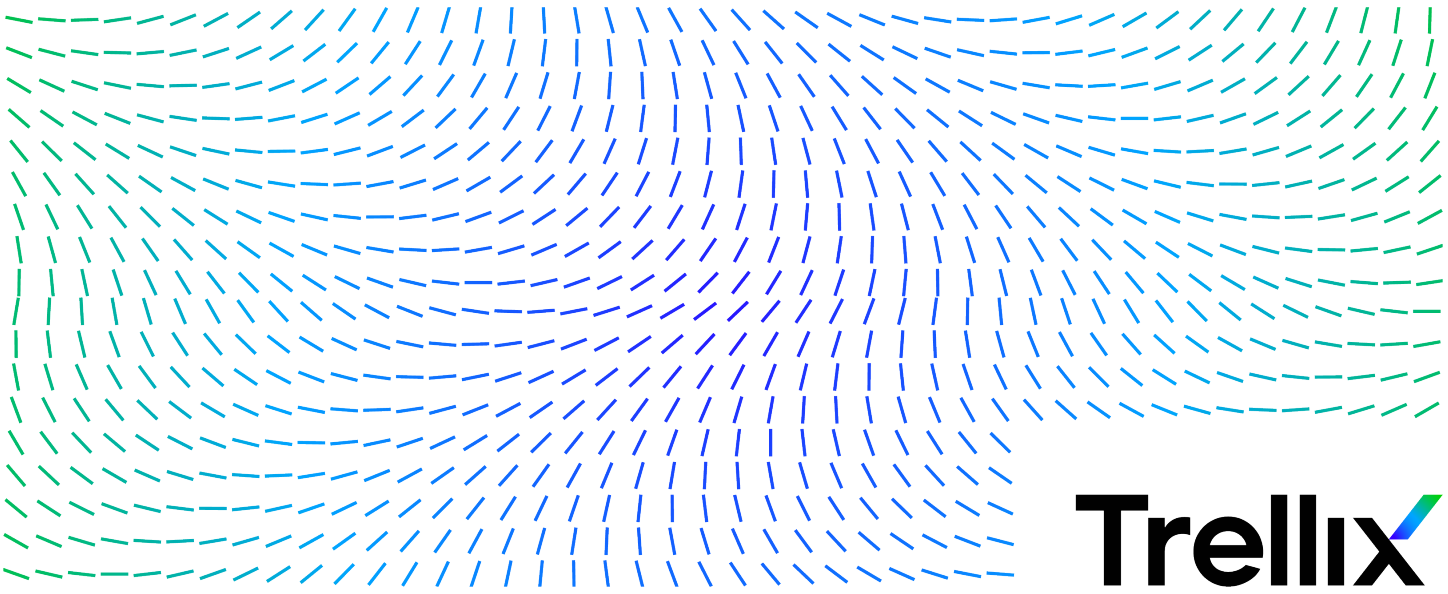
McAfee Application and Change Control 8.3.x - Windows Product Guide



Contents

Product overview. 9

Overview. 9

Key features. 9

How Application Control works in a managed environment. 11

How Change Control works in a managed environment. 12

How the software works in an unmanaged environment. 13

Using the software. 14

Determining database sizing. 14

Staffing considerations. 14

Software modes. 15

Enable the software in a managed environment. 17

Enable the software in an unmanaged environment. 18

Using recommended configuration. 19

File and certificate reputation. 20

Reputation sources and communication. 20

Reputation values received from sources. 21

McAfee ePO workflow. 23

Endpoint workflow. 23

How reputation is computed. 24

Change file reputation. 25

Memory-protection techniques. 26

Configuring CASP. 28

Configuring bypassing rules for NX. 28

Configuring Forced DLL Relocation. 29

Using checksum values. 30

Authorize binaries. 31

Ban binaries. 31

Remove checksum rules. 32

Authorizing and banning execution of binaries by name. 32

View authorized and banned binaries. 33

Remove authorized and banned rules. 33

Using trusted directories. 34

Manage trusted directories in a managed environment. 34

Manage trusted directories in an unmanaged environment. 34

Specify directory paths. 35

Using rule groups in a managed environment. 36
What are rule groups?. 36
Manage rule groups and policies. 37
Using monitoring rules. 50
What can you monitor?. 50
Framework to define monitoring rules. 52
Create or change monitoring rules. 54
Create monitoring policies. 55
Configure settings for tracking content changes. 55
Track content changes. 57
Manage file versions. 58
Using protection rules. 59
What are protection rules?. 59
System variables. 59
Path considerations. 60
Apply protection rules. 61
Create a protection policy. 62
Enable read protection. 63
Using execution control rules in a standalone environment. 63
Defining attribute-based rules for file execution. 63
Add attribute-based rules. 65
Remove attribute-based rule. 66
View attribute-based rules. 68
Using certificates with McAfee ePO. 68
What are certificates?. 68
Add certificates with McAfee ePO. 69
Search for a certificate. 70
Verify assignments for a certificate. 70
Add a certificate to a policy or rule group. 71
Using certificates in a standalone environment. 71
Add certificates in a standalone environment. 71
Extracting certificates. 73
View certificates. 74
Remove certificates. 74
Using updaters. 76
What are updaters?. 76
Script as Updater feature. 76
Manage updaters in a managed environment. 79
Manage updaters in an unmanaged environment. 80
Discover potential updaters. 82

Configure processes and certificates. . . . 83
Using interpreters. . . . 84
Configure interpreters. . . . 84
Using installers in a managed environment. . . . 86
What are installers?. . . . 86
Add an installer in a managed environment. . . . 88
Add an installer to a policy or rule group. . . . 89
Verify assignments for an installer. . . . 89
Configure Package Control. . . . 89
Using events. . . . 90
What are events?. . . . 90
View and manage events in a managed environment. . . . 91
Processing events. . . . 92
List of events in a managed environment. . . . 92
Customize end-user notifications in a managed environment. . . . 105
View and manage events in an unmanaged environment. . . . 106
List of events in an unmanaged environment. . . . 106
Managing the inventory with McAfee ePO. . . . 113
What is inventory. . . . 113
Configure inventory updates. . . . 114
Configure settings for fetching the inventory. . . . 114
Fetch the inventory. . . . 115
Export SHA-1s. . . . 115
Run the Offline GTI tool. . . . 116
Import the GTI result file. . . . 117
Set enterprise reputation for files and certificates. . . . 118
Review the inventory. . . . 118
Manage the inventory. . . . 119
Define filters for inventory data. . . . 120
Create an approved repository of known applications. . . . 120
Compare the inventory. . . . 121
Matching applications using Common Platform Enumeration (CPE). . . . 122
Using Common Platform Enumeration (CPE). . . . 122
Import the CPE dictionary. . . . 123
Create a server task for matching applications. . . . 123
Run a server task to match applications. . . . 124
Using dashboards and queries with McAfee ePO. . . . 125
Dashboards. . . . 125
Available queries. . . . 125
View queries. . . . 128

Using trusted users. 128
What are trusted users?. 128
Add trusted users with McAfee ePO. 129
Add trusted users in a standalone environment. 129
List trusted users. 130
Remove trusted users. 131
Using trusted local group. 131
Trusted local group. 131
Write protection and read protection. 131
What is write protection?. 131
Apply write protection. 132
Exclude components from write protection. 133
View write-protected components. 134
Remove write protection. 134
What is read protection?. 134
Apply read protection. 135
Exclude specific components from read protection. 135
View read-protected components. 136
Remove read protection. 136
Optimizing your software. 136
Recommended tasks. 136
Applying Windows updates. 137
Monitoring server performance. 140
Participating in the MACC Product Improvement Program. 140
Using the software in virtual environment. 141
Using the software with third-party tools. 143
Upgrading the software. 143
McAfee Secure Policy. 145
Client Configuration for MACC. 146

Using Application Control in Observe mode. 151
What is Observe mode?. 151
Deployment strategy. 154
Deployment workflow. 154
Deployment recommendations and guidelines. 155
Configure processes and certificates. 158
Place endpoints in Observe mode. 158
Policy discovery permissions. 159
Allow non-global administrators to manage enterprise-wide requests. 160
Managing requests. 160

Review requests. . . . 160
Allow a file on all endpoints. . . . 162
Allow a file by certificate. . . . 162
Allow network files on all endpoints. . . . 163
Ban by SHA-1 or SHA-256 on all endpoints. . . . 163
Define rules for specific endpoints. . . . 164
Allow by adding to whitelist for specific endpoints. . . . 165
Define bypass rules for all endpoints. . . . 166
Change file reputation. . . . 166
Delete requests. . . . 166
Define filters for observations and events. . . . 167
Define filters for user comments. . . . 167
Throttling observations. . . . 168
Define the threshold value for throttling. . . . 168
Review filter rules for throttling. . . . 169
Restart observation generation for throttling. . . . 169
Exit Observe mode. . . . 169

Using Application Control in Inventory mode. . . . 171
What is Inventory mode?. . . . 171
Place endpoints in Inventory mode. . . . 171
Exit Inventory mode. . . . 172
Inventory mode events in McAfee ePO. . . . 172

Self-approval requests. . . . 174
What is self-approval?. . . . 174
Enable self-approval on endpoints. . . . 174
Self-approval dialog box. . . . 175
Policy discovery permissions. . . . 176
Allow non-global administrators to manage enterprise-wide requests. . . . 176
Review approval requests. . . . 177
Process approval requests. . . . 178
Allow a file on all endpoints. . . . 178
Allow a file by certificate. . . . 179
Ban by SHA-1 or SHA-256 on all endpoints. . . . 179
Define rules for specific endpoints. . . . 180
Allow by adding to whitelist for specific endpoints. . . . 181
Change file reputation. . . . 182
Delete requests. . . . 182

Maintaining your system in a managed environment. 183
Monitoring enterprise health. 183
Reports to run. 184
Review congestion status and trend. 184
Why to configure notifications?. 185
Configure notifications. 186
Making emergency changes. 186
Switch to Update mode. 186
Exit Update mode. 187
Administering throttling for your enterprise. 187
Set up throttling. 188
Configure throttling values. 188
Manage throttling. 189
Identify endpoints where throttling is initiated. 190
Review throttling status. 190
Process data where throttling is initiated. 191
Configure CLI breach notifications. 192
Change the CLI password. 193
Collect debug information. 193
Place the endpoints in Disabled mode. 194
Sending McAfee GTI feedback. 194
Configure server tasks. 195
Purge reporting data. 196
Configuring Case sensitivity on ePO Managed Solidcore Client. 196

Maintaining your system in an unmanaged environment. 198
View product status and version. 198
Manage the whitelist. 199
Configure whitelist thread priority. 199
Add and remove components from the whitelist. 200
View whitelisted files. 201
Check and update the status of whitelisted components. 202
Review product features. 203
Enable or disable features. 205
Package Control feature. 206
Configure Package Control. 207
Making emergency changes. 208
Switch to Update mode. 208
Exit Update mode. 209
Enable or disable password protection. 209

Review changes using events. . . . 210
Configure event sinks. . . . 210
Set the event cache size. . . . 211
Define the limits for the event cache. . . . 211
View events. . . . 212
Configuring log files. . . . 212
Switch to Disabled mode. . . . 213
Configure Case sensitivity on standalone Solidcore Client. . . . 214

Fine-tuning your configuration. . . . 215
Configure a syslog server. . . . 215

Using the command-line interface. . . . 217
List of Commands for Application Control and Change Control. . . . 217
Command short forms. . . . 223
Argument details. . . . 224

Troubleshooting. . . . 234
Troubleshooting and logs. . . . 234
Troubleshooting Inventory issues. . . . 235

Best practices for using the software. . . . 238
Best practices for managing applications. . . . 238
Application Control rules (Windows). . . . 239
Tips and tricks for client deployments. . . . 240
Managing Solidcore client tasks. . . . 241
Tips and tricks for server performance. . . . 241
Policy Discovery request best practices. . . . 244

Frequently asked questions. . . . 245

Product overview

Overview

McAfee® Application Control blocks unauthorized executables on servers, corporate desktops, and fixed-function devices. McAfee® Change Control monitors and prevents changes to the file system.

Important

You can deploy Application Control and Change Control in a managed McAfee® ePolicy Orchestrator® (McAfee® ePO™) environment or in an unmanaged environment, also called standalone, or self-managed.

Application Control uses dynamic whitelisting to guarantee that only trusted applications run on servers, devices, and desktops. It eliminates the need for IT administrators to manually maintain lists of approved applications. It guarantees protection without impacting productivity.

With Application Control, you can:

- Prevent malicious, untrusted, or unwanted software from being executed.
- Automatically identify trusted software and grant it authorization to run.
- Block users from introducing software that poses a risk to your company.

Change Control allows you to write-protect and read-protect critical files from unauthorized tampering. You can also define trusted programs or users to allow updates to protected files and registry keys. A change is allowed only if it's applied according to the software policies.

With Change Control, you can:

- Detect, track, and validate changes in real time.
- Prevent changes using protection rules.
- Enforce approved change policies.

Key features

Application Control protects your organization against malware attacks before they occur by proactively controlling the applications that run on your devices. Change Control blocks change activities in server environments to prevent security breaches and data loss, and lowers the impact of outages.

Dynamic whitelisting

You can manage your whitelist in a secure and dynamic way. IT administrators don't need to manually maintain lists of approved applications. Application Control groups executables (binaries, libraries, and drivers) across your company.

