



Best Practices Guide

McAfee Application Control 6.2.0

For use with McAfee ePolicy Orchestrator

COPYRIGHT

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

1	Introduction	5
	About this guide	5
	How to use this guide	6
	Supported McAfee ePO versions	6
2	Installing and upgrading Application Control	7
	Determining database sizing	7
	Installing in cloned or imaged environments	7
	Installing with third-party tools	8
	Upgrading Application Control	9
3	Deploying Application Control in Observe mode	11
	Deployment strategy	11
	Deployment workflow	12
	Deployment recommendations and guidelines	13
4	Defining policies	17
	Before you begin	17
	Guidelines for default policies	18
	Creating policies	18
5	Managing inventory	21
	Recommendations for fetching inventory	21
	Best practices for managing applications	21
	Defining inventory filters	22
6	Maintaining your software	23
	Processing events	23
	Reports to run	24
7	Optimizing your software	25
	Recommended tasks	26
	Applying Windows updates	26
	Managing Solidcore client tasks	27
	Configuring alerts	27
	Configure an alert	27
	Monitoring server performance	28
	Using McAfee® Assurance Information Module	28
A	Frequently asked questions	29
	Index	31

1

Introduction

This document provides information about the McAfee® Application Control software so that you can easily and effectively use the software.

This document outlines some core recommendations for using Application Control. Use these recommendations to plan and maintain your software deployment.

Contents

- [About this guide](#)
- [How to use this guide](#)
- [Supported McAfee ePO versions](#)

About this guide

This document is one component of the Application Control software documentation set and supplements the information in the other documents.

This document frequently references other documents in the Application Control documentation set. The information contained in the other guides is not duplicated in this guide, but this guide points you to that information. For a list of the other documents in the set, see *How to use this guide?*.

Use the information in this document during these four stages.

Stage	Associated chapters
Installing and configuring your software	<ul style="list-style-type: none">• Database sizing• Installing and upgrading Application Control on page 3
Deploying your software	<ul style="list-style-type: none">• Deploying Application Control in Observe mode on page 3• Managing inventory on page 3
Managing and reporting on your environment	<ul style="list-style-type: none">• Maintaining your software on page 3• Reporting
Maintaining and optimizing your software	<ul style="list-style-type: none">• Optimizing your software on page 3• Frequently asked questions on page 3

How to use this guide

Here are a few prerequisites for using this document.

- Before using this guide, review *McAfee ePolicy Orchestrator Best Practices Guide* available [here](#). The guidelines and recommendations included in this guide are for use with McAfee ePO 5.0 and later. For more information about the recommended McAfee ePO versions, see *Supported McAfee ePO versions*.
- Use this document with other existing Application Control documents. This guide is not a comprehensive guide for all implementations. To fully understand the recommendations included in this guide, you must have a basic understanding of Application Control software. If you do not know or you need more information, see one of these documents:

Document	Configuration	Description
McAfee Change Control and McAfee Application Control 6.2.0 Product Guide	Managed	Information to help you configure, use, and maintain the product.
McAfee Change Control and McAfee Application Control 6.2.0 Help	Managed	Context-sensitive help for all product-specific interface pages and options in McAfee ePO.
McAfee Change Control and McAfee Application Control 6.2.0 Installation Guide	Managed	Information to help you install, upgrade, and uninstall the product.
McAfee Application Control 6.2.0 Product Guide	Standalone	Information to help you use and maintain the product.
McAfee Change Control and McAfee Application Control 6.2.0 Installation Guide	Standalone	Information to help you install, upgrade, and uninstall the product.
McAfee Application Control 6.2.0 Command Line Interface Guide	Standalone	All Application Control commands that are available when using the command line interface (CLI).

These guides are available on the [McAfee Support](#) page.

Supported McAfee ePO versions

This release of McAfee Application Control is compatible with these versions of McAfee ePO.

- McAfee ePO 5.0.1 — 5.1.3
- McAfee ePO 5.3.0



We don't guarantee that McAfee Application Control works with other versions of McAfee ePO.

2

Installing and upgrading Application Control

Successfully installing and upgrading the software is the first step in protecting your network environment.

Contents

- *Determining database sizing*
- *Installing in cloned or imaged environments*
- *Installing with third-party tools*
- *Upgrading Application Control*

Determining database sizing

Before you install the Application Control software, you must determine the database and hardware requirements for your enterprise.

Here are suggested sizing requirements for enterprises based on the number of nodes.

Enterprise size	Number of nodes	Suggested sizing requirements
Small	Less than 10,000 nodes	200 GB
Medium	Between 10,000 to 50,000 nodes	200 GB–1 TB
Large	More than 50,000 nodes	1–2 TB

For detailed sizing calculations and feature-specific sizing details, see the Application Control database sizing guide available in [KB83754](#). A few Application Control features are database heavy, so we recommend that you review the guide if you are running 50,000 to 100,000 nodes.

Installing in cloned or imaged environments

Application Control is compatible with cloned images.

