Best Practices Guide

McAfee Application Control 7.0.0

For use with McAfee ePolicy Orchestrator

Contents

Preface

This guide provides the information you need to work with your McAfee product.

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	**Note:** Additional information, like an alternate method of accessing an option.
	**Tip:** Suggestions and recommendations.

Important/Caution: Valuable advice to protect your computer system, software installation, network, business, or data.

Warning: Critical advice to prevent bodily harm when using a hardware product.

Purpose of this guide

This document provides information about the McAfee® Application Control software so that you can easily and effectively use the software. Also, the document outlines some core recommendations for using Application Control. Use these recommendations to plan and maintain your software deployment.

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 *Using this guide*.

Use the information in this document during these four stages.

Stage	Associated chapters
Installing and configuring your software	• Before you begin • Installing and upgrading Application Control
Deploying your software	• Deploying Application Control in Observe mode • Defining policies
Managing and reporting on your environment	• Managing inventory • Maintaining your software
Maintaining and optimizing your software	• Optimizing your software • Frequently asked questions

Using this guide

Here are a few prerequisites for using this document.

- 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 7.0.0 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 7.0.0 Installation Guide	Managed	Information to help you install, upgrade, and uninstall the product.
McAfee Application Control 7.0.0 Product Guide	Standalone	Information to help you use and maintain the product.
McAfee Change Control and McAfee Application Control 7.0.0 Installation Guide	Standalone	Information to help you install, upgrade, and uninstall the product.
McAfee Application Control 7.0.0 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.

Find product documentation

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

Task

1. Go to the **ServicePortal** at https://support.mcafee.com and click the **Knowledge Center** tab.
2. In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
3. Select a product and version, then click **Search** to display a list of documents.

1 Before you begin

Follow these security best practices to appropriately configure the protection available with Application Control and make your environments as safe as possible.

Contents

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.

Customizing McAfee default configuration

Use these guidelines to configure the default configuration.

1 **Evaluate customer environment.**

The McAfee default configuration is optimal for most enterprise security requirements. However, work with your Sales Engineer to evaluate the configuration based on your specific workflows, applications, and requirements.

2 **Build and test custom configuration.**

After completing environment analysis, build and test the configuration in a staging environment before rollout.

3 **Assess security against usability.**

Before creating the default configuration, evaluate the risk against the usability of the system and applications. Several features of Application Control restrict or allow users to run applications on the endpoint. For example, the self-approval feature allows users to run business-critical applications immediately instead of waiting for approval. This feature can be enabled on specific endpoints, as needed. For servers, we recommend that you disable this option.

Disabling unwanted applications and files

Review the installed applications on your managed endpoints and disable any unwanted applications, script interpreters, and binary files.

1 **Identify unwanted applications.**

   Application Control pulls the entire inventory of the system to the McAfee ePO console, which also provides a view of all installed applications on your managed endpoints. You must then evaluate all installed applications and identify any that are not required or allowed in the enterprise.

2 **Ban or remove the unwanted items.**

   You must either ban or remove all unneeded and unsafe inventory items, such as applications, script interpreters, or binary files. This action reduces the risk of threat in your environment. Application Control and McAfee ePO work together effectively to meet and enforce the security requirements in your environment.

For more information about managing inventory, see the *McAfee Change Control and McAfee Application Control Product Guide*.

For more information about inventory-related best practices, see *Managing inventory*.

Layering security protection

Adding different layers of security products provides optional protection and effectively secures your enterprise.

Layer	Description
Perimeter security	Network security for endpoints that are exposed to the external world to prevent unwanted attacks to the system. For example, you can deploy McAfee® Web Gateway and McAfee® Firewall Enterprise to protect endpoints.
Physical access security	Protecting endpoints from unauthorized physical access and offline access of the system drive. We recommend using encryption software.
Administrator access control	Protecting endpoints against unauthorized administrative access, using the principal of least privilege. Role Based Access Control and User Access Control allow access only to authorized users.
Endpoint security controls	Deploy endpoint controls based on the security requirements of your organization. Although, Application Control provides protection through multiple techniques, you might need additional products to ensure that endpoints are protected. Collaborate with your Sales Engineer for information and guidance on other security controls that can be used. Based on your requirements, you can choose to deploy products, such as McAfee® Email Protection, McAfee® Web Protection, McAfee® Endpoint Encryption, McAfee® Data Loss Prevention (McAfee DLP), and McAfee® Deep Defender™.

Applying updates and patches

Apply updates and security patches as soon as possible to keep the systems protected, especially critical security patches recommended by the operating system and application vendors.