You can easily search for useful information such as:

- Applications added this week
- Uncertified binaries
- Systems running outdated versions
- Files with unknown reputations (in a McAfee ePO managed environment only)

Protection against threats

Application Control extends coverage to executable files, libraries, drivers, Java applications, ActiveX controls, and scripts for greater control over application components. It enforces control on connected or disconnected servers, virtual machines, endpoints, and fixed devices, such as kiosks and point-of-sale (POS) terminals. It also locks down protected endpoints against threats and unwanted changes, with no file system scanning or other periodic activity that might impact system performance.

Advanced memory protection

Application Control offers multiple memory-protection techniques to prevent zero-day attacks. Memory-protection techniques provide extra protection over the protection from native Windows features or signature-based buffer overflow protection products. These techniques also prevent whitelisted applications from being exploited by memory buffer overflow attacks on Windows 32-bit and 64-bit systems.

Knowledge acquisition

You can switch to Observe mode to discover policies for dynamic desktop environments without enforcing a whitelist lockdown. This mode helps you deploy the software in pre-production environments without affecting the operation of existing applications.

Note

This feature is available only in a McAfee ePO managed environment.

Reputation-based execution

Application Control integrates with a reputation source to receive reputation information for files and certificates. Based on the reputation received from one of these sources, Application Control allows or bans the execution and software installation.

Note

This feature is available only in a McAfee ePO managed environment.

Centralized management

Application Control integrates with McAfee ePO software for consolidated and centralized management, and a global view of enterprise security from a single console.

Note

This feature is available only in a McAfee ePO managed environment.

Write protection

Use write protection rules to prevent users from creating and changing files, directories, and registry keys. Write-protecting a file makes it read-only.

Read protection

Read protection rules prevent users from reading the content of specified files, directories, and volumes. If a directory or volume is read-protected, all files in that directory or volume are also read-protected. Subdirectories inherit read protection rules.

Real-time monitoring

Change Control monitors file and registry changes in real time, eliminating need for multiple scans on endpoints to identify change violations.

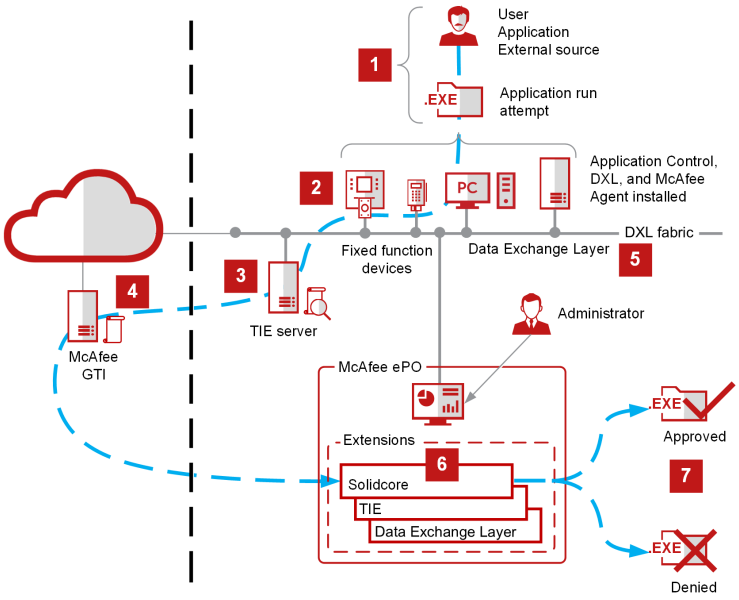
Content change tracking

Change Control tracks content and attribute changes for files and includes special alerting mechanisms to instantly notify you of critical changes.

How Application Control works in a managed environment

Application Control creates a whitelist of all authorized executable files. When you attempt to run an executable file that isn't whitelisted, Application Control checks the reputation of the file and allows or blocks its execution.

1. A user or application tries to execute a file on a managed endpoint where Application Control and McAfee® Agent are installed.
2. Application Control checks the reputation of the file and allows or blocks its execution.
3. Application Control communicates with the McAfee® Threat Intelligence Exchange (TIE) servers to receive reputation information for the file and any associated certificates. Based on this information, Application Control allows or blocks the file execution.
4. If the TIE server is unavailable, Application Control communicates with the McAfee® Global Threat Intelligence™ (McAfee GTI) server to fetch the reputation of the file.
5. McAfee® Data Exchange Layer (DXL) provides the framework for communication between Application Control and TIE or McAfee GTI, so products can share threat information.
6. The administrator manages all endpoints, deploys policies, creates rules, adds certificates, manages the inventory, monitors activities, and approves requests.
7. Information about the attempt to run the application is sent to the McAfee ePO server, where it appears in a dashboard, report, or log.



How Change Control works in a managed environment

Change Control prevents unauthorized changes to critical system files, directories, and configurations while implementing new policies and compliance measures.

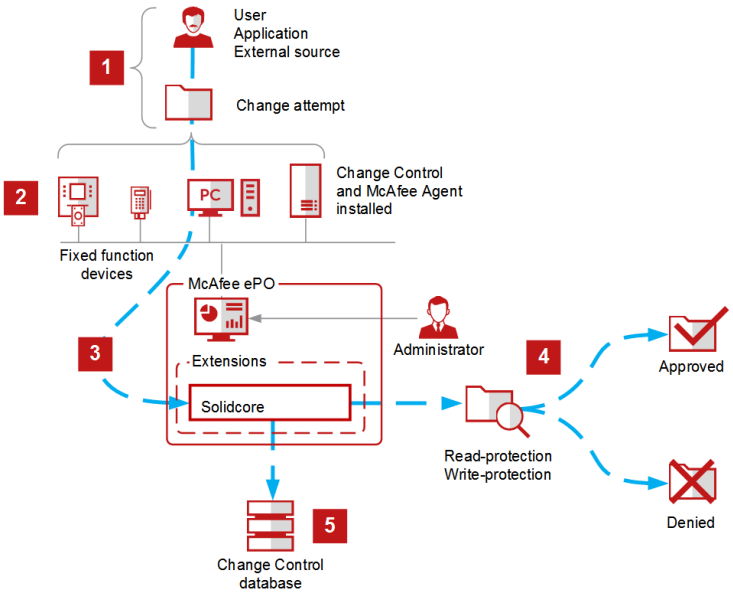
It tracks changes to files and registry keys in real time and it identifies who made changes to which files.

1. A system user tries to change a file or registry on a managed system where Change Control and McAfee Agent are installed.
2. The Change Control software recognizes the attempted change and uses the McAfee Agent to send a Change Control event to McAfee ePO.
3. Change Control analyzes the rules and policies enforced on the endpoint, and allows or blocks the change.

   Note

   The administrator manages these rules and policies through McAfee ePO.

4. Read protection or write protection is enforced and the user's change attempt is approved or denied.
5. The Change Control database logs the file change attempt and local user information.



How the software works in an unmanaged environment

Application Control creates a whitelist of all authorized executable files and blocks the execution of any program that isn't whitelisted. Change Control monitors and prevents changes to the file system and it write-protects and read-protects critical files from unauthorized tampering.

The whitelist details authorized files and determines trusted or known files. In Enabled mode, only files that are present in the whitelist are allowed to run. All files in the whitelist are protected and can't be changed or deleted.

Application Control stores the whitelist for each drive or volume at the following location:

- <drive>\Solidcore\scinv

Here is a list of the types of files included in the whitelist.

- Binary executables (.exe, .sys, and .dll files)
- Script files (such as .bat, .cmd, and .vbs files)

Note

When the whitelist is created for Windows, Application Control doesn't include system-specific files that are protected by the operating system. For example, pagefile.sys and hiberfil.sys.

When you execute a file, Application Control compares the checksum and path of the binary with the checksum and path stored in the whitelist and allows the execution only if the checksum value and path match.

Using the software

Determining database sizing

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

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

Enterprise size	Number of nodes	Suggested database sizing
Small	Less than 10,000 nodes	200 GB
Medium	Between 10,000–50,000 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.

Staffing considerations

With additional administrative overhead per endpoint in mind, adding systems to the scope of the project and hardening them needs dedicated staff to manage the product.

This table shows the recommended staffing during the sustainment phase of the project. This staffing suggestion considers that further deployments might need additional staffing and moderate configuration changes. Major changes such as workstations might need more staffing. Minor changes such as ATM's or manufacturing might need less staffing.

Number of endpoints	% of time dedicated	Number of staff
Up to 1000	30	1 (2 if an alternate is needed)
1000–5000	50	2
5000–10000	100	2

Number of endpoints	% of time dedicated	Number of staff
10000 and above	100	Minimum of 3

With staffing considerations in mind, McAfee recommends only protecting business critical applications such as domain controllers, high revenue generating servers, and any other critical systems defined by your organization.

Software modes

Application Control and Change Control can operate in four different modes. Each mode is different in principle and usage.

Enabled mode in an unmanaged environment

This mode indicates that only whitelisted applications and files are allowed to run. Execution of unauthorized software, such as a virus or spyware, is prevented. In Enabled mode, Application Control protects files in the whitelist from unauthorized change. After the initial whitelist is created, switch to Enabled mode which makes sure that no unauthorized changes are allowed.

Enabled mode in a managed environment

This mode indicates that Application Control is running and protection is enabled. Enabled mode supports reputation-based execution. When you execute a file, Application Control fetches its reputation and that of all certificates associated with the file to determine whether to allow or ban the file execution. Application Control works with TIE Server and McAfee GTI to fetch reputation information for a file.

These are the available reputation values:

- **Trusted files**— If the reputation is trusted, the file is allowed to run, unless it is blocked by a predefined ban rule. No observation or event is generated.
- **Malicious files**— If the reputation is malicious, the file isn't allowed to run. An event is generated and displayed on the **Solidcore Events** page. You can configure the reputation values that are banned in your endpoints. You can ban Known Malicious, Most Likely Malicious, Might be Malicious files, or all malicious files.
- **Unknown**— If the reputation is unknown, reputation values aren't used to determine execution. Instead, Application Control performs other checks to determine whether to allow or block the file.

In Enabled mode, Application Control:

- Allows only trusted (based on reputation) or authorized (based on rules) applications and installers to run on servers and endpoints.
- Protects against memory-based attacks and application tampering.

Regardless of the file's reputation, if a ban by name, SHA-1, or SHA-256 rule exists for an executable file, its execution is banned. No corresponding observation is generated. A corresponding event is generated and displayed on the **Solidcore Events** page.

Observe mode

This mode indicates that Application Control is running but it only monitors and logs observations. The application doesn't prevent any execution or changes made to the endpoints. Instead, it monitors execution activities and compares them with the local inventory and predefined rules.

Observe mode also supports reputation-based execution. When you execute a file, Application Control fetches its reputation and that of all certificates associated with the file to determine whether to allow or ban the file execution.

All files that are allowed to run in Observe mode are automatically added to the whitelist, if not already present in the whitelist. An observation is logged that corresponds to the action Application Control takes in Enabled mode.

Important

This mode is available only with Application Control and in a McAfee ePO managed environment.

Update mode

This mode indicates that protection is effective but changes are allowed on protected endpoints. When you perform software updates in Update mode, Application Control tracks and records each change. Also, it dynamically updates the whitelist to make sure that the new binaries and files are authorized to run when the system returns to Enabled mode. In Update mode, all tracked changes are added to the whitelist. If you delete any software or program files from the system, their names are also removed from the whitelist.

In a managed environment, Update mode supports reputation-based execution. When you execute a file at an endpoint, the software fetches the file's reputation and the reputation of all associated certificates to determine whether to allow or ban the file execution.

Tip

Best practice: Use Update mode only for installing minor software updates. For example, define an interval to allow the IT team to complete maintenance tasks, such as installing patches or upgrading software.

Disabled mode

This mode indicates that the software isn't running on your system. Although the application is installed, its features are disabled. After installation, the application appears in Disabled mode by default. You can then switch to Observe, Update, or Enabled mode.

Inventory mode

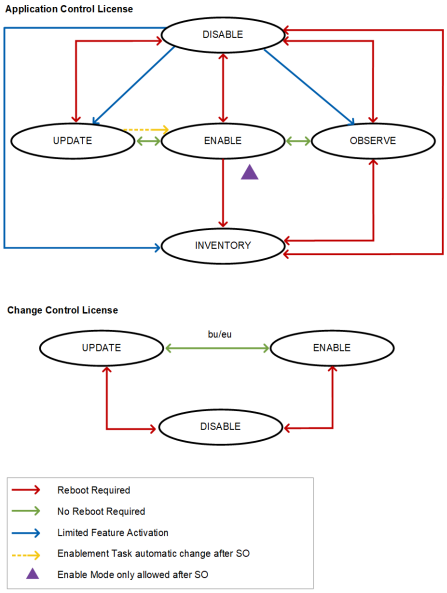
This mode indicates that protection is not effective but changes are allowed on endpoints. When you perform software updates in Inventory mode, Application Control tracks and records each change. Also, it dynamically updates the whitelist with the new binaries and files. In this mode, all tracked changes are added to the whitelist. If you delete any software or program files from the system, their names are also removed from the whitelist. On managed systems, all these changes on the whitelist will fetch the Inventory on the ePO, keeping this information updated with all the changes on the endpoint.