Here are the high-level steps to successfully install the software in a cloned environment:

- 1 Build a master image.
 - a Install Application Control and place the system in Enabled mode. For details, see *McAfee Change Control and McAfee Application Control Installation Guide*.
 - b Place Application Control in Update mode. For details, see *McAfee Change Control and McAfee Application Control Product Guide*.
 - c Complete other changes, as required, before locking down the image.

d Delete the Agent GUID value from this registry key.

- **32-bit systems** — HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent
- **64-bit systems** — HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Associates\ePolicy Orchestrator\Agent



If you have McAfee Agent 5.0 installed, run this command on the system (to be used as the master image) to make sure the GUIDs are not duplicated.

```
maconfig -enforce -noguid
```

e Shut down the system.

2 Clone the required systems using the master image.

3 Perform any post-cloning operations or tasks to personalize the system. For example, you can configure that system for a specific user or install applications present on the system.

4 End Update mode and place all cloned systems in Enabled mode. For details, see *McAfee Change Control and McAfee Application Control Product Guide*.



If you choose to clone the system in Enabled mode (without placing the system in Update mode) and are using the Microsoft System Preparation Tool (Sysprep) utility, make sure that relevant updaters are identified and applied. The required rules for this utility are added to the **Operating System Imaging** rule group.

5 Manage the systems using the McAfee ePO console.

Installing with third-party tools

You can install, upgrade, or uninstall Application Control using third-party tools, such as Microsoft System Center Configuration Manager.

- Make sure that McAfee Agent is installed in Managed mode on each endpoint where you want to install Application Control.
- Make sure that when you configure third-party software to distribute and deploy the Application Control software, use the following command for silent installation on the Windows platform.

```
<installer-file> /s /v" /qn UNLICVER=1"
```

For details about command-line arguments, see *McAfee Change Control and McAfee Application Control Installation Guide* for standalone configuration.

Upgrading Application Control

Follow the recommendations to successfully upgrade the software.

- Upgrade the Solidcore extension before upgrading the Solidcore client.
- Review the Solidcore extension usage guidelines.

Guideline	Example
You cannot use an old version of the Solidcore extension with a new version of the Solidcore client.	Solidcore 6.2.0 client cannot be run with the Solidcore 6.1.2 extension.
You can use a new version of the Solidcore extension with an old version of the Solidcore client.	Solidcore 6.1.2 client can be run with the Solidcore 6.2.0 extension.

- Use these modes for upgrading the Solidcore client.

Operating system	Managed configuration	Standalone configuration
UNIX and Linux	Update mode	Update mode
Windows	Enabled mode	Update mode

3

Deploying Application Control in Observe mode

We recommend using Observe Mode to put systems through a full-functionality testing cycle that allows you to identify and review policy suggestions.

Observe mode offers two benefits.

- Helps you develop policies and determine rules that allow applications to run in Enabled mode
- Allows you to validate policies and check that the created rules allow authorized changes on endpoints



We recommend that you complete your initial deployment and testing in a non-production or test environment before deploying to the production environment.

Contents

- [Deployment strategy](#)
- [Deployment workflow](#)
- [Deployment recommendations and guidelines](#)

Deployment strategy

When using Observe mode, deploy Application Control in incremental batches of 10,000 endpoints. For example, if you have 50,000 endpoints in your enterprise, you must deploy in five batches of 10,000 endpoints. This approach allows you to effectively manage deployment and identify relevant rules. When a batch meets the required criteria (review the deployment workflow), change the mode to Enabled for this batch of endpoints. Also, place a new batch of endpoints in Observe mode. To ensure optimal performance, run only two batches simultaneously in Observe mode.