The presence of Application Control can mitigate risks due to delay in applying updates. However, if the attack involves a critical system process, the mitigation for buffer overflow might result in Denial of Service (DoS) or make the system unusable.

Using recommended configuration

Using these guidelines to configure Application Control in your enterprise for optimal protection.

Feature	Description
Memory protection	Memory protection features (CASP, VASR, DEP) of Application Control protect against exploits that cause buffer overflows. Enable all memory protection features and consult with McAfee support team to evaluate the risk for any exception or bypass. For more information, see the *McAfee Change Control and McAfee Application Control Product Guide*.
Script authorization	A default script interpreter list comes with the product to whitelist script execution. Update the list based on the scripts and interpreters used or allowed in your organization. Script interpreters, such as PowerShell, Perl, PHP, and Java, and their supported extensions must be evaluated. Adding scripting languages can change the security posture of a system. Several factors must be considered before making decisions, such as: • Administrative capabilities • Degree of expected exposure to potential attack of a system • Level of approval to grant scripting access and administrative permissions • Ancillary access controls that might protect networks and systems Periodically review the list of allowed script interpreters because of changing security needs and circumstances. If any of the script interpreters are present but not in use, remove them from the whitelist and prevent them from executing. For more information, see the *McAfee Application Control Product Guide*. The needed commands can be issued from the McAfee ePO console using the **SC: Run Commands Client Task**.
Trusted update mechanisms	Application Control includes various methods to ensure proper functioning and updating of applications. We also provide a default list of trusted executables. We recommend you carefully update or change this list. For more information, see the *McAfee Change Control and McAfee Application Control Product Guide*.
Alerts and notifications	Constant monitoring is an integral part of protecting your systems. Application Control sends events to the McAfee ePO console whenever it prevents an unwanted operation. We recommend configuring the required alerts and email notifications to be aware of the activities at the endpoints. For more information, see *Configuring alerts*.

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

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 that 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 7.0.0 client cannot be run with the Solidcore 6.2.0 extension.
You can use a new version of the Solidcore extension with an old version of the Solidcore client.	Solidcore 6.2.0 client can be run with the Solidcore 7.0.0 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

Use 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

Complete your initial deployment and testing in a non-production or test environment before deploying to the production environment.

Contents

Deployment strategy

When using Observe mode, deploy Application Control in incremental batches of 10,000 endpoints.