Switching between modes

- From Observe mode, you can switch to Enabled, Disabled, or Inventory mode.
- From Enabled mode, you can switch to Disabled, Update, Observe, or Inventory mode.
- From Update mode, you can switch to Enabled, Disabled, or Inventory mode.
- From Disabled mode, you can switch to Enabled, Update, Observe, or Inventory mode.
- From Inventory mode, you can switch to Disabled, Update, or Observe mode.

Note

You can't use the **SC:Disable** task to switch from Observe mode to Disable mode. You must use the **SC:Observe Mode** task and set Enable/Disable as needed. Or from the local CLI, use **sadmin eo -d** than **sadmin disable**.



Enable the software in a managed environment

When Application Control is running in Enabled mode, the only programs that are allowed to run are trusted and authorized. Malicious or unauthorized programs are not allowed to run.

Before you begin

Use the **SC: Pull Inventory** client task to fetch the inventory details from the endpoints before placing them in Enabled mode. This ensures that the inventory is loaded and updated in McAfee ePO database and prevent any mismatch.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Select a group or an endpoint:
    - Group — Go to **System Tree** and click the **Assigned Client Tasks** tab.

- Specific endpoint — On the **Systems** tab, select the endpoint you want to work with and click **Actions** → **Agent** → **Modify Tasks on a Single System**.

3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
   a. For **Product**, select **Solidcore 8.x.x**.
   b. For **Task Type**, select **SC: Enable**.
   c. For **Task Name**, click **Create New Task** to open the **Client Task Catalog** page.
   d. Enter the task name and add any descriptive information.
   e. Select the platform and sub-platform, then select **Application Control**, **Change Control**, or both.
4. Based on the sub-platform, perform these actions, then click **Save**.
   - **Windows NT/2000** — Select **Reboot endpoint** to restart the endpoints when solidification is complete, which enables the software.
   - **All except NT/2000**
     - Select the initial scan priority of the thread that creates the whitelist on the endpoints:
       - **Low** — Minimal performance impact
       - **High** — Faster results
     - Select an option for activation
       - **Limited Feature Activation** — Endpoints aren't restarted and limited features of Application Control are activated. Memory Protection and Script As Updater (SAU) features are available only after the endpoint is restarted.
       - **Full Feature Activation** — Endpoints are restarted, whitelist created, and all features including Memory Protection are active.
     - (Optional) Select **Start Observe Mode** to place the endpoints in Observe mode.
     - (Optional) Select **Start Inventory Mode** to place the endpoints in Inventory mode.
     - (Optional) Select **Pull Inventory** to manage the inventory with McAfee ePO.

   Five minutes before the endpoint is restarted, a message is displayed at the endpoint to allow the user to save important work and data.
5. Click **Next** to open the **Schedule** page.
6. Specify scheduling details, then click **Next**.
7. Review and verify the task details, then click **Save**.
8. (Optional) Wake up the agent to send your client task to the endpoint immediately.

Enable the software in an unmanaged environment

Add the license and place the software in Enabled mode.

Task

1. Add the software license, then restart the service:
   a. `sadmin license add <license_key>`
   b. `net stop scsrvc`

c. `net start scsrvc`

2. For Application Control, create a whitelist of authorized executable files, then verify its status:
   a. `sadmin so`
   b. `sadmin status`
      Make sure that the status of drives or volumes is `Solidified`.
3. Enable the software, then restart the service:
   a. `sadmin enable`
   b. `net stop scsrvc`
   c. `net start scsrvc`
4. Verify that the software is in Enabled mode:
   `sadmin status`

Using recommended configuration

Use 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 overflow. Enable all memory protection features and consult with McAfee support team to evaluate the risk for any exception or bypass. For information about disabling memory protection for Endpoint Security, see KB81465 and KB89678.
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 on 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 to keep up with the 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. The needed commands can be issued from the McAfee ePO console using the **SC: Run Commands Client Task**.

Feature	Description
Trusted update mechanisms	Application Control includes several methods to make sure proper functioning and updating of applications. We also provide a default list of trusted executables. We recommend you carefully update or change this list.
Alerts and notifications	Constant monitoring is a part of protecting your systems. Application Control sends events to the McAfee ePO console when it prevents an unwanted operation. We recommend configuring the needed alerts and email notifications to inform the user about these activities.

File and certificate reputation

Reputation sources and communication

Application Control works with multiple sources to fetch reputation information for files and certificates.

Important

Reputation information is available only in a McAfee ePO managed environment.

Application Control supports reputation-based execution. When you run a file at an endpoint, the software fetches its reputation and reputation of all certificates associated with the file to determine whether to allow or ban the file execution. The settings configured for your enterprise determine the reputation values that are allowed and banned.

Reputation sources

Based on the configuration, the software regularly synchronizes with these sources:

- **TIE server** – The TIE server is a local reputation server that communicates with multiple reputation sources. It effectively combines and collates intelligence from global sources with local threat intelligence and customized organizational knowledge to provide aggregated reputation values.
- **McAfee GTI server** – McAfee GTI is a cloud-based service that functions as a reputation source. Application Control periodically synchronizes with the McAfee GTI server to fetch ratings for executable files and certificates. The **Fetch File Details from McAfee GTI Server** and **Fetch Certificate Reputation from McAfee GTI Server** tasks are internal tasks that run automatically several times a day to fetch McAfee GTI ratings for executable files and certificates.

Communication with TIE server and McAfee GTI.

Here is how Application Control communicates with the TIE server and McAfee GTI server.

- **TIE server –** Application Control communicates directly with the TIE server configured in your environment.

- **McAfee GTI–** Application Control communicates directly with the McAfee GTI server. But, if a proxy server is configured in your setup, Application Control uses it to communicate with the McAfee GTI server. The proxy server is configured on the **Menu → Configuration → Server Settings → Proxy Settings** page.
- With 8.3.0, 8.2.1, and earlier versions we fetched McAfee GTI using SHA1 and cert hashes from both URLs below.
- MACC extension 8.2.6 started supporting TLS Protocol version 1.2 for McAfee GTI. This is done by updating McAfee GTI server URL along with all the underlying McAfee GTI APIs.

Firewall URL and ports needed for GTI communication:

8.3.0, 8.2.1 and below:

URL	Ports
Cwl2.gti.mcafee.com	443
Mace.rest.gti.mcafee.com	443

8.2.6, 8.3.1 or above:

URL	Ports
Mace.rest.gti.mcafee.com	443

Reputation values received from sources

Application Control communicates with TIE and McAfee GTI servers at regular intervals to fetch reputation information for executable files and certificates.

Values from TIE server

The TIE server offers scores from various providers, such as McAfee® Advanced Threat Defense, McAfee GTI, and event trace logs (ETL) that Application Control uses to compute reputation.

- **Known trusted** – A trusted file or certificate.
- **Most likely trusted** – Almost certainly a trusted file or certificate.
- **Might be trusted** – Seemingly a benign file or certificate.
- **Unknown** – The reputation provider can't determine its reputation at the moment.
- **Might be malicious** – A suspicious file or certificate.
- **Most likely malicious** – Almost certainly a malicious file or certificate.
- **Known malicious** – A malicious file or certificate.

- **Not set** – Undetermined file or certificate reputation.

Values from McAfee GTI

For each executable file, McAfee GTI provides the reputation and classification values.

- **File Hash Reputation** indicates if the file is trusted or malicious. Based on information fetched from McAfee GTI, the application and files are sorted into categories on the Application Control pages.
- **File Hash Classification** indicates the reliability or credibility of the file. The assigned value indicates if the file is trusted, unknown, or malicious.

For each certificate, McAfee GTI provides a score that indicates its reputation.

McAfee GTI classification for files	McAfee GTI score for certificates	Description
known_clean	99	Known trusted
analysed_clean, assumed_clean	85	Most likely trusted
raiden_analyzed_clean, noise_clean	70	Might be trusted
unknown	50	Unknown
assumed_dirty, assumed_dirty2	30	Might be malicious
assumed_dirty3, assumed_dirty4	15	Most likely malicious
pup, trojan, virus, app	1	Known malicious
Not available	0	Not set

Values from Application Control

Application Control can track the enterprise trust level or reputation by Application Control value for each executable file. When edited, this value for a file overrides the existing reputation for the file.

For example, your organization uses an internally developed application that is set as an unknown application because it is specific to your organization. Because you trust the application, you can recategorize it as a trusted file by editing its reputation. The values are:

- Known Malicious
- Unknown

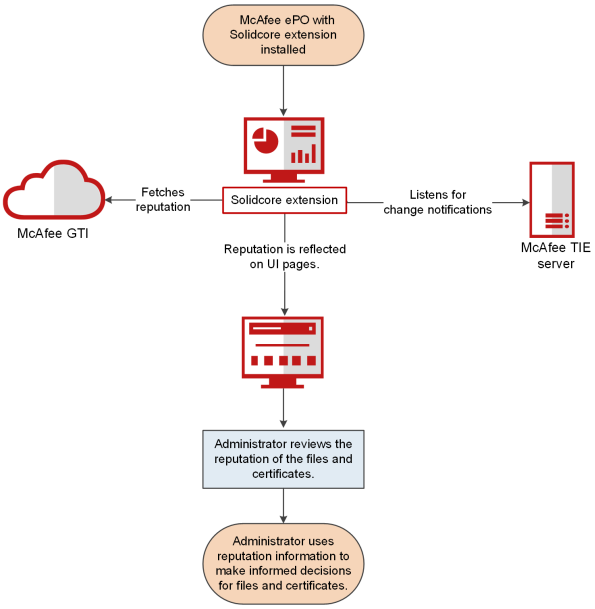
- Known Trusted

McAfee ePO workflow

Application Control communicates with the McAfee GTI server at regular intervals to fetch reputation information for executable files and certificates. But, if the TIE server is configured in your environment, Application Control also continuously listens to reputation change notifications received from the TIE server.

A change to the reputation of a file triggers a **Reputation change notification**. Values are updated and a corresponding **Reputation changed** entry is added to the **Server Task Log Details** page. Each entry includes information about the file, its old and updated reputation, and file SHA-1.

If communication with the TIE server is temporarily suspended, all missed notifications are synced after communication resumes.



Endpoint workflow

The Solidcore client supports reputation-based execution on endpoints.

When the user executes a file, Application Control contacts the reputation source to fetch reputation information as follows:

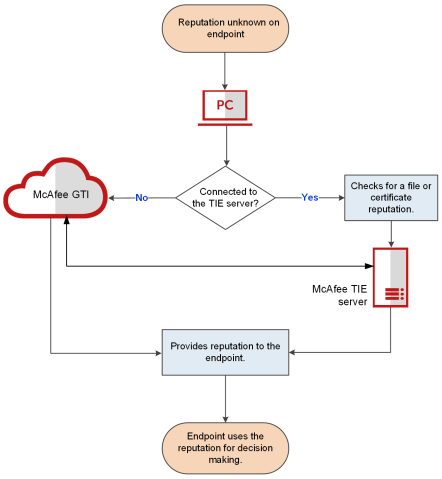
- If the TIE server is configured, the endpoint communicates with the server to fetch reputation for the executable file or all certificates associated with the file.
- If the TIE server isn't installed or is unavailable, the endpoint communicates with the McAfee GTI server to fetch reputation for the executable file or all certificates associated with it.

Note

To verify if fetching reputation from TIE server or McAfee GTI server is enabled for an endpoint, review the value for the **Reputation (TIE)** or **Reputation (GTI)** property for the endpoint. To navigate to the property, click the row corresponding to the endpoint on the **Systems** page and click the **Solidcore** row in the **Products** tab.

1. Check if an explicit ban rule exists for the file.
    - If yes, prevent file execution.
    - If no, verify the file and certificate reputation.
2. Allow or block file execution based on reputation according to the defined reputation settings.

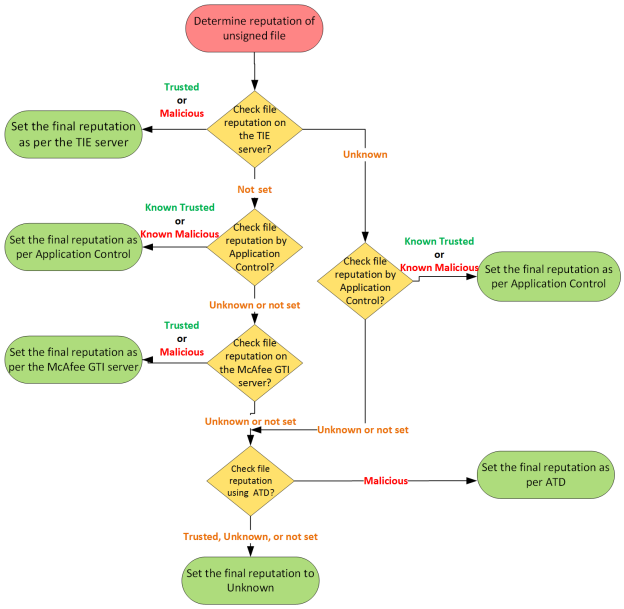
Application Control also uses defined rules and policies to determine file execution status.



How reputation is computed

On the McAfee ePO console, reputation information for a file is received from various sources, then collated to compute reputation. Application Control uses values and parameters provided by these sources to determine final reputation for files and certificates.

Here is how final reputation is computed for an unsigned file.



Here is how final reputation is computed for a signed file.

