), then send a wake-up agent call on the system(s).
5. Restart the system(s) as per convenience.
6. After restart, create a **SC: Initial Scan to create whitelist (Solidcore 5.1.0)** task, then select these Task settings:
   - Select Schedule status as **Enabled**.
   - Select Schedule type as **Run Immediately**.
   - Save the task.
7. Apply this task on the specified system(s), then send a wake-up agent call on the system(s).
8. After this task is run, User will get a pop-up on the client system stating, **McAfee Application Control Initial Scan task is complete and Application Control is enforced on the system now**.
9. Now, McAfee Application Control is enforced on the system