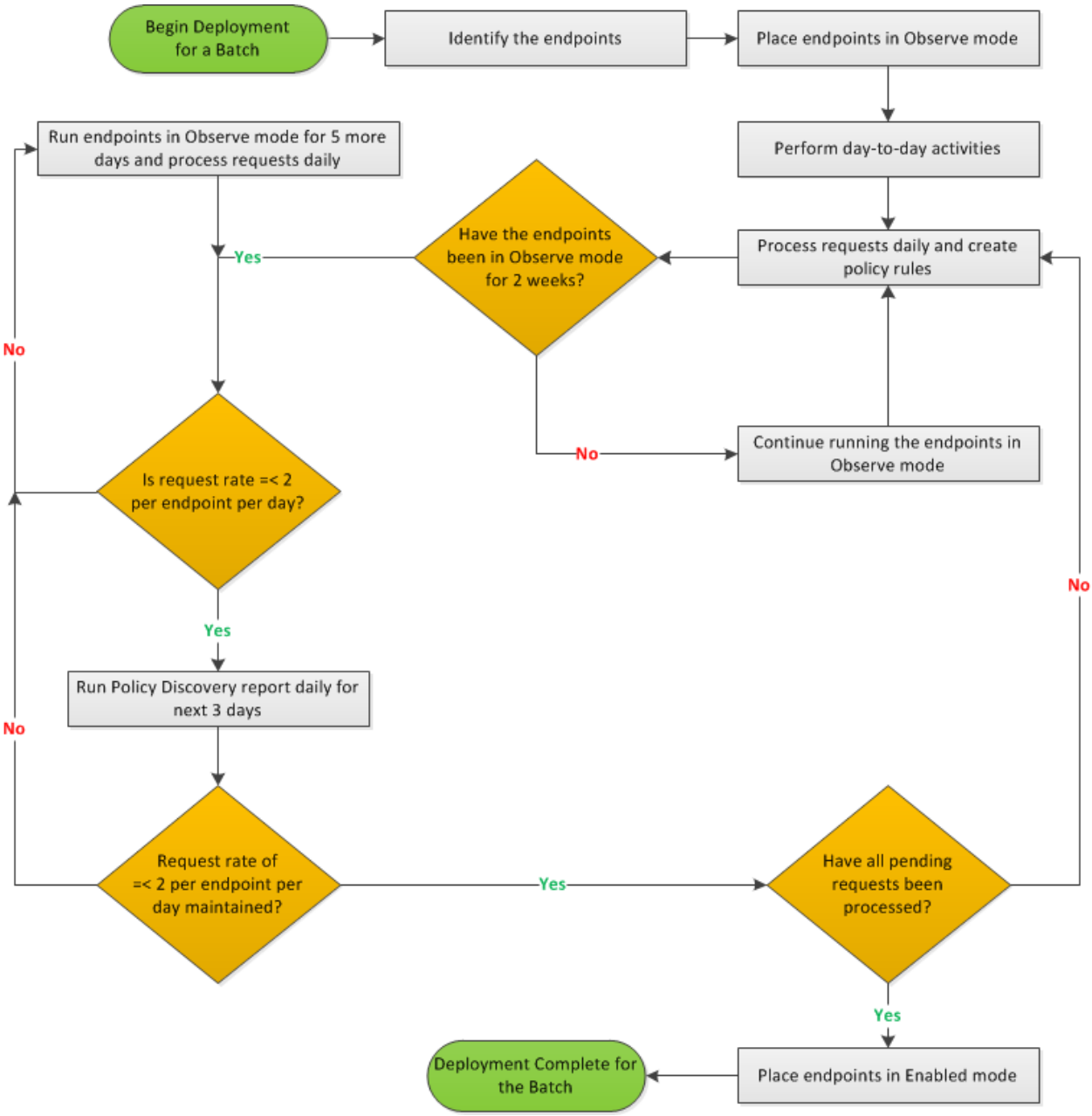
For example, if you have 50,000 endpoints in your enterprise, you must deploy in five batches of 100,00 endpoints. This approach allows you to effectively manage deployment and identify relevant rules. When a batch meets the required criteria (review the deployment workflow), change the mode to Enabled 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 when 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	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.  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.
	Pre-deployment tasks	Complete these activities for your endpoints: • 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 details, see *Place endpoints in Observe mode* in *McAfee Change Control and McAfee Application Control Product Guide*.	Pulling inventory	Pull an inventory for endpoints when placing endpoints in Observe mode. Select **Pull Inventory** when placing the endpoints in Observe mode.
	Verifying placement	Run the **Application Control Agent Status** query to verify that selected endpoints are placed in Observe mode. For more information, see *McAfee Change Control and McAfee Application Control Product Guide*.
	Number of endpoints	At any time, there should be 10,000–20,000 endpoints running in Observe mode. At any point, only 2 batches can simultaneously run in Observe mode.

Task	Recommendation	Description
	Determining scan priority	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**. 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.
	Selecting activation option	Wherever possible, use **Full Feature Activation** to ensure the highest level of security. Use **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.	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, use the tool in the initial two-week deployment period. If you are aware of activities or applications that run periodically, such as monthly payroll, make sure that the deployment period includes these activities.	
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. For detailed information, see *McAfee Change Control and McAfee Application Control Product Guide*.	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	• Process requests daily and define needed rules. • Run report weekly to gather request trend and summary. Failure to process requests regularly results in a build-up of requests that become progressively harder to manage.
	Analyzing requests	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	You can create custom rules or approve globally based on your choice and setup. Regardless of the action, the same rule is created. If the application is common to your setup, you can 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.
	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 reputation 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.

Task	Recommendation	Description		
	Rule identification	Rules are identified for requests based on event and activity type.		
		Event Type	**Activity Type**	**Rule type**
		File Write Denied	Binary Modification	Updater Process rule
		Installation Denied	Software Installation	Installers rule
		ActiveX installation Prevented	ActiveX Installation	Certificates rule
		NX Violation Detected	Memory Protection Violation	Exclusions rule
		Process Hijack Attempted	Memory Protection Violation	Exclusions rule
		VASR Violation Detected	Memory Protection Violation	Exclusions rule
		Execution Denied	Software Installation	Installer rule
		Execution Denied	Application Execution	Binary rule to allow execution or Allow locally to add to whitelist
		File Write Denied	Binary Addition	Updater rule

4 Defining policies

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

Contents

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 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 when 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 polices that allow for effective policy use and improved policy organization. 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, 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.

Item	Best practices
Rule groups	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.
Policies	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.
Users	Low	Allow technical support users to remotely log on to fix or administer systems that are geographically distant.
Certificates	Medium	Allow your application to update a system, regardless of how the application enters the system, or use signed application from a vendor. This method provides more flexibility than a hashed installer.
Updater Processes	High	Update existing whitelisted applications based on a program that can make changes. This is a commonly used updating method.
Binaries	High	Allow or block execution of programs based on name or hash. • 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). This method is typically used for execution control and not for making changes to a system.
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.
Directories	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

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 can work with a reputation source, such as TIE server or McAfee® Global Threat Intelligence™ (McAfee GTI) file reputation service to fetch reputation information for files and certificates.