Change file reputation

Application Control works with multiple sources to fetch reputation information. The software regularly synchronizes with TIE and McAfee GTI. You can review or edit the reputation for a file on the **TIE Reputations** page.

Task

1. Select **Menu** → **Application Control** → **Policy Discovery**.
2. On the **Policy Discovery** page, select a request and click **Actions** → **More** → **Change File Reputation (TIE)**
3. Review the file information about the **TIE Reputations** page.
4. (Optional) Edit file reputation: click **Actions**, then select an action.

Memory-protection techniques

Memory-protection techniques prevent malware execution and unauthorized attempts to gain control of a system through buffer overflow. Application Control offers multiple techniques to prevent zero-day attacks.

At a high-level, the available techniques stop two kinds of exploits.

- Buffer overflow followed by direct code execution.
- Buffer overflow followed by indirect code execution using Return-Oriented Programming.

For a detailed and updated list of exploits prevented by memory-protection techniques, subscribe to McAfee Threat Intelligence Services (MTIS) security advisories.

<table>
<tr><th>Technique</th><th colspan="2">Description</th></tr>
<tr><td rowspan="3">CASP — Critical Address Space Protection (mp-casp)</td><td colspan="2">CASP is a memory-protection technique that renders useless any shellcode running from the non-code area. This shellcode is an abnormal event that usually happens because of a buffer overflow.

CASP allows code to execute from non-code area but disallows the code from invoking any meaningful API calls, such as CreateProcess() and DeleteFile(). When exploit code invokes these APIs, CASP blocks it and it fails to do any damage.

Note: When you use CASP, it protects all processes running on your Windows system except for those processes that are already protected by Windows protection feature.</td></tr>
<tr><td>Supported operating systems</td><td>32-bit and 64-bit — Windows Server 2008, Windows 7, Windows Embedded 7, Windows 8, Windows Embedded 8, Windows 8.1, Windows Embedded 8.1, Windows 10, Windows 10 IoT Enterprise, and Windows Server 2016.</td></tr>
<tr><td>Default state</td><td>Enabled</td></tr>
</table>

Technique	Description	
	Event generated	PROCESS_HIJACK_ATTEMPTED
NX — No eXecute (mp-nx)	The NX feature uses the Windows Data Execution Prevention (DEP) feature to protect processes against exploits that try to execute code from writable memory area (stack/heap). NX also provides granular bypass capability and raises violation events that can be viewed on the McAfee ePO console. Windows DEP prevents code from being run from a non-executable memory region. This abnormal event mostly occurs due to a buffer overflow. The malicious exploit attempts to execute code from these non-executable memory regions.	
	Supported operating systems	64-bit — Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows Embedded 7, Windows 8, Windows Embedded 8, Windows 8.1, Windows Embedded 8.1, Windows 10, Windows 10 IoT Enterprise, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016. This feature isn't available on the IA64 architecture.
	Default state	Enabled
	Event generated	NX_VIOLATION_DETECTED
Forced DLL Relocation (mp-vasr-forced-relocation)	This feature forces relocation of those dynamic-link libraries (DLLs) that have opted out of the Windows native ASLR feature. Some malware relies on these DLLs always being loaded at the same and known addresses. By relocating such DLLs, these attacks are prevented.	
	Supported operating systems	32-bit and 64-bit — Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows Embedded 7, Windows 8, Windows Embedded 8, Windows 8.1, Windows Embedded 8.1, Windows 10, Windows 10 IoT Enterprise, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.
	Default state	Enabled
	Event generated	VASR_VIOLATION_DETECTED

Occasionally, some applications (as part of their day-to-day processing) might run code in an atypical way and be prevented from running by the memory-protection techniques. To allow such applications to run, you can define specific rules to bypass the memory-protection techniques.

Configuring CASP

CASP is a memory-protection technique that renders useless any shellcode running from the non-code area. This shellcode is an abnormal event that usually happens because of a buffer overflow.

CASP allows code to execute from non-code area but disallows the code from invoking any meaningful API calls.

To protect the code in a non-code area from making API calls, configure rules to add executables to CASP.

Task	Syntax	Description
Bypass executables from CASP.	`sadmin attr add -c <filename1 ... filenameN>`	Specify one or more executables where CASP must be bypassed. For example, `sadmin attr add -c alg.exe`
Remove executables from CASP bypass.	`sadmin attr remove -c <filename1 ... filenameN>`	Specify one or more executables to remove from CASP bypass; in effect CASP is enforced. For example, `sadmin attr remove -c alg.exe`
List the executables that CASP bypasses.	`sadmin attr list -c`	Lists all executables that CASP bypasses. For example, `sadmin attr list -c`
Flush the CASP bypass rules from all executables.	`sadmin attr flush -c`	Removes the CASP bypass rules from all executables. For example, `sadmin attr flush -c`

Configuring bypassing rules for NX

The NX feature uses the Windows Data Execution Prevention (DEP) feature to protect processes against exploits that try to execute code from writable memory area (stack/heap). MP-NX also provides granular bypass capability and raises violation events that can be viewed on the Windows Event Viewer console.

To protect processes against exploits that try to execute code from writable memory area, configure rules to add executables to NX. This technique prevents code from being run from a non-executable memory region.

Task	Syntax	Description
Bypass executables from NX.	`sadmin attr add –n <filename1 ... filenameN>`	Specify one or more executables where NX must be bypassed. For example, `sadmin attr add –n alg.exe`
Bypass an executable and its child processes from NX.	`sadmin attr add –n -y <filename1 ... filenameN>`	Specify an executable where NX must be bypassed, including its child processes. You can specify the `-y` option only with the `-n` option. For example, `sadmin attr add –n -y alg.exe`
Remove executables from NX bypass.	`sadmin attr remove –n <filename1 ... filenameN>`	Specify one or more executables to remove from NX bypass; in effect NX is enforced. For example, `sadmin attr remove –n alg.exe`
List the executables that are bypassed from NX.	`sadmin attr list –n`	Lists all executables that NX bypasses. For example, `sadmin attr list –n`
Flush NX bypass rules from all executables.	`sadmin attr flush –n`	Removes the NX bypass rules from all executables. For example, `sadmin attr flush –n`

Configuring Forced DLL Relocation

This feature forces relocation of those dynamic-link libraries (DLLs) that have opted out of the Windows native ASLR feature. Some malware relies on these DLLs always being loaded at the same and known addresses. By relocating such DLLs, these attacks are prevented.

Configure rules to add one or more executables to Forced DLL Relocation.

Task	Syntax	Description
Bypass executables from Forced DLL Relocation.	`sadmin attr add –v <filename1 ... filenameN>`	Specify one or more protected components where you bypass Forced DLL Relocation. For example, `sadmin attr add –v AcroRD32.exe`
Enforce Forced DLL Relocation on executables.	`sadmin attr remove –v <filename1 ... filenameN>`	Specify one or more components where you enforce Forced DLL Relocation. For example, `sadmin attr remove –v AcroRD32.exe`
List the executables that Forced DLL Relocation bypasses.	`sadmin attr list –v`	Lists all components that Forced DLL Relocation bypasses. For example, `sadmin attr list –v`
Flush Forced DLL Relocation rules from all executables.	`sadmin attr list –v`	Removes Forced DLL Relocation rules from all executables. For example, `sadmin attr flush –v`
Bypass a DLL module that is loaded for a specific process.	`sadmin attr add –o module=<DLLmodulename> –v <processname>`	Bypass the DLL module name for a process. For example, `sadmin attr add –o module=wuauserv.dll –v svchost.exe`

Using checksum values

You can override the protection applied to a system by authorizing certain files based on their SHA-1 or SHA-256 values.

Authorizing files by their SHA-1 or SHA-256 value allows them to run on a protected system. If a file is not added to the whitelist but configured as an authorized file, it is allowed to run. Regardless of the source of a file, if the SHA-1 or SHA-256 value matches, the file is allowed to run. Likewise, files can be banned from execution based on their checksum, preventing them to run even if the files are in the whitelist.

You can also provide updater permissions to an authorized file. Configuring an authorized binary as an updater provides the updater permissions in addition to the execution. An authorized file that is configured as an updater is allowed to update or run software on a protected system. Installers can also be authorized by SHA-1 or SHA-256 value and configured as updaters to allow

them to install new software and update the software components. For example, if you authorize the installer for the Microsoft Office 2010 suite by SHA-1 or SHA-256 and also configure the installer as an updater, if the SHA-1 or SHA-256 value matches, the installer is allowed to install the Microsoft Office suite on the protected systems.

Authorize binaries

You can authorize binaries to allow them to execute on a protected system.

Syntax	Description
`sadmin auth -a -c <checksumvalue>`	Specify the SHA-1 or SHA-256 value of the binary to be authorized. For example: `sadmin auth -a -c 803291bcc5aa45a0221b4016f62d63a26d3ee4af`
`sadmin auth -a [-t tagname] -c <checksumvalue>`	Include the tag name and the checksum value of the binary to be authorized. For example: `sadmin auth -a -t Win_up_schedule1 -c 803291bcc5aa45a0221b4016f62d63a26d3ee4af`
`sadmin auth -a -u -c <checksumvalue>`	Authorize a binary and also provide updater permissions. Specify the checksum value of the binary to be authorized and added as an updater. For example: `sadmin auth -a -u -c 803291bcc5aa45a0221b4016f62d63a26d3ee4af`

Note

Use `sadmin auth -l` to list authorized binaries.

Ban binaries

You can restrict binaries from executing on a protected system.

Syntax	Description
`sadmin auth -b -c <checksumvalue>`	Specify the SHA-1 or SHA-256 value of the file to be banned. For example: `sadmin auth -b -c 803291bcc5aa45a0221b4016f62d63a26d3ee4af`
`sadmin auth -b -t <tagname> -c <checksumvalue>`	Include the tag name and SHA-1 or SHA-256 value of the file to be banned. For example: `sadmin auth -b -t AUTO_1 -c 583291bcc5aa45a0221b4016f62d63a26d3ee9at`

Note

Use `sadmin auth -l` to list banned binaries.

Remove checksum rules

You can remove authorized or banned binaries from your system.

Syntax	Description
`sadmin auth -r <checksumvalue>`	Specify the SHA-1 or SHA-256 value of the file to be removed. For example: `sadmin auth -r 803291bcc5aa45a0221b4016f62d63a26d3ee4af`
`sadmin auth -f`	This command removes all authorized or banned binaries.

Authorizing and banning execution of binaries by name

You can override the applied protection by specifying the name of binaries (programs or files) to authorize or ban their execution.

When you specify a binary name to authorize its execution on a protected system, all binaries that have the same name and are present on the system or network directories are authorized to execute. Similarly, if you ban a binary by specifying its name, all binaries that have the same name are not allowed to execute.

For example,

- `sadmin attr add -a setup.exe`
- `sadmin attr add -u setup.exe`

Note

On Windows platforms, the drive letter is truncated. So, if the file path \Program Files\Google\Picasa3\setup.exe is located in any other drive instead of C, the file is still authorized to execute.

View authorized and banned binaries

You can view authorized and banned files on a protected system.

Task

Run these commands at the command prompt.

Command	Description
`sadmin attr list -a`	Lists all files that are authorized by name.
`sadmin attr list -m`	Lists all the files that are blocked in interactive mode.
`sadmin attr list -u`	Lists all files that are banned by name.

Remove authorized and banned rules

You can remove binaries authorized by name to prevent them from executing on a protected system.

Task

Run these commands at the command prompt.

Command	Description
`sadmin attr remove -a <filename>`	Removes the added rule to authorize the specified binary by name. Specify the same file name or path that was used to add the rule.
`sadmin attr remove -m <filename>`	Removes the added rule to block the interactive mode for a file.
`sadmin attr remove -u <filename>`	Removes the added rule to ban the specified binary by name. Specify the same file name or path that was used to add the rule.
`sadmin attr flush -a`	Removes the authorized by name rules for all files.
`sadmin attr flush -m`	Removes the block in interactive mode rules for all files.
`sadmin attr flush -u`	Removes the banned by name rules for all files.

Using trusted directories

Manage trusted directories in a managed environment

When you add directories as trusted directories, systems can run any software present in these directories.

Task

1. On the McAfee ePO console, create or modify an Application Control policy or rule group.
2. On the **Rule Groups** tab, locate your **Group Name** and under **Actions**, click **Edit**.
3. On the **Directories** tab, click **Add**.
4. Enter the location of the directory.
5. Select **Include** or **Exclude**.
   Use **Exclude** to exclude a specific folder or subfolder within a trusted directory.
6. Click **OK**.

Manage trusted directories in an unmanaged environment

You can add directories as trusted directories to run any software present in these directories in an unmanaged environment.

Task

1. Add one or more specified paths to the directories or volumes as trusted directories or volumes:

   ```
   sadmin trusted -i <pathname1...pathnameN>
   sadmin trusted -i C:\Documents and Settings\admin\Desktop\McAfee
   sadmin trusted -i \\192.168.0.1\documents
   ```

2. Provide updater rights to all binaries and scripts in the trusted directories or volumes:

   ```
   sadmin trusted -u <pathname1...pathnameN>
   sadmin trusted -u C:\Documents and Settings\admin\Desktop\McAfee
   sadmin trusted -u \\192.168.0.1\documents
   ```

   Note

   You can also add a trusted volume by specifying a volume name with this command to include all binaries and scripts present in the specified volume as updaters. Use the `sadmin trusted -i -u <volumename>` command to specify the volume name.