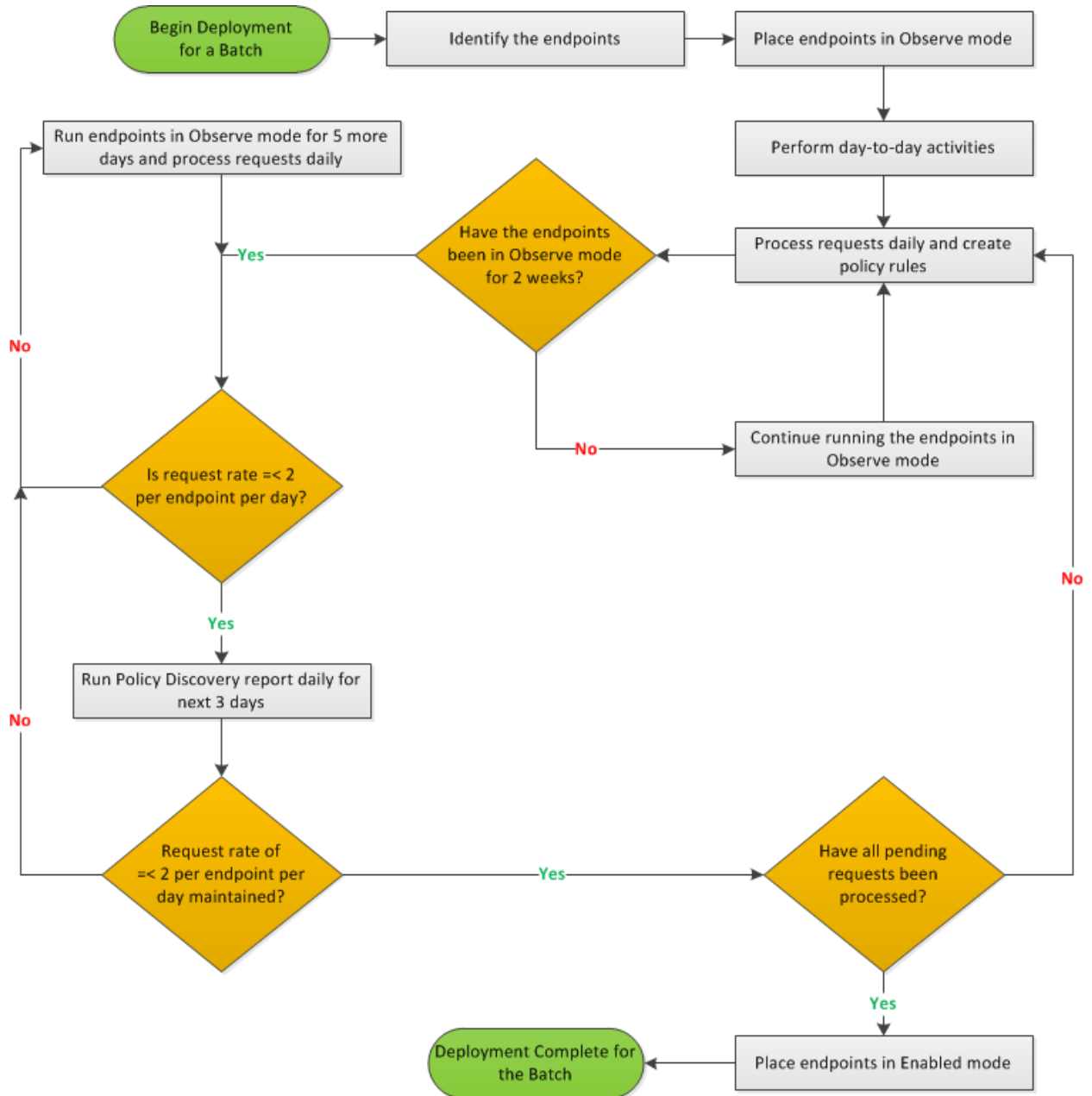


Before adding a new batch to Observe mode, verify that no upcoming planned activity, such as maintenance tasks or Windows update applications, will impact the request rate for the current batch in Observe mode.

Enterprise size	Number of nodes	Batch size	Suggested deployment period
Small	Less than 10,000	10,000 nodes per batch	2–3 weeks
Medium	Between 10,000 and 50,000		6–7 weeks
Large	More than 50,000		12–13 weeks


Deployment workflow


Here is the high-level workflow that you must follow for each batch while deploying Application Control.



Deployment recommendations and guidelines

Follow these recommendations and guidelines to successfully deploy in Observe mode.

Task	Recommendation	Description
Identify and place the endpoints in Observe mode to analyze product impact on the endpoints and identify and define the required rules.	Number of endpoints	For effective deployment in a large setup, begin with an initial batch of 10,000 endpoints.
	Selecting endpoints	<p>Select any 10,000 endpoints from your setup and place them in Observe mode. If your existing groups consist of similar endpoints, this allows you to analyze product impact on the endpoints, discover policy groups, and validate the policies to apply to each group.</p> <div>  <p>To reduce deployment time and quickly identify relevant rules, you can instead select or create a group that more accurately represents the enterprise. If you have multiple types of endpoints in your setup, create a subgroup within each existing group. For example, the HR subgroup within HR Department group. Use a combination of all subgroups, such as HR, Finance, Engineering, IT, and Admin to identify 10,000 endpoints for initial deployment. Because you select endpoints from varied groups, you effectively choose a set of endpoints with different operating systems, across different locations, used for different purposes and with varying usage. This type of selection effectively represents each type of system in the enterprise and allows you to quickly identify and define the required rules. After you identify the rules for this representative set, you can reduce deployment time by directly placing the remaining endpoints (within each group) in Enabled mode.</p> </div>
	Pre-deployment tasks	<p>We recommend that you complete these activities for the endpoints:</p> <ul style="list-style-type: none"> • Run an on-demand scan. • Patch applications and operating system. • Scan and pull applications in enterprise. • Run GetClean to classify the gray applications. • Block unwanted applications.
Place a batch in Observe mode by running the SC: Enable client task. For information about placing the endpoints in Observe mode, see <i>Place endpoints in Observe mode</i> in McAfee	Pulling inventory	We recommend that you pull inventory for endpoints while placing endpoints in Observe mode. Select the Pull Inventory checkbox when placing the endpoints in Observe mode.