Based on information fetched from the reputation source, the application and binary files in the inventory are sorted into trusted, malicious, and unknown categories.

- Manage the **Unclassified Apps** for your enterprise to reduce the number of unknown applications in your enterprise. This 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 unknown 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 unknown list.
    - If the TIE server is configured in your server, reset the files reputation on the **TIE Reputations** page. When resetting the reputation for a signed file, you must set the reputation for the file's certificate to Unknown to allow the overridden reputation to be used. For more information, see the *McAfee Threat Intelligence Exchange Product Guide* for your version of the software.
    - If the TIE server is unavailable, change the Enterprise Trust level or Reputation by Application Control 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 File Found in Enterprise** from the **Menu** | **Automation** | **Automatic Responses** page.

  For Known Malicious and Might be Malicious files or certificates encountered in your environment, the software generates **Malicious File Found** events that are displayed on the **Menu** | **Reporting** | **Threat Event Log** page. The **Bad File Found in Enterprise** automatic response is preconfigured in Application Control but 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 Trusted** 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

Using reputation sources

By default, Application Control is configured to work with the TIE server or McAfee® Global Threat Intelligence™ (McAfee GTI) file reputation service to fetch reputation information.

Here is how the reputation information is helpful.

On the McAfee ePO console	• Helps make quick and informed decisions for binary files and certificates in your enterprise. • Reduces the administrators effort and allows them to quickly define policies for the enterprise on the McAfee ePO server.
On the endpoints	• Allows for reputation-based execution permitting only trusted and authorized files to execute. • Determines whether to allow or ban execution for a file based on its reputation and reputation of all certificates associated with the file.

The settings configured for your enterprise determine the reputation values that are allowed or banned.

- **Trusted files** — If the reputation for a binary file or its associated certificate is trusted, the file is allowed to run, unless blocked by a predefined ban rule.
- **Malicious files** — If the reputation for a binary file or its associated certificate is malicious, the binary is not allowed to execute. You can choose to ban only Known Malicious, Most Likely Malicious, Might be Malicious files, or all such files.
- **Unknown** — If the reputation for a binary file or its associated certificate is unknown, reputation is not used to determine execution. Application Control performs multiple other checks to determine whether to allow or block the file. For more information, see *Checks that Application Control runs for a file*.

Regardless of the file's reputation, if a ban by name or SHA-1 rule exists for a binary file, its execution is banned.

For more information, see *File and certificate reputation* in the *McAfee Change Control and McAfee Application Control Product Guide*.

Best practices for configuring reputation sources

- Review the default settings on the **Reputation** tab of the **Application Control Options (Windows)** policy. The default settings work for most enterprises. If needed, you can tweak the settings for your enterprise.
- If Internet access is not available to endpoints in your enterprise, we recommend that you deselect the **Use McAfee Global Threat Intelligence (McAfee GTI)** option in the **Application Control Options (Windows)** policy. This allows optimal performance for endpoints in Air Gap environments.

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 finetune the filter rules for your enterprise. 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 malicious or unknown.
- Multiple **Installation Denied** 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, 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	Review the **Number of Systems where Throttling Initiated in Last 7 Days** monitor on the Health Monitoring dashboard. 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.
Policy Discovery requests	Review these monitors on the Health Monitoring dashboard. • **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	Review the **Top 10 Events for 10 Most Noisy Systems in Last 7 days** monitor on the Health Monitoring dashboard. 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.

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

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	• 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 *Throttle observations* in the *McAfee Change Control and McAfee Application Control Product Guide*.
Weekly	• Review and manage events. • Run the **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 *Managing inventory*.

Monthly	• 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, 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 **Solidcore: Purge** server task to purge data. See *McAfee Change Control and McAfee Application Control Product Guide* for instructions.
	• Routinely purge data for inventory, events, client task logs, alerts, and observations. For more information, see *McAfee Change Control and McAfee Application Control Product Guide*. We recommend that you purge:
	  • Events older than 3 or 6 months (based on your auditing needs).
	  • Client task logs older than 30 days.
	  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 *Determining database sizing*.
	• **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. 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 **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 notifications for Known Malicious and Might be Malicious files or certificates encountered in your setup, enable the **Bad File Found 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 details about product features, usage, and best practices, click **?** or **Help**.

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 **SC: Event Display Name** 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.

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