3. View the list of trusted directories:

   ```
   sadmin trusted -l
   ```

4. Exclude specific directories:

   ```
   sadmin trusted -e <pathname1...pathnameN>
   sadmin trusted -e C:\Documents and Settings\admin\Desktop\McAfee
   sadmin trusted -e \\192.168.0.1\documents
   ```

5. Remove trusted directories:

   ```
   sadmin trusted -r <pathname1...pathnameN>
   sadmin trusted -r C:\Documents and Settings\admin\Desktop\McAfee
   sadmin trusted -r \\192.168.0.1\documents
   ```

Specify directory paths

You can specify directory paths to be added as trusted directories on a mounted network file system.

Task

Add the directory path.

- Specify the server name that has a network share or the name of the network share:

  ```
  sadmin trusted -i \\server-name\share-name
  ```

- Specify all network shares by all servers:

  ```
  sadmin trusted -i \\*
  ```

Paths can include the wildcard characters to specify file paths and file names. When using wildcards, specified strings must match a limited set of file paths or file names. If the specified string matches many files, we recommend you revise the string.

Paths can include the ***** and **?** wildcard characters. When specifying a trusted directory, \\10.10.10.10*****\User2, \ \10.10.10.10\????\User2, \\10.10.10.10*AD** and \\10.10.10.10\?AD?***\User1 are allowed while *\AD\User1, *. 10.10.10\AD*\User1, and \\10.**10.10\AD*\User1 are not supported.

Using rule groups in a managed environment

What are rule groups?

A rule group is a collection of rules. Although you can directly add rules to any McAfee ePO-based policy, the rules defined in a policy are specific to that policy. In contrast, a rule group is an independent unit that collates a set of similar or related rules.

After you define a rule group, you can reuse the rules by associating the group with different policies. Also, when you change or update a rule group, the change is automatically introduced into all associated policies.

Application Control provides predefined rule groups to allow commonly used applications to run smoothly. Although you can't edit the predefined rule groups, you can use an existing rule group as a starting point to develop new rule groups. If needed, you can also import or export rule groups.

Rule groups can drastically reduce the effort required to define similar rules across policies. If you have a large setup and you are deploying the software across numerous endpoints, use rule groups to minimize the deployment time and effort.

Rule group ownership

Users can edit and delete only the rule groups that they own. A user who creates a rule group, is automatically set as the owner of the rule group. Only the owner and McAfee ePO administrator can edit and delete the rule group. Also, the administrator can assign ownership to other users or revoke ownership from the owner. In this case, the ownership is automatically granted to the McAfee ePO administrator.

Users who don't own a rule group can only view the rule group and its policy assignments, duplicate the rule group, and add the rule group to policies. But, if the owner or the McAfee ePO administrator updates a rule in the rule group, the change cascades across all associated McAfee ePO policies.

This scenario suits non-global administrators who want to use a rule group (created by theMcAfee ePO administrator) without maintaining it. If this scenario does not suit your requirements, duplicate the rule group that you don't own, then assign the duplicate to policies. This method provides you ownership of the duplicated rule group.

Rule group example

Here is an example of how rule groups are used.

An organization runs Oracle on multiple servers. Each of these servers is used by the HR, Engineering, and Finance departments for different purposes. To reduce rule redundancy, we define an Application Control rule group (named AC-Oracle) with rules to define the relevant updaters for Oracle to function.

After the rule group is defined, we can reuse these rule groups across policies for the different departments. So, when defining the HR Servers policy, add the AC-Oracle rule group to the policy with rule groups for the other applications installed on the HR server. Similarly, add the AC-Oracle rule group to the relevant policies for the Engineering Servers and Finance Servers. After defining the policies, if the rule for a critical file was not created, directly update the rule group to automatically update all policies.

Manage rule groups and policies

Create a rule group

You can create a rule group from scratch or copy an existing rule group and change it as needed.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
2. On the **Rule Groups** tab, select **Application Control** from the **Type** menu.
3. Create a rule group or copy an existing rule group.
    - Create a rule group:
        - Click **Add Rule Group** to open the **Add Rule Group** dialog box.
        - Specify the rule group name, type, and platform, then click **OK**.
        - Under **Actions**, click **Edit** to specify the required rules, then click **Save Rule Group** to save all changes.
    - Copy an existing rule group:
        - Under **Group Name**, select the rule group you want to duplicate.
        - Under **Actions**, click **Duplicate** to open the **Duplicate Rule Group** dialog box.
        - Specify the rule group name, then click **OK**.
        - Under **Actions**, click **Edit** to specify the required rules, then click **Save Rule Group** to save all changes.

Manage permissions for rule group tabs

Specify permissions for the **Rule Groups**, **Certificates**, **Installers** pages, and the tabs contained in rule group and policy pages.

Task

1. On the McAfee ePO console, select **Menu** → **User Management** → **Permission Sets**.
2. Click **New Permission Set** to create a permission set.
3. Enter a name for the permission set, select the users you want to assign the permission set to and click **Save**.
   The selected level of permissions is granted to the user.

Note

When multiple permission sets are applied to a user account, they aggregate. Consider this as you plan your strategy for granting permissions to the users in your environment.

4. Under **Permission Sets**, click **Solidcore Admin** or **Solidcore Reviewer**.
5. On the right pane, click **Edit** on the **Solidcore General** permissions category.
6. Grant permissions for **Certificates**, **Installers**, and **Rule Groups**, as needed.
7. Grant permissions selectively for the tabs (**Updater Processes**, **Certificates**, **Installers**, **Directories**, **Users**, **Executable Files**, **Exclusions**, **Filters**, and **Execution Control**) contained in rule group and policy pages, as needed.
8. Click **Save**.

Delete or rename rule groups

You can delete or rename a rule group, as needed.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
2. Complete one of these actions from the **Rule Groups** tab.
    - To rename a rule group, click **Rename**, specify a new name, and click **OK** to close the **Rename Rule Group** dialog box.
    - To delete a rule group, click **Delete** and click **Yes** to close the **Delete Rule Group** dialog box.

View assignments for a rule group

Instead of navigating through all created policies, you can directly view all policies where a rule group is being used. This feature provides a convenient way to verify if each rule group is assigned to the relevant policies.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
2. On the **Rule Groups** tab, click **Assignments** for a rule group to view its assigned policies.

Attribute-based rules

Application Control performs multiple checks to determine whether to allow or block a file's execution. If a file's execution is allowed after the Application Control checks, attribute-based or granular rules, if any are defined, come into play. The rules are based on the concept of fine-grained whitelisting and can be created on the attributes of a file.

You can define specific rules using attributes to allow, block, or monitor the file. Rules that allow execution take precedence over rules that block or monitor execution.

Attribute-based rules help you allow or block files in different scenarios based on file context. On a protected system, only whitelisted interpreters are allowed to run. But, in certain scenarios, whitelisted interpreters might be misused to execute malicious scripts. You can prevent misuse of interpreters by defining attribute-based rules to block potentially malicious scenarios.

Attribute-based rules provide flexibility to allow or block file execution, as needed. If an administrator needs to block a user from running a specific file, they can add an attribute-based rule to prevent its execution by that user. Similarly, an administrator can choose to block execution of a certain file altogether, unless when run by a specific parent process.

Tip

We recommend that before creating a *block rule* for a file, create a *monitor rule* to observe the file's use and execution in your setup. After you define the monitoring rule, if no **OBSERVED_FILE_EXECUTION** events are generated for the file over a reasonable time window, you can safely define a block rule for a file. But, the applied rules are ineffective when the system is in update mode, observe mode, or when any process is selected as updater process and only the events are generated.

Define attribute-based rules for file execution

Attribute-based rules provide flexibility to allow or block file execution, as needed.

Task

1. On the **Rule Groups** tab, locate your **Group Name** and under **Actions**, click **Edit**.
2. On the **Execution Control** tab, click **Add**.
3. To define an attribute-based rule for a file, select **Based on specified attributes**.
4. Select the type of rule to define: **Allow**, **Block**, or **Monitor**.
5. Specify the file name.
6. Specify the attributes to define the rule.
   You can use one or all attributes to define the rule. Available attributes are path, command line, parent process, and user.
   You can use the AND operator to combine rules based on different attributes.
   a. Select the checkbox associated with the attribute.
   b. Select the operator for the attribute.
   c. Enter the string.
7. (Optional) Enter the rule description.
8. Click **OK**.

Create a policy

Add specific rules to a rule group or policy. Most Application Control policies are multi-slot policies; a user can assign multiple policies to a single endpoint in the System Tree.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select **Solidcore 8.x.x: Application Control** for the product.
3. Click **New Policy** to open the **Create a new policy** dialog box and select the category.
4. Based on the category, perform one of these actions:
   - If you selected **Application Control Options (Windows)** category, select the policy you want to duplicate from **Create a policy based on this existing policy** list.
   - If you selected any other category, select **Blank Template** from **Create a policy based on this existing policy** list to define a policy from scratch.
5. Specify the policy name, then click **OK** to open the **Policy Settings** page.
6. Add a rule group to the policy.
   a. Select the rule group in the **Rule Groups** tab.
   b. Select **Add** in the **Rule Groups** tab to open the **Select Rule Groups** dialog box.
   c. Select the rule group to add, then click **OK**.
7. Add the rules to the policy and save changes.

Predefined rules in default policies

Application Control includes predefined rules for commonly used applications for all supported operating systems.

Apply these default policies to the endpoints to ensure proper product functionality. If available, you can use the blank template or duplicate these policies to configure the settings. These are the predefined rules included in these policies.

Default policy	Product	Category	Policy type	Description	Blank template available
McAfee Default	**Solidcore 8.x.x: General**	**Configuration (Client)**	Single-slot	Default settings for CLI, throttling, and more for the Solidcore client.	No
McAfee Default	**Solidcore 8.x.x: General**	**Exception Rules (Unix)**	Multi-slot	Default exception rules for the UNIX platform.	Yes
McAfee Default	**Solidcore 8.x.x: General**	**Exception Rules (Windows)**	Multi-slot	Default rules for memory protection and other bypass techniques on the Windows platform.	Yes

Default policy	Product	Category	Policy type	Description	Blank template available
McAfee Default	**Solidcore 8.x.x: Application Control**	**Application Control Options (Windows)**	Single-slot	Default settings for self-approval, end-user notifications, inventory, reputation, and Application Control features on the Windows platform.	No
My Default	**Solidcore 8.x.x: Application Control**	**Application Control Options (Windows)**	Single-slot	Default settings for self-approval, end-user notifications, inventory, reputation, and Application Control features on the Windows platform.	No
McAfee Default	**Solidcore 8.x.x: Application Control**	**Application Control Rules (Unix)**	Multi-slot	Default rules to design the trust model on the UNIX platform. This policy also includes default filters to exclude events that aren't relevant for your setup.	Yes
McAfee Default	**Solidcore 8.x.x: Application Control**	**Application Control Rules (Windows)**	Multi-slot	Default rules to design the trust model on the Windows platform. This policy also includes default filters to exclude events that aren't relevant for your setup.	Yes
McAfee Applications (**McAfee Default**)	**Solidcore 8.x.x: Application Control**	**Application Control Rules (Windows)**	Multi-slot	McAfee-specific rules that allow other McAfee products to run successfully on protected endpoints. These rules are also included in the McAfee Default policy for the Application Control Rules (Windows) category.	No

Default policy	Product	Category	Policy type	Description	Blank template available
Common ActiveX Rules	**Solidcore 8.x.x: Application Control**	**Application Control Rules (Windows)**	Multi-slot	Predefined read-only rules to install commonly used ActiveX controls on endpoints.	No
Throttling Rules	**Solidcore 8.x.x: Application Control**	**Application Control Rules (Windows)**	Multi-slot	Predefined read-only rules to filter and stop observations received from managed endpoints. When the number of observations received at the McAfee ePO server reaches the defined threshold, this policy is applied to all systems and groups in your organization.	No
Throttling Rules (Deprecated)	**Solidcore 8.x.x: Application Control**	**Application Control Rules (Windows)**	Multi-slot	Predefined read-only rules to filter and stop observations received from managed endpoints. When the number of observations received at the McAfee ePO server reaches the defined threshold, this policy is applied to all systems and groups in your organization.	No

Evaluation of trust model

Use recommended rule groups when evaluating trust model for the correct functioning of the policy.

During evaluation of your trust model and policy configuration, we recommend that you use the following rule groups to build your policies by testing your systems with default rule groups:

- McAfee Default
- McAfee Applications (McAfee Default)

McAfee Default policy contains rule groups for applications that are frequently requested by customers. We recommend that you duplicate the rules and customize them according to your organization's needs before applying to endpoints.

Note

Make sure McAfee default rules and Windows update rules are always included in your policy.

The McAfee Applications (McAfee Default) policy contains rules to allow McAfee applications, including McAfee Agent, and the McAfee certificate to function correctly in your environment.

Note

Make sure McAfee Applications (McAfee Default) rules are always assigned to endpoints.

Guidelines for domain controller policy

Use these guidelines when editing custom scripts on domain controllers.

Standard deployment process and frequently modified custom scripts must not be solidified. This can be done by adding script repositories to the skiplist -s policy within McAfee ePO. This must only be performed on domain controllers.

Note

Unsolidified scripts are designed to be executed on clients only and not on the system they are stored on.