Task	Recommendation	Description
<i>Change Control and McAfee Application Control Product Guide.</i>	Verifying placement	Run the Solidcore: Application Control Agent Status query to verify that selected endpoints are placed in Observe mode. For more information, see <i>McAfee Change Control and McAfee Application Control Product Guide</i> .
	Number of endpoints	At any time, there should be 10,000–20,000 endpoints running in Observe mode. At any point, only two batches can simultaneously run in Observe mode.
	Determining scan priority	<p>The scan priority determines the priority of the thread that is run to create the whitelist on the endpoints. For most scenarios, we recommend that you set the scan priority to Low.</p> <p>For systems that are in Production mode, use Low priority to make sure that there is minimal input and output impact. Also, you must use Low priority if the system cannot be restarted. If you can restart the system and you want the initial scan to be completed as soon as possible, select High priority.</p>
	Selecting activation option	Wherever possible, use Full Feature Activation to make sure that there is the highest level of security. We recommend using Full Feature Activation if the system does not have an alternate Memory Protection mechanism, such as the one provided by anti-virus or McAfee® Host Intrusion Prevention software.
Perform day-to-day operations and tasks to help generate corresponding requests.	<p>Based on the requests, you can define relevant rules required for your setup. Also, if you are using a specific tool for product updates or new deployments, we recommend that you use the tool in the initial two-week deployment period.</p> <p>If you are aware of activities or applications that run periodically, such as monthly payroll, make sure that the deployment period includes these activities.</p>	
<p>Review the requests received from endpoints and define relevant rules for each request to make sure that you configure Application Control correctly for your setup.</p> <p>For detailed information, see <i>McAfee Change Control and McAfee Application Control Product Guide</i>.</p>	Specifying processing ownership	The McAfee ePO administrator must process requests. Based on your setup, you might need to make sure that there is collaboration between global and site administrators.
	Determining frequency	<ul style="list-style-type: none"> • Process requests daily and define needed rules. • Run report weekly to gather request trend and summary. <div>  Failure to process requests regularly results in a build-up of requests that become progressively harder to manage. </div>

Task	Recommendation	Description
	Analyzing requests	We recommend that you process requests received from network paths. Then, process requests for updaters and installers on priority (for Software Installation activity type). If you trust the certificate associated with a request, define certificate-based rules for the request.
	Determining the action to take	<p>You can create custom rules or approve globally based on your choice and setup. Regardless of the action, the same rule is created.</p> <p>If the application is common to your setup, we recommend that you approve globally to add rules that apply to all endpoints in your enterprise. This allows for quick and simple processing. Or, create custom rules that you can add to a rule group and apply to selected endpoints.</p>
	Criteria for processing	Review each received request and check its prevalence and associated application. You can sort the view based on request prevalence. For more information, review the trust level and publisher for the application.
	Running reports	Review the Top 10 Pending Policy Discovery Requests and Systems with Most Pending Requests Generated in Observe Mode monitors on the Solidcore: Health Monitoring dashboard.

4

Defining policies

Based on your requirements, define policies to customize Application Control features.

Contents

- *Before you begin*
- *Guidelines for default policies*
- *Creating policies*

Before you begin

Consider your change management process before defining or developing policies.

Review how to change existing programs, tools, users, and processes. Here are some questions to consider.

- Do you have a formal change process?
- Can you easily differentiate between an authorized change and unauthorized change?
For example, you might not allow any changes to the systems during production hours.
- How do you make changes? Do you use manual updates, an automatic software, or an agent-based push mechanism?
- How homogeneous or not is your environment?
- Do you have any specific security requirements?

Guidelines for default policies

Here are some guidelines for Application Control default policies.

- Make sure that all default policies are applied to endpoints. The default policies are applied to the global root, such as the My Organization node in the System Tree and are inherited by all managed endpoints where Application Control is installed. When an endpoint connects to the McAfee ePO server, the policy applicable to the endpoint's operating system is activated. For more information about the available default policies, see *McAfee Change Control and McAfee Application Control Product Guide*.
- Do not change any existing default policy assignments. If you need to edit a default policy, contact McAfee Support.




Typically, for other managed products, you duplicate the available default policies to create custom policies, apply the custom policies, and do not apply default policies. However, when using Application Control, you must apply the default policies to make sure that McAfee product updates are handled. If needed, you can apply other custom policies in addition to the default policies.

For example, if you remove the McAfee Default policy assignments, the contained default rules to allow successful application of Windows updates are also removed from the endpoints. This can result in errors at the endpoint and many irrelevant events.

Creating policies

Follow these guidelines while creating policies in your enterprise.