Skiplist can be applied using a policy in McAfee ePO or by executing the command `Sadmin skiplist add -s <path/file>` on Command Prompt.

```
Sadmin skiplist add -s <path/file>
```

To apply skiplist as a policy, go to the specified **Rule Groups**, click **Filters**, and select exclude local path and all its files and subdirectories from the whitelist. You must specify a path/file.

Path considerations when defining rules

Regardless of whether you create a policy or define a rule group, the framework available to define rules is the same.

Supported system variables

The path specified in a rule can include system environment variables. This table lists the supported system variables.

Variable	Example value (most Windows platforms)
%ALLUSERSPROFILE%	C:\Documents and Settings\All Users
%APPDATA%	C:\Documents and Settings\{username}\Application
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES (x86)%	C:\Program Files (x86)\Common Files
%HOMEDRIVE%	C:
%HOMEPATH%	C:\Documents and Settings\{username} (\ on earlier Windows versions)
%PROGRAMFILES%	C:\Program Files
%PROGRAMFILES (x86)%	C:\Program Files (x86) (only for 64-bit versions)
%SYSTEMDRIVE%	C:
%SYSTEMROOT%	C:\windows (C:\WINNT on earlier Windows versions)
%TEMP% (system) %tmp% (user)	C:\Documents and Settings\{username}\local Settings\Temp C:\Temp
%USERPROFILE%	C:\Documents and Settings\{username} (C:WINNT\profiles\{username} for earlier versions)
%WINDIR%	C:\Windows

These considerations apply to path-based rules.

- Paths don't need to be absolute when specifying rules. For example, when defining an updater, you can specify partial or fully qualified paths.

- **Partial paths** — If you specify partial paths, such as AcroRd32.exe or Reader\AcroRd32.exe, all programs with names that match the specified string are assigned updater rights. Similarly, when blocking a file, all programs with names that match the specified string are blocked.
- **Fully qualified paths** — When you specify fully qualified paths, such as C:\Program Files\Adobe\Reader 9.0\Reader \AcroRd32.exe or \Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe only the specified program is assigned updater rights. When blocking a file, if you specify the fully qualified path, for example C:\Windows \system32\notepad.exe, only the specified file is blocked.

- Paths can contain white spaces.
- Paths can include the wildcard characters to specify file paths and file names. When using wildcards, ensure that specified string matches a limited set of file paths or file names. If the specified string matches many files, we recommend you revise the string.
- Paths can include the ***** and **?** wildcard characters.

Wildcard patterns

Paths specified in a rule can include the ***** and **?** wildcard characters.

These are the valid and invalid wildcard patterns you can use based on each feature.

Feature	Valid pattern	Invalid pattern
Read protect Write protect	• C:\Test1**\Test.txt • C:\Test1****\Test.txt • C:\Test1*****\Test.txt • C:**\Test.txt • C:*\Test.txt • C:\Test1\?\?\Test.txt • C:\Test1\?\???\Test.txt • C:\Test1\?????\Test.txt • C:\Test1\?\?.txt • C:\?\?\Test.txt • C:\?\Test.txt • C:\?\?.txt • C:\Test*\Test1\Test.txt • C:\Test?\Test1\Test.txt • C:\Test*\Test1*\Test.txt • C:\Test?\Test1?\Test.txt • C:\Test\Test????? • C:*Test\Test1\Test.txt • C:\?Test\Test1\Test.txt • C:*Test?\Test1\Test.txt	• *:\Test1\Test2\Test.txt • ?:\Test1\Test2\Test.txt • *\Test1\Test2\Test.txt • ?\Test1\Test2\Test.txt • *:\Test1**\Test.txt • C:\Test1\Test2\Test.* • C:\Test**** • C:\Test*.* • C:\Test\Test**** • C:*? • C:\?* • Test\Test1*\Test.txt • Test\Test1*\Test.* • Test\Test1*\Test.?

Feature	Valid pattern	Invalid pattern
	• C:\?Test*\Test1\Test.txt • C:*Test?QA\Test1\Test.txt • C:\?Test*QA\Test1\Test.txt	
Registry Write protect Monitor-registry	• HKEY_LOCAL_MACHINE\TestLevel1\Level2 • HKEY_LOCAL_MACHINE\TestLevel*\Level2 • HKEY_LOCAL_MACHINE\Test*1\Level2 • HKEY_LOCAL_MACHINE*TestLevel1\Level2 • HKEY_LOCAL_MACHINE*TestLevel*\Level2 • HKEY_LOCAL_MACHINE*\Level2 • HKEY_LOCAL_MACHINE**\Test • HKEY_LOCAL_MACHINE\TestLevel1*Level2 • HKEY_LOCAL_MACHINE\TestLevel?\Level2 • HKEY_LOCAL_MACHINE\Test?1\Level2 • HKEY_LOCAL_MACHINE\?TestLevel1\Level2 • HKEY_LOCAL_MACHINE\?TestLevel?\Level2 • HKEY_LOCAL_MACHINE\?\Level2 • HKEY_LOCAL_MACHINE\?\?\Test • HKEY_LOCAL_MACHINE\TestLevel1\?Level2 • HKEY_LOCAL_MACHINE\TestLevel1\?Level? • HKEY_LOCAL_MACHINE\TestLevel1\Level? • HKEY_LOCAL_MACHINE*?Test?Level1*\Level2	• *\TestLevel1\Level2 • HKEY_*_MACHINE\TestLevel1\Level2 • HKEY_LOCAL_MACHINE\TestLevel1* • HKEY_LOCAL_MACHINE\TestLevel1*Level* • HKEY_LOCAL_MACHINE\TestLevel1\Level* • ?\TestLevel1\Level2 • HKEY_?_MACHINE\TestLevel1\Level2 • HKEY_LOCAL_MACHINE\TestLevel1\?
Trusted Directory	• c:\windows*\test • c:\windows*\test*\test2 • *\AD\User1 • \\?\AD\User1 • \\10.??10.10\AD?\User1 • \\10.10.10.10\?AD?\User1 • \\10.10.10.10\????\User2 • \\10.10.10.10\?AD\User1 • \\10.10.10.10\AD?\User1 • \\10.10.10.10\?AD?\User? • \\10.10.10.10\?AD?\?User1 • \\10.10.10.10\?AD?\?User1? • \\10.10.10.10\?AD?\?	• c:\windows*\a* • c:\windows* • c:\windows*\ • c:\windows*?\a • c:\windows**\a • c:\windows***\a • \\10.10.10.10\AD*\User1 • \\10.**10.10\AD*\User1 • \\10.10.10.10*AD*\User1 • \\10.10.10.10*****\User2 • \\10.10.10.10*AD\User1 • \\10.10.10.10*AD*\User* • \\10.10.10.10*AD**User1* • \\10.10.10.10*AD** • \\10.10.10.10*AD**User1 • \\10.10.10.10\?AD?***\User1

Feature	Valid pattern	Invalid pattern
		• \\10.10.10.10\?***?***\User1 • \\10.10.10.10\Test1\User**? • \\10.10.10.10?AD?***\User1 • \\10.10.10.10?AD?*\User1
Monitor File Changes	• *:\Test1\Test2\Test.txt • ?:\Test1\Test2\Test.txt • *\Test1\Test2\Test.txt • ?\Test1\Test2\Test.txt • *:\Test1**\Test.txt • C:\Test1**\Test.txt • C:\Test1****\Test.txt • C:\Test1*****\Test.txt • C:\Test1**.txt • C:**\Test.txt • C:*\Test.txt • C:**.txt • C:\Test1\?\?\Test.txt • C:\Test1\?\???\Test.txt • C:\Test1\?????\Test.txt • C:\Test1\?\?.txt • C:\?\?\Test.txt • C:\?\Test.txt • C:\?\?.txt • C:\Test1\Test2\Test.? • C:\Test*\Test1\Test.txt • C:\Test?\Test1\Test.txt • C:\Test*\Test1*\Test.txt • C:\Test?\Test1?\Test.txt • C:\Test\Test????? • C:*Test\Test1\Test.txt • C:\?Test\Test1\Test.txt • C:*Test?\Test1\Test.txt • C:\?Test*\Test1\Test.txt • C:*Test?QA\Test1\Test.txt • C:\?Test*QA\Test1\Test.txt	• C:\Test1\Test2\Test.* • C:\Test**** • C:\Test\????? • C:\Test*.* • C:\Test\?.? • C:\Test\Test**** • C:*? • C:\?* • Test\Test1*\Test.txt • Test\Test1*\Test.* • Test\Test1*\Test.?
Monitor Process	• *:\Test1\Test2\Test.exe • ?:\Test1\Test2\Test.exe	• C:\Test1\Test2\Test.* • C:\Test****

Feature	Valid pattern	Invalid pattern
	• *\Test1\Test2\Test.exe • ?\Test1\Test2\Test.exe • *:\Test1**\Test.exe • C:\Test1**\Test.exe • C:\Test1****\Test.exe • C:\Test1*****\Test.exe • C:\Test1**.exe • C:**\Test.exe • C:*\Test.exe • C:**.exe • C:\Test1\?\?\Test.exe • C:\Test1\?\???\Test.exe • C:\Test1\?????\Test.exe • C:\Test1\?\?.exe • C:\?\?\Test.exe • C:\?\Test.exe • C:\?\?.exe • C:\Test1\Test2\Test.? • C:\Test*\Test1\Test.exe • C:\Test?\Test1\Test.exe • C:\Test*\Test1*\Test.exe • C:\Test?\Test1?\Test.exe • C:\Test\Test????? • C:*Test\Test1\Test.exe • C:\?Test\Test1\Test.exe • C:*Test?\Test1\Test.exe • C:\?Test*\Test1\Test.exe • C:*Test?QA\Test1\Test.exe • C:\?Test*QA\Test1\Test.exe • Test\Test1*\Test.exe • Test\Test1*\Test.?	• C:\Test\????? • C:\Test*.* • C:\Test\?.? • C:\Test\Test**** • C:*? • C:\?* • Test\Test1*\Test.*
Updaters	• C:\Test1**\Test.exe • C:\Test1****\Test.exe • C:\Test1*****\Test.exe • C:\Test1**.exe • C:**\Test.exe • C:*\Test.exe • C:\Test1\Test2\Test.* • C:\Test1\?\?\Test.exe	• *:\Test1\Test2\Test.exe • ?:\Test1\Test2\Test.exe • *\Test1\Test2\Test.exe • ?\Test1\Test2\Test.exe • *:\Test1**\Test.exe • C:**.exe • C:\Test1\?\?.exe • C:\Test1\Test2\Test.?

Feature	Valid pattern	Invalid pattern
	• C:\Test1\?\???\Test.exe • C:\Test1\?????\Test.exe • C:\?\?\Test.exe • C:\?\Test.exe • C:\?\?.exe • C:\Test*\Test1\Test.exe • C:\Test?\Test1\Test.exe • C:\Test*\Test1*\Test.exe • C:\Test?\Test1?\Test.exe • C:*Test\Test1\Test.exe • C:\?Test\Test1\Test.exe • C:*Test?\Test1\Test.exe • C:\?Test*\Test1\Test.exe • C:*Test?QA\Test1\Test.exe • C:\?Test*QA\Test1\Test.exe • Test\Test1*\Test.exe	• C:\Test**** • C:\Test\????? • C:\Test*.* • C:\Test\?.? • C:\Test\Test**** • C:\Test\Test????? • C:*? • C:\?* • Test\Test1*\Test.* • Test\Test1*\Test.?

Define bypass rules

Define specific rules in a policy to bypass applied memory-protection and other techniques.

Some applications (as part of their day-to-day processing) run code in an atypical way and hence are prevented from running. To allow such applications to run, define appropriate bypass rules. A bypassed file or application is no longer considered by the memory-protection features of Application Control.

Task

1. On the McAfee ePO console, perform one of these actions.
    - Create an Application Control policy or rule group.
    - Create an Application Control policy (to apply bypass rules to one endpoint).
2. Select the **Exclusions** tab.
3. Click **Add** to open the **Add exclusion rules** dialog box.
4. Expand nodes for the options where you want to add bypass rules.
    - **Memory protection**
    - **Installation detection**
    - **Advanced options**
5. (Optional) Select the **Memory protection** options where you want to add bypass rules, then provide the needed information.

- **Disable buffer overflow protection (CASP) for a process** — Specify a process in the **Process Name** field to bypass the process from the Critical Address Space Protection (CASP) technique.
- **Disable buffer overflow protection (NX) for a process on 64-bit Windows** — Specify a process in the **Process Name** field to bypass the process from the No eXecute (NX) technique. Select **Enable Inheritance** to bypass child processes started by the file from the No eXecute (NX) technique.
- **Disable ROP protection for a process using Forced Relocation (VASR)** — Specify a process in the **Process Name** field to bypass the process from the VASR Forced-Relocation technique. Optionally, specify the name of the DLL file associated with the process in the **Library Name** field.
- **Disable ROP protection for a DLL using DLL Relocation (VASR)** — Specify a DLL file in the **Library Name** field to bypass the DLL file from the VASR DLL Relocation technique. The file isn't rebased and is loaded from its preferred base address.
- **Disable ROP protection for a process using Stack Randomization (VASR)** — Specify a process in the **Process Name** field to bypass the process from the VASR Process Stack Randomization technique.

6. (Optional) Select **Allow uninstallations** and provide the needed information.
7. (Optional) Select **Advanced options** where you want to add bypass rules, then provide the needed information.
   - **Exclude file from write-protection rules and allow script execution** — Specify a process in the **Process Name** field to bypass the process from write protection rules and also allow execution for a script file using the Process Context File Operations bypass technique. Optionally, specify the name of the parent process in the **Parent Process Name** field to allow the file to bypass only if it is launched by the specified parent.
   - **Ignore path for file operations** — Specify a relative path in the **Relative Path** field to ignore the relative path for file operations using the `skiplist -i` command.
   - **Exclude path from file operations** — Specify a relative path in the **Relative Path** field to bypass the relative path from file operations using the `skiplist -f` command.
   - **Exclude path from write-protection rules**, specify a relative path in the **Relative Path** field to bypass the relative path from file write protection rules using the `skiplist -d` command.
   - **Exclude local path and all its contained files and sub-directories from the whitelist**, specify a local path in the **Path** field to bypass the local path and all its contained files and subdirectories from the whitelist using the `skiplist -s` command.
   - **Exclude volume from Application Control protection**, specify a volume in the **Volume** field to bypass the volume from Application Control protection using the `skiplist -v` command. This option detaches the specified volume from the whitelist and the volume is not protected by Application Control.
8. Click **OK** to apply the rules.

Important

Contact McAfee Support before applying these exclusions.

Using monitoring rules

What can you monitor?

You can monitor files, directories, registry keys, users, and programs.

Element	Tracked operations
File	• File creation • File change (file content and attributes, such as permissions, owner, or group) • File deletion • File rename • Alternate Data Stream creation • Alternate Data Stream change (content and attributes, such as permissions or owner) • Alternate Data Stream deletion • Alternate Data Stream rename
Process	• Process start • Process stop
Registry key	• Registry key creation • Registry key change • Registry key deletion
User account	• User account creation • User account change • User account deletion • User logon (success and failure) • User logoff **Note:** User account tracking is disabled by default. You must enable this feature to track operations for user accounts. To enable this feature, execute the **SC: Run Commands** client task to run the `sadmin features enable mon-uat` command on the endpoint.

Note

Change Control includes predefined monitoring rules.

Order of precedence for monitoring rules

This is the order of precedence applied (highest to lowest) when processing monitoring rules.

1. Advanced exclusion filters (AEF) rules
2. Exclude rules
3. Rules based on user name
4. Rules based on program name
5. Rules based on file extension
6. Rules based on file names or paths

Framework to define monitoring rules

Regardless of whether you create a monitoring policy or define a monitoring rule group, the framework available to define monitoring rules is the same.

System variables

The path specified in a monitoring rule can include system environment variables. This table lists the supported system variables.

Variable	Example value (for most Windows platforms)
%ALLUSERSPROFILE%	C:\ProgramData C:\Documents and Settings\All Users (in earlier Windows versions)
%APPDATA%	C:\Users\(username)\AppData\Roaming C:\Documents and Settings\{username}\Application (in earlier Windows versions)
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES (x86)%	C:\Program Files (x86)\Common Files
%HOMEDRIVE%	C:
%HOMEPATH%	C:\Users\(username) C:\Documents and Settings\{username} or \ (in earlier Windows versions)
%PROGRAMFILES%	C:\Program Files
%PROGRAMFILES (x86)%	C:\Program Files (x86) (only in 64-bit versions)

Variable	Example value (for most Windows platforms)
%SYSTEMDRIVE%	C:
%SYSTEMROOT%	C:\Windows (C:\WINNT in earlier Windows versions)
%TEMP% (system) %tmp% (user)	C:\Users\(username)\AppData\Local\Temp C:\Documents and Settings\{username}\local Settings\Temp (in earlier Windows versions) C:\Temp (in earlier Windows versions)
%USERPROFILE%	C:\Users\(username) C:\Documents and Settings\{username} (in earlier Windows versions) C:WINNT\profiles\{username}(in earlier Windows versions)
%WINDIR%	C:\Windows

These considerations apply to path-based rules.

- Paths must be absolute when specifying rules to monitor files and directories.
- Paths aren't required to be absolute when specifying rules to monitor program activity. You can specify the partial path, such as AcroRd32.exe or Reader\AcroRd32.exe or fully qualified path, such as C:\Program Files\Adobe\Reader 9.0\Reader \AcroRd32.exe. If you specify the partial path, all programs with names that match the specified string are monitored. If you specify the fully qualified path, activity is monitored for only the specified program.
- Paths can contain white spaces.
- Paths can include the wildcard character (*). But, it can only represent one complete path component. Here are a few examples.
    - Using \abc*\def is allowed while \abc*.doc, \abc*.*, or \abc\doc.* are not supported.

Note

You can't use the wildcard character while defining a rule to track content and attribute changes for a file.

- Paths used in registry key-based rules can include the wildcard character (*). But, the wildcard character can only represent one path component in the registry path. Make sure that you don't use the character for the component at the end of the complete registry path.

Also, at any time, the CurrentControlSet in the Windows Registry is linked to the relevant HKEY_LOCAL_MACHINE\SYSTEM\ControlSetXXX key. For example, the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet can be linked to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001 key. When a change is made to either link, it is automatically updated on both links. For a monitored key, events are always reported with the path of CurrentControlSet and not ControlSetXXX.

Create or change monitoring rules

You can perform these actions when creating or changing a monitoring policy or rule group.

Task

1. Monitor files and directories.
   a. On the **File** tab, click **Add**.
   b. In the **Add File** dialog box, specify the file or directory name.
   c. Indicate whether to include or exclude from monitoring.
   d. (Optional) To track content and attribute changes for a file, select **Enable Content Change Tracking**.
   e. Click **OK**.
2. Monitor specific file types.
   a. On the **Extension** tab, click **Add** to open the **Add Extension** dialog box.
   b. Type the file extension. Don't include the period (dot) in the extension. For example, log.
   c. Indicate whether to include or exclude from monitoring and click **OK**.
3. Monitor program activity.
   You can choose to track or not track file changes made by a specific program.
   a. On the **Program** tab, click **Add** to open the **Add Program** dialog box.
   b. Enter the name or full path of the program.
   c. Indicate whether to include or exclude from monitoring and click **OK**. We recommend that you exclude background processes, such as the lsass.exe process.
4. Choose users you don't want to monitor.
   All changes made by this user aren't tracked.
   a. On the **User** tab, click **Add** to open the **Add User** dialog box.
   b. Specify the user name.
   c. Click **OK**.
5. Specify advanced exclusion filters for events.
   a. On the **Filters** tab, click **Add Rule** to add a filter row. You can create filters based on files, events, programs, registry keys, and users.
   b. Edit the settings to specify the filter.
   c. Click **+** or **Add Rule** to specify additional `OR` conditions or `AND` conditions.
6. Monitor registry keys.
   a. On the **Registry** tab, click **Add** to open the **Add Registry** dialog box.
   b. Specify the registry key.
   c. Indicate whether to include or exclude from monitoring and click **OK**.
7. Review predefined monitoring rules.

a. Select **Menu** → **Policy** → **Policy Catalog**.
b. Select the **Solidcore 8.x.x: Integrity Monitor** product.
c. Open the relevant **Minimal System Monitoring** policy.
d. Select a rule group in the **Rule Groups** pane to review the filters included in the rule group, then click **Cancel**.

By default, these filters are applied to the global root in the System Tree and are inherited by all McAfee ePO-managed endpoints where Change Control is installed.

Create monitoring policies

You can control monitoring of files, directories, registry keys, file types (based on file extension), programs, and users.

To create a monitoring policy, you can define rules in a rule group and add the rule group to a policy. You can also define the rules directly in a policy. You can also assign multiple policies to one node in the **System Tree**.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.x.x: Integrity Monitor** product.
3. Click **New Policy** to open the **Create a new policy** dialog box and select the category.
4. Select **Blank Template** from **Create a policy based on this existing policy** list to define a policy from scratch, specify the policy name, then click **OK**.
5. Click the policy name to open the **Policy Settings** page.
6. Add a rule group to the policy.
   a. Click **Add** in the **Rule Groups** pane to open the **Select Rule Groups** dialog box.
   b. Select the rule group to add.
   c. Click **OK**.
   d. Select the rule group in the **Rule Groups** pane.
      The rules included in the rule group are displayed in the various tabs.
   e. Review the rules.
7. Add the monitoring rules to the policy, then save the policy.

Configure settings for tracking content changes

You can track content and attribute changes by configuring these settings.

Setting	Description
Maximum file size	By default, you can track changes for any file with a size of 1000 KB or lower. You can also configure the maximum file size for tracking content changes.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td></td><td>Note: Changing the maximum file size affects the McAfee ePO database sizing requirements and might have an impact on performance.</td></tr>
<tr><td rowspan="3">File extensions for which to track only attribute changes</td><td colspan="2">For executable files, the content change tracking feature tracks only attributes (content changes aren't tracked). By default, only attribute changes are tracked for these extensions.</td></tr>
<tr><td>zip
bmp
7z
pdf
rar
tar
gz
bz
tgz</td><td>bz2
jpg
exe
gif
dll
tiff
sys
png
jar</td></tr>
<tr><td colspan="2">You can edit the list to specify file extensions specific to your setup for which to track only attribute changes.</td></tr>
<tr><td>Maximum number of files to retrieve per rule</td><td colspan="2">When you apply the content change tracking rule on a directory, base versions of all files in the directory that match the specified include or exclude patterns, if any, are collected and sent to the McAfee ePO server. These base versions are used to track content changes and allow comparison with future versions of the files.

If the number of qualifying files for one rule is too high, operational performance of the endpoint and occasionally of the McAfee ePO server can deteriorate. To prevent such disruptions, you can specify a value to control the maximum files to retrieve per rule. This limit applies to the number of qualifying files in the directory and not to the total number of files in the directory. If the number of qualifying files for a specified rule exceeds the set threshold value, the base versions of the files aren't retrieved to the server. All subsequent changes to the files are reported and base versions of new files are sent to the server.

By default, the limit is set to 100 files per rule. You can configure this setting, as needed.</td></tr>
</table>

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.x.x: General** product.
   The **McAfee Default** policy includes customizable configuration settings.
3. In the **Configuration (Client)** category, click **Duplicate** for the **McAfee Default** policy.
4. Specify the policy name, then click **OK**.
   The policy is created and listed on the **Policy Catalog** page.
5. Click the new policy.
6. Switch to the **Miscellaneous** tab and specify values for the settings.
7. Save the policy and apply it to the relevant endpoints.

Track content changes

When you create or change a monitoring (Integrity Monitor) policy or rule group, you can specify the files for which to track content changes.

Task

1. Navigate to the **File** tab.
2. Perform one of these steps.
   - Click **Add** to monitor and track changes for a new file.
   - Select an existing rule and click **Edit**.
3. Review or add the file information.
4. Select **Enable Content Change Tracking**.
5. Select the file encoding.
   You can choose **Auto Detect**, **ASCII**, **UTF-8**, and **UTF-16**. **Auto Detect** works for most files. If you are aware of the file encoding, select **ASCII**, **UTF-8**, or **UTF-16** (as appropriate). If needed, you can add new file encoding values. Contact McAfee Support for assistance in adding a file encoding value.
6. Track content changes for files in a directory.
   a. Select **Is Directory**.
   b. Select **Recurse Directory** to track changes for files in all subdirectories of the specified directory.
   c. (Optional) Specify patterns to match file names in the **Include Patterns** or **Exclude Patterns**. While specifying multiple patterns, make sure that each pattern is on a separate line.
   If you do not specify a pattern, all files are included for change tracking. You can add an asterisk (*****) at the beginning or end of a pattern. If you specify *.txt as an include pattern, only txt files in the directory are monitored. If you specify *.ini as an exclude pattern, all ini files in the directory are not monitored. Also, while specifying multiple patterns, make sure that each pattern is on a separate line. For example:

   *.log

   Test.txt

Test*

If you erroneously add *.log and Test.txt in one line, the software considers it as a single pattern and matches accordingly.

Note

Exclude patterns take precedence over include patterns. For example, if you erroneously define an include and exclude pattern for the same file, the exclude pattern applies.

7. Click **OK**.

Manage file versions

You can review all versions available for a file, compare file versions, reset the base version, and delete versions.

The base version identifies the starting point or initial document to use for comparison or control. Typically, the oldest version of a file is set as the base version. When you start tracking changes for a file, the initial file content and attributes are stored on the McAfee ePO database and set as the base version.

Task

1. On the McAfee ePO console, select **Menu** → **Reporting** → **Content Change Tracking**.
   All files for which content change tracking is enabled are listed.
2. Identify the file for which you want to review versions.
   - In the **Quick find** text box, specify the endpoint or file name, then click **Apply**. The list is updated based on the specified search string.
   - Sort the list based on the system name, file path, or status.
3. Perform file operations.
   a. Check the **File Status** column to review the content change tracking status.
   b. Select **View versions** to view all versions of the file.
   c. On the **File Versions** page, you can compare file versions.
      You can perform one of these actions:
      - Select **Compare with previous** versions.
      - Select **Compare with base** version.
      - Choose any two versions, then select **Actions** → **Compare Files**.
      - Select **Advanced File Comparison** to compare two specific files by providing their group, host, and versions.
   d. To reset the base version, choose a version, select **Actions** → **Set as base version** to open the **Set as base version** dialog box, then click **OK**.
      This resets the base version and deletes all previous versions (older than the new base version) of the file.
   e. To delete file versions, select **Actions** → **Delete**, then click **OK**.