- Review and understand the information available for multi-slot policies in the *McAfee ePolicy Orchestrator Product Guide*. You can define multi-slot policies that allow for effective policy use and improved policy organization. We recommend that you use the functionality to effectively define and manage rules for your enterprise. For example, instead of duplicating a default policy and adding more rules to it, we recommend that you create a new blank policy and add all custom rules to the policy. Then, apply the new policy in an extra slot with the default policy.
- All policies should use rule groups to manage policies. A rule group is a collection of rules. For more information about rule groups, see *McAfee Change Control and McAfee Application Control Product Guide*.
- Make sure that when creating rules, you follow these best practices.
 - Create rule groups so that they have a one-to-one mapping to applications or software. This allows you to add your application-specific rules to a rule group.
 - Define policies so that they have a one-to-one mapping to groups in System Tree on the McAfee ePO console.
 - Create a policy for a group of similar systems. For example, a specific policy for Domain Controllers and another for Oracle Servers. This allows you to add rules specific to a group or department to a policy (and apply the policy to the group).
 - Define granular policies rather than one large policy with many rules because you can apply multiple policies simultaneously to a system.
 - Analyze the impact of each policy type. Some rule or policies are more free or restrictive than others.
- Review and understand the relative degree of restriction each rule mechanism or method offers.

Updater method	Restriction level	Reason
Update mode	Low	Make emergency changes to systems.
Trusted users	Low	Allow technical support users to remotely log on to fix or administer systems that are geographically distant.
Publishers	Medium	Allow your code to update a system, regardless of how the code enters the system, or use signed code from a vendor. This method provides more flexibility than a hashed installer.
Authorized updaters	High	Update existing whitelisted applications based on a program that can make changes. This is a commonly used updating method.
Binary	High	<p>Allow or block execution of programs based on name or hash.</p> <ul style="list-style-type: none"> • Allow — Scripts created dynamically, such as by end of day or closing process on a kiosk for back-office reporting. • Block — Ban installed programs that should not run, such as iTunes. Or, reduce the risk exposure for a server by banning specific files, such as executables (net.exe or msconfig.exe). <p> This method is typically used for execution control and not for making changes to a system.</p>
Installers	High	Allow a non-whitelisted standalone executable that is identified by its hash to install applications on a protected system. This method is useful to distribute software based on approved applications.
Trusted directory	High	Allow print drivers, in-house applications, or startup scripts placed on a remote share to run. Although this method is easier to manage than hashes or certificates, it is not as secure.

5

Managing inventory

Follow these recommendations and best practices to successfully manage the inventory of endpoints in your enterprise.

Contents

- ▶ *Recommendations for fetching inventory*
- ▶ *Best practices for managing applications*
- ▶ *Defining inventory filters*

Recommendations for fetching inventory

Follow these recommendations to successfully fetch inventory from endpoints in your environment.

- Fetch inventory from 10,000 or fewer endpoints at a time.
- Fetch inventory once in two weeks or later to keep the inventory information updated.
- Use batches and follow a staggered approach to fetch inventory from more than 10,000 endpoints.



To keep the McAfee ePO repository from being overwhelmed, you can randomize your deployment or use tag-based deployment. For more information about using randomization or tagging, see the McAfee ePO documentation.

- Multiple methods are available to pull inventory immediately. For more information about the best approach, see *Guidelines for fetching inventory* in the *McAfee Change Control and McAfee Application Control Product Guide*.

Best practices for managing applications

Application Control is integrated with the McAfee® Global Threat Intelligence™ (McAfee GTI) file reputation service. Based on information fetched from McAfee GTI, the application and binary files in the inventory are sorted into Good, Bad, and Unclassified categories.

- Manage the Unclassified list for your enterprise to reduce the number of unknown binaries in your enterprise. The unclassified list typically includes all unknown applications, effectively creating the graylist for your enterprise. The goal is to achieve 95% classification by removing or reclassifying

unknown files and applications. Review and process the graylist routinely for your enterprise to keep it to a minimum size. By reclassifying files and applications, you minimize the risk to your enterprise.

- Run GetClean on endpoints with a high number of unclassified files. The GetClean utility submits files for analysis to McAfee Labs where they are checked and classified automatically and correctly.
- Reclassify internally developed, recognized, or trusted (from a reputed vendor or signed by a credible certificate) files that are currently in the unclassified list by changing the Enterprise Trust level of the file to Good. For more information, see *Manage the inventory* in the *McAfee Change Control and McAfee Application Control Product Guide*.
- Enable the automatic response **Bad Binary has been detected in Enterprise** from the **Menu | Automation | Automatic Responses** page.
For every bad binary file encountered in your environment, the software generates the **Bad File Found** event that is displayed on the **Menu | Reporting | Threat Event Log** page. To immediately receive a notification, the **Bad Binary has been detected in Enterprise** automatic response is preconfigured in Application Control. This automatic response is disabled by default. Make sure that the mail server for your enterprise is configured on the McAfee ePO console. For more information about how to set up an email server, see *McAfee ePolicy Orchestrator Product Guide*.
- Review the **Solidcore: Inventory** dashboard regularly to track and monitor inventory status for your environment.
- Designate a base image for your enterprise to create an approved repository of known applications, including internally developed, recognized, or trusted (from a reputed vendor) applications. This makes management of desktop systems easier by verifying the corporate applications. Here are high-level steps to follow:
 - 1 Validate and review all applications on a system.
 - 2 Run GetClean on the system to classify all unknown applications on the system.
 - 3 Set the base image on the approved system by using the **Mark Good** option.
For more information, see *Set the base image* in the *McAfee Change Control and McAfee Application Control Product Guide*.

Defining inventory filters

Tune advanced exclusion filters for inventory data to exclude non-meaningful files from the endpoints.

- Review the files contained in the `temp` folder and create rules for them.
- Exclude file names that contain special characters. For example, files names containing the \$ symbol.
- Exclude `.mui` files (Windows localized files).
- Delete the folder (GUID name) that contains extracted files when applying Windows updates. If you cannot delete the folder, create rules to filter these files.

6

Maintaining your software

After Application Control is deployed, you can perform various tasks to maintain the endpoints. Review these topics for details about maintenance tasks.

Contents

- *Processing events*
- *Reports to run*

Processing events

Create relevant rules to process events generated at endpoints. This helps control the flow of events from endpoints to the McAfee ePO server by gradually reducing the number of received events.

Create and apply relevant scenario-based rules to process events. If you receive:

- Numerous **Registry modified** or **File modified** events, review and fine-tune the filter rules for your enterprise. We recommend that you define rules to exclude specific files or registry entries based on the event type and file name or registry key.
- Multiple **Write Denied** events in your setup, review the events and define appropriate updater or filter rules. Updater rules are appropriate when the events are for a good file. Or, filter (AEF) rules might be relevant if the file is bad or unclassified.
- Multiple **Package Modification Prevented** events in your environment, review the events and define appropriate updaters.

- Numerous **Execution Denied** events in your environment, the file might not be whitelisted or is banned. The file is not whitelisted when it is added to an endpoint through a non-trusted method. If you receive **Execution Denied** events:
 - From a single host, run an anti-virus scan of the system, then resolidify the endpoint.
 - From multiple hosts for a file, review the file execution status on the Inventory page to verify if and why the file is banned. If the ban rule for the file is legitimate, we recommend that you add filter (AEF) rules for the file.

Reports to run

Based on the activity, review these monitors on the **Solidcore: Health Monitoring** dashboard.

Activity	Monitor
Data throttled or dropped	<p>Review the Number of Systems where Throttling Initiated in Last 7 Days monitor on the Health Monitoring dashboard.</p> <p>This monitor displays the number of systems on which Event, Inventory Updates (Diff), or Policy Discovery (Observations) throttling is initiated in last 7 days. The summary table sorts the data in descending order.</p>
Policy Discovery requests	<p>Review these monitors on the Health Monitoring dashboard.</p> <ul style="list-style-type: none"> • Top 10 Pending Policy Discovery Requests This monitor displays the top 10 pending policy discovery requests in your setup. The chart includes a bar for each object name and indicates the number of pending policy discovery requests for each object name. Click a bar on the chart to review detailed information. • Systems with Most Pending Requests Generated in Observe Mode This monitor displays the systems (running in Observe mode) that have the most pending Policy Discovery requests. The chart includes the system name and the number of pending policy discovery requests for each system. The summary table sorts the data in descending order.
Rogue host detection	<p>Review the Top 10 Events for 10 Most Noisy Systems in Last 7 days monitor on the Health Monitoring dashboard.</p> <p>This monitor displays the top 10 events generated on the 10 most noisy systems in last 7 days. The chart includes a bar for each system and indicates the number of events of the top 10 types for each system. Click a bar on the chart to review detailed information.</p>

For more information, see *McAfee Change Control and McAfee Application Control Product Guide*.

7

Optimizing your software


Optimization improves your experience about using the software and allows you to make the software work more efficiently for you. You can optimize the software by following these tasks.

Contents

- *Recommended tasks*
- *Applying Windows updates*
- *Managing Solidcore client tasks*
- *Configuring alerts*
- *Monitoring server performance*
- *Using McAfee® Assurance Information Module*

Recommended tasks

McAfee recommends that you perform certain tasks daily, weekly, and monthly to make sure that your systems are protected and Application Control is working efficiently.

Frequency	Recommended Tasks
Daily	<ul style="list-style-type: none"> Review the health monitoring dashboard. Review and manage policy discovery requests. Review the Policy Discovery page to make sure that Observation throttling isn't initiated. For detailed information, see <i>Throttle observations</i> in the <i>McAfee Change Control and McAfee Application Control Product Guide</i>.
Weekly	<ul style="list-style-type: none"> Review and manage events. Run the Solidcore: Non Compliant Solidcore Agents query to identify systems in the enterprise that are not compliant. Apply filters to suppress unneeded or irrelevant events. Optionally, pull inventory for systems where throttling is reset. Review and manage inventory for endpoints. For details, see <i>Managing inventory</i>.
Monthly	<ul style="list-style-type: none"> Application Control allows you to run queries that report on events data from multiple McAfee ePO databases. If you are using a distributed McAfee ePO environment, we recommend that you periodically roll up data for a consolidated report. To regularly roll up event data, you can schedule and run the Roll Up Data server task. When running the task, you can optionally purge data. In addition to collating data on a centralized server, you can drop events from other McAfee ePO servers. Use the Purge server task to purge data. See <i>McAfee Change Control and McAfee Application Control Product Guide</i> for instructions. Routinely purge data for inventory, events, client task logs, alerts, and observations. For more information, see <i>McAfee Change Control and McAfee Application Control Product Guide</i>. We recommend that you purge: <ul style="list-style-type: none"> Events older than 3 or 6 months (based on your auditing needs). Client task logs older than 30 days. <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  Based on your compliance requirements, you might choose to retain data older than three months. To understand implications of retaining older data on database requirements, see <i>Determining database sizing</i>. </div> <ul style="list-style-type: none"> Solidcore: Auto Purge Policy Discovery Requests server task is configured to automatically delete requests older than 3 months. This is an internal task that runs weekly by default. If needed, edit this task to change the configuration. Periodically delete Server Task Logs by running the Purge Server Task Log server task. We recommend that you delete data older than 6 months.

Applying Windows updates

Here are considerations to review before applying Windows updates in your enterprise.

- Make sure that the McAfee Default policy is applied to all endpoints.
- (Optional) Suppress unneeded or irrelevant events by applying filter rules.

Managing Solidcore client tasks

Here are a few best practices to manage Solidcore client tasks.

- Review the **Solidcore Client Task Log** page to check the client task status (success or failure).
- Before configuring a client task, make sure that the CLI on the endpoint is not recovered. Review the **Solidcore: Non Compliant Solidcore Agents** monitor in the Application Control dashboard to verify if CLI is recovered.

Configuring alerts

Configure alerts or automatic responses to receive notifications about important occurrences in your environment.

When to configure an alert?

- To receive a notification for every bad binary file encountered, enable the **Bad Binary has been detected in Enterprise** automatic response from the **Menu | Automation | Automatic Responses** page. For more information, see *Managing inventory*.
- To receive a notification when event or policy discovery request throttling is initiated for an endpoint in your environment, configure an alert for the **Data Throttled** event. Similarly, to receive a notification when the cache is full and old data is dropped from the event or request cache or throttling of inventory updates is initiated for an endpoint, configure an alert for the **Data Dropped** event.
- To receive a notification when data congestion exists for inventory items and observations at the McAfee ePO console, configure an alert for the **Data Congestion Detected** event.

Configure an alert

You can configure an alert or automatic response.

To learn how to configure an alert, view this [video](#). Alternatively, follow these steps to configure an automatic response.

Task

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

- 1 Select **Menu | Automation | Automatic Responses**.
- 2 Click **Actions | New Response**.
 - a Enter the alert name.
 - b Select the **Solidcore Events** group and **Client Events** event type.
 - c Select **Enabled**, then click **Next** to open the **Filter** page.
- 3 Select **Event** from the **Available Properties**.
- 4 Select **Data Throttled**, **Data Dropped**, or **Data Congestion Detected** from the **Value** list, then click **Next**.
- 5 Specify aggregation details, then click **Next** to open the **Actions** page.
- 6 Select **Send Email**, specify the email details, then click **Next** to open the **Summary** page.
- 7 Review the details, then click **Save**.

Monitoring server performance

Periodically check to see how your Application Control software is working so that you can avoid performance problems.

- Periodically make sure that your McAfee ePO server is working well. For more information about maintaining your McAfee ePO server, see *McAfee ePolicy Orchestrator Best Practices Guide*.
- Set up Windows Performance Monitor (PerfMon) to gather performance counters. Review the [Performance Monitor](#) page on the Microsoft Developer Network website for information about setting up PerfMon. Collect data for these counters to determine if any services are consuming resources:
 - McAfee ePO or database CPU consumption
 - McAfee ePO or database memory consumption
 - McAfee ePO or database disk input and output
 - Network latency between McAfee ePO and the database
- Determine parsing rates for the McAfee ePO parser. For more information, see *Finding and using Performance Monitor* in the *McAfee ePolicy Orchestrator Best Practices Guide*.
- Estimate and adjust the agent-server communication interval (ASCI) for your environment. For information about adjusting ASCI, see *McAfee ePolicy Orchestrator Best Practices Guide*.
- Maintain your SQL database to make sure that there is optimal performance. For information, see *McAfee ePolicy Orchestrator Best Practices Guide*.

Using McAfee® Assurance Information Module

McAfee continually strives to improve the product experience for customers. We recommend that you enable Assurance Information Module to help us collect information about how you use our products. This collected data helps us improve product features and customers' experience with the product.

Assurance Information Module collects the data from the client systems where McAfee products are installed, and that are managed by the McAfee ePO server. It helps improve McAfee products by collecting the following data:

- System environment (software and hardware details).
- Effectiveness of installed McAfee product features.
- McAfee product errors and related Microsoft Windows events.

We recommend that you install and enable the software and enforce the policy for the software. For detailed instructions, review the [Quick Start Guide](#) for Assurance Information Module.

A

Frequently asked questions

Here are answers to frequently asked questions.

Although I fetched inventory for an endpoint, the inventory is not displayed on the McAfee ePO console.

Inventory information might not be displayed on the McAfee ePO console in the following two scenarios:

- | | |
|--|---|
| Inventory information received for the endpoint is incomplete. | This can occur if you experience connectivity issues. To resolve this issue, check the connection and fetch the inventory for the endpoint again. |
| Inventory for an endpoint consists of many files. | To understand and resolve this issue, review KB79173 . |

Do we have any best practices for deploying Application Control in a Cluster Shared Volumes (CSV) environment?

Before deploying Application Control in a CSV environment, review the guidelines listed in [KB84258](#).

Index

A

- alerts [27](#)
- Application Control
 - default policies [18](#)
 - define policies [17](#)
 - deploy in Cluster Shared Volumes (CSV) environments [29](#)
 - determine database and hardware requirements [7](#)
 - fetch inventory [21](#)
 - install [7](#), [8](#)
 - install, cloned or imaged environment [7](#)
 - inventory management [21](#)
 - recommended tasks [26](#)
 - reports [24](#)
 - suggested sizing requirements [7](#)
 - supported McAfee ePO versions [6](#)
 - uninstall [8](#)
 - upgrade [7–9](#)
- automatic response
 - configure [27](#)
 - for bad binary [21](#)
 - when to create [27](#)

B

- best practices
 - default policies [18](#)
 - define advance exclusion filters, inventory [22](#)
 - deploy in Cluster Shared Volumes (CSV) environments [29](#)
 - enable McAfee Assurance Information Module [28](#)
 - fetch inventory [21](#)
 - how to use the guide [5](#)
 - inventory management [21](#)
 - manage applications [21](#)
 - manage Solidcore client tasks [27](#)
 - perform tasks [26](#)
 - policy, creation [18](#)
 - run reports [24](#)
 - upgrade [9](#)
- binaries
 - allow [18](#)
 - ban [18](#)
 - categories [21](#)

C

- cloned images [7](#)
- Cluster Shared Volumes (CSV) environment [29](#)

D

- dashboards
 - inventory status [21](#)
 - monitor health, enterprise [24](#)
 - verify, CLI status [27](#)

E

- enterprise
 - change management process [17](#)
 - considerations for defining policies [17](#)
 - guidelines to create policies [18](#)
 - manage applications [21](#)
 - manage inventory of endpoints [21](#)
 - monitor health, dashboard [24](#)
 - specific security requirements [17](#)
 - suggested sizing requirements [7](#)
- environment
 - apply Windows updates [26](#)
 - change management process [17](#)
 - cloned or imaged [7](#)
 - define advance exclusion filters, inventory [22](#)
 - fetch inventory for endpoints [21](#)
 - maintain endpoints [23](#)
 - monitor server performance [28](#)
 - run reports [24](#)
 - using third-party tools [8](#)
- ePolicy Orchestrator
 - adjust agent-server communication interval (ASCI) [28](#)
 - check database consumption [28](#)
 - check server performance [28](#)
 - fetch inventory for endpoints [21](#)
 - inventory information not displayed [29](#)
 - parsing rates [28](#)
 - supported versions [6](#)
- events
 - configure alerts [27](#)
 - configure automatic response [27](#)
 - for bad binary [21](#)
 - for data throttling [24](#)

events (*continued*)

process [23](#)

F

frequently asked questions [29](#)

G

guidelines

default policies [18](#)

define advance exclusion filters, inventory [22](#)

deploy in Cluster Shared Volumes (CSV) environment [29](#)

fetch inventory [21](#)

inventory management [21](#)

manage applications [21](#)

policy, creation [18](#)

upgrade [9](#)

I

installers [18](#)

inventory

categorization [21](#)

classification, binaries [21](#)

define advance exclusion filters [22](#)

incomplete information [29](#)

information not displayed [29](#)

manage [21](#)

monitor status [21](#)

recommendations to fetch [21](#)

M

managed configuration

upgrade UNIX and Linux [9](#)

upgrade Windows [9](#)

McAfee Assurance Information Module [28](#)

McAfee Global Threat Intelligence (McAfee GTI) [21](#)

P

policies

define [17](#)

policies (*continued*)

guidelines for default [18](#)

guidelines to create [18](#)

prerequisites for defining [17](#)

publishers [18](#)

R

recommendations

apply Windows updates [26](#)

daily tasks [26](#)

default policies [18](#)

define advance exclusion filters, inventory [22](#)

fetch inventory [21](#)

how to use the guide [5](#)

monthly tasks [26](#)

policy, creation [18](#)

weekly tasks [26](#)

S

Solidcore client, upgrade guidelines [9](#)

Solidcore extension, upgrade guidelines [9](#)

standalone configuration

upgrade UNIX and Linux [9](#)

upgrade Windows [9](#)

T

tools

GetClean [21](#)

how to change [17](#)

third party [8](#)

trusted directory [18](#)

trusted users [18](#)

U

Update mode [18](#)

updaters [18](#)

W

Windows Performance Monitor (PerfMon) [28](#)