Note

The software can track up to 200 versions for a file. If the number of versions exceeds 200, the application deletes the oldest versions to bring the version count to 200. Then, it automatically sets the oldest version as the base version. If needed, you can configure the number of versions to maintain for a file. For more information, contact McAfee Support.

Using protection rules

What are protection rules?

You can define read protection and write protection rules to prevent unauthorized data access and changes.

Read protection rules prevent users from reading the content of files, directories, and volumes. When a directory or volume is read-protected, all files in it are read-protected. Any unauthorized attempt to read data from protected files is prevented and an event is generated. Writing to read-protected files is allowed.

Note

You cannot define read protection rules for registry keys.

Write protection rules prevent users from creating and changing existing files, registry keys, and directories. When a directory is included for write protection, all files in that directory and its subdirectories are write protected.

Note

You can also define additional rules to override the read or write protection that is in effect. You can choose programs or users to override read or write protection.

Order of precedence for protection rules

These considerations are used when protection rules are applied at the endpoint.

- Exclude rules are given precedence over include rules.

  For example, if you erroneously define an include and exclude rule for the same file, the exclude rule applies.

- Longer paths are given precedence.

  For example, if C:\temp is included for write protection, and C:\temp\foo.cfg is excluded, the changes to foo.cfg are permitted. Similarly, if you exclude the HKEY_LOCAL_MACHINE key and include the HKEY_LOCAL_MACHINE\System key for write protection, the changes to the HKEY_LOCAL_MACHINE\System key are prevented.

System variables

The path specified in a protection rule can include system environment variables. This table lists the supported system variables.

Variable	Example value (for most Windows platforms)
%ALLUSERSPROFILE%	C:\Documents and Settings\All Users
%APPDATA%	C:\Documents and Settings\{username}\Application
%COMMONPROGRAMFILES%	C:\Program Files\Common Files
%COMMONPROGRAMFILES (x86)%	C:\Program Files (x86)\Common Files
%HOMEDRIVE%	C:
%HOMEPATH%	C:\Documents and Settings\{username} or \ (for earlier Windows versions)
%PROGRAMFILES%	C:\Program Files
%PROGRAMFILES (x86)%	C:\Program Files (x86) (only in 64-bit versions)
%SYSTEMDRIVE%	C:
%SYSTEMROOT%	C:\windows (C:\WINNT in earlier Windows versions)
%TEMP% (system) %tmp% (user)	C:\Documents and Settings\{username}\local Settings\Temp C:\Temp
%USERPROFILE%	C:\Documents and Settings\{username} (C:WINNT\profiles\{username} in earlier versions)
%WINDIR%	C:\Windows

Path considerations

These considerations apply to path-based rules.

- Paths must be absolute when specifying rules to read-protect or write-protect files and directories.

- Paths don't need to be absolute when specifying rules to add a trusted program or updater. For example, you can specify the partial path, such as AcroRd32.exe or Reader\AcroRd32.exe or fully qualified path, such as C:\Program Files\Adobe \Reader 9.0\Reader\AcroRd32.exe. If you specify the partial path, all programs with names that match the specified string are added as trusted programs. If you specify the fully qualified path, only the specified program is added as a trusted program.
- Paths can contain white spaces.
- Paths can include the wildcard characters to specify file paths and file names. When using wildcards, make sure that specified string matches a limited set of file paths or file names. If the specified string matches many files, we recommend you revise the string.
    - Paths can include the ***** and **?** wildcard characters.

    When specifying a file path, C:\Test1**\Test.txt, C:\Test\????*?, and C:\?Test*\Test1\Test.txt are allowed while *: \Test1**\Test.txt, *\Test1\Test2\Test.txt, and *:\Test1\Test2\Test.txt are not.

- Paths used in registry key-based rules can include the wildcard character (*). But, the wildcard character can only represent one path component in the registry path. Make sure that you don't use the character for the component at the end of the complete registry path (if used at the end, the rule is not effective).

Apply protection rules

You can define protection rules when changing or creating a protection policy or rule group.

Task

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. Select **Solidcore 8.x.x: Change Control** for the product.
   You can create a policy or duplicate an existing one.
3. Read-protect files and directories.
    a. Select a policy from the list, then click **Add** on the **Read-Protect** tab. The **Add File** dialog box appears.
    b. Specify the file or directory name and indicate whether to include or exclude from read protection.
    c. Click **OK**.
4. Write-protect files and directories.
    a. Select a policy from the list, then click **Add** on the **Write-Protect File** tab. The **Add File** dialog box appears.
    b. Specify the file or directory name and indicate whether to include or exclude from write protection.
    c. Click **OK**.
5. Write-protect registry keys:
    a. Click **Add** on the **Write-Protect Registry** tab. The **Add Registry** dialog box appears.
    b. Specify the registry key and indicate whether to include or exclude from write protection.
    c. Click **OK**.
6. Specify trusted programs permitted to override the read and write protection rules.
    a. Click **Add** on the **Updater Processes** tab. The **Add Updater** dialog box appears.

b. Specify whether to add the updater based on the file name, SHA-1, or SHA-256. If you add the updater by name, it isn't authorized automatically. But, when you add the updater by SHA-1 or SHA-256, the updater is authorized.
c. Enter the location of the file (when adding by name), SHA-1, or SHA-256 of the executable file.
d. Enter a unique identification label for the executable file. For example, if you specify **Adobe Updater Changes** as the identification label for the Adobe_Updater.exe file, all change events made by the Adobe_Updater.exe file are tagged with this label.
e. Specify conditions that the file must meet to run as an updater:
    - Select **None** to allow the file to run as an updater without any conditions.
    - Select **Library** to allow the file to run as updater only when it has loaded the specified library. For example, when configuring iexplore.exe as an updater to allow Windows Updates using Internet Explorer, specify wuweb.dll as the library. This makes sure that the iexplore.exe program has updater rights only until the Web Control library (wuweb.dll) is loaded.
    - Select **Parent** to allow the file to run as an updater only if it is started by the specified parent. For example, when configuring updater.sh as an updater to allow changes to Mozilla Firefox, specify firefox as the parent. Although updater.exe is a generic name that can be part of any installed application, using the parent makes sure that only the correct program is allowed to run as an updater.
f. Indicate whether to disable inheritance for the updater. For example, if Process A (that is set as an updater) starts Process B, disabling inheritance for Process A makes sure that Process B doesn't become an updater.
g. Indicate whether to suppress events generated for the actions performed by the updater. Typically, when an updater changes a protected file, a `File Modified` event is generated for the file. If you select this option, no events are generated for changes made by the updater.
h. Click **OK**.

7. Specify users permitted to override the read and write protection rules.
    a. On the **Users** tab, click **Add**. The **Add User** dialog box appears.
    b. On the **Add User** dialog box, create two rules for each user: one with UPN/SAM and domain account name (in *domainName\user* format) and another with domain netbiosName (in *netbiosName\user* format).
    c. Specify a unique identification label for the user. For example, if you specify **John Doe Changes** as the identification label for the John Doe user, all changes made by the user are tagged with this label.
    d. Type the user name, then click **OK**.

Create a protection policy

Protection policies are multi-slot policies so you can assign multiple policies to one node in the System Tree.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.x.x: Change Control** product.
3. Click **New Policy** to open the **Create a new policy** dialog box.
4. Select the category.
5. Select **Blank Template** from **Create a policy based on this existing policy** list to define a policy from scratch.

6. Specify the policy name, then click **OK** to save the policy.
7. Click the policy and specify protection rules.

Note

The read-protect feature is disabled by default. To use read protection rules, enable the feature for the endpoints.

Enable read protection

By default, the read-protect feature is disabled for optimal system performance. Run a command on the endpoint to enable read protection.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Perform one of these actions.
   - Group — Select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
   - Endpoint — Select the endpoint on the **Systems** page and click **Actions** → **Agent** → **Modify Tasks on a Single System**.

   a. Click **Actions** → **New Client Task Assignment**.
   The **Client Task Assignment Builder** page appears.
   b. Select the **Solidcore 8.x.x** product, **SC: Run Commands** task type, and click **Create New Task**.
   The **Client Task Catalog** page appears.
   c. Specify the task name and add any descriptive information.
3. Type this command.

   ```
   features enable deny-read
   ```
4. Select **Requires Response** if you want to view the status of the commands in **Menu** → **Automation** → **Solidcore Client Task Log** tab.
5. Click **Save**, then **Next** to open the **Schedule** page.
6. Specify scheduling details, then click **Next**.
7. Review and verify the task details, then click **Save**.
8. (Optional) Wake up the agent to send your client task to the endpoint immediately.

Using execution control rules in a standalone environment

Defining attribute-based rules for file execution

Application Control performs multiple checks to determine whether to allow or block a file's execution. If a file's execution is allowed after the Application Control checks, attribute-based or granular rules, if any are defined, come into play. The rules are based on the concept of fine-grained whitelisting and can be created on the attributes of a file.

Note

This feature is also known as Execution Control and it is enabled by default. To disable this feature, use this command: `sadmin features disable execution-control`

You can define specific rules using one or more attributes to allow, block, or monitor the file. Rules that allow execution take precedence over rules that block or monitor execution.

Attribute-based rules help you allow or block files in different scenarios based on file context and offer flexibility.

- Context-based allowing or blocking of files — On a protected system, only whitelisted interpreters are allowed to execute. But, in certain scenarios, whitelisted interpreters might be misused to execute malicious scripts. For example, a powershell.exe script can be used to execute unsolidified scripts and execute file-less scripts by invoking its execution with atypical input arguments. You can prevent misuse of interpreters by defining attribute-based rules to block potentially malicious scenarios.
- Flexibility and control — Attribute-based rules provide flexibility to allow or block file execution, as needed. You might need to block a user from running a specific file. If an administrator wants to block the execution of powershell.exefor a specific user, a rule can be added to prevent its execution. You can achieve such scenarios using attribute-based rules.

  Similarly, you might choose to block execution of a certain file in your setup completely, unless when run by a specific parent process. You can achieve this by creating a generic block rule and a parent process-based allow rule for the file. Because the allow rule has precedence over the block rule, it overrides the block rule when applied.

  Or, you might choose to only observe or monitor a file to determine its execution in your setup. To do this, you can define a monitor rule for the file.

  Note

  We recommend that before creating a block rule for a file, create a monitor rule to observe the file's use and execution in your setup. After you define the monitoring rule, if no **OBSERVED_FILE_EXECUTION** events are generated for the file over a reasonable time window, you can safely define a block rule for a file.

When configuring an attribute-based rule, you can choose to allow, block, or monitor a file. This table describes the behavior of a rule in various supported modes.

Type of rule	Enable	Update
Allow	• Allow file execution. • No event is generated.	• Allow file execution. • No event is generated.
Block	• Block file execution.	• Allow file execution. • The **OBSERVED_FILE_EXECUTION** event is generated.

Type of rule	Enable	Update
	• The **PREVENTED_FILE_EXECUTION** event is generated.	
Monitor	• Allow file execution. • The **OBSERVED_FILE_EXECUTION** event is generated.	• Allow file execution. • The **OBSERVED_FILE_EXECUTION** event is generated.

Note

The applied rules are ineffective when any process is selected as an updater. Only the events are generated.

Add attribute-based rules

You can create rules based on one or more attributes of a file to allow, block, or monitor its execution.

Task

1. Enter the command with attribute type as command_line:
   - `sadmin ruleengine add <ruletype> processname command_line <operation> <REGEX/STRING>`

   This table describes the command's tokens and their functionality.

Token	Possible values	Description
Ruletype	• allow • block • monitor	Allows you to create a rule to allow, block or monitor execution.
Attributetype	• command_line	Defines the `command_line` argument with which a process is launched. The attribute-based rule can be formed on it for decision making in the rule engine.
Operation	• matches • notmatches • equals • notequals	Performs the rule based on operation configured on the attribute of a process. Only `matches` and `notmatches` support REGEX. For others, string is used.

Token	Possible values	Description
REGEX	A regular expression	Includes a regular expression or a string of characters. It describes a grammar that can be constructed based on ECMA script.
STRING	Any characters	Defines a string of characters.

2. Enter the command with attribute type as parent_process_name, user, or path:
   - `sadmin ruleengine add <ruletype> processname <attributetype> <operation> STRING`

   This table describes the command's tokens and their functionality.

Token	Possible values	Description
Ruletype	• allow • block • monitor	Allows you to create a rule to allow, block or monitor execution.
Attributetype	• user • parent_process_name • path	Defines the attribute type on which attribute-based rules can be formed for decision making in the rule engine.
Operation	• equals • notequals	Performs the rule based on operation configured on the attribute of a process.
STRING	Any characters	Defines a string of characters.

You can use multiple attributes when creating attribute-based rules. Use **AND** as a connector while creating a rule based on two or more attribute types. For example, `sadmin ruleengine add block powershell.exe command_line matches .*iex* AND user equals "user1"` rule prevents user1 from running powershell.exe when run with command-line argument that matches regex *iex* in this case. In other scenarios, user1 is allowed to execute powershell.exe.

Remove attribute-based rule

You can remove attribute-based rules defined on the system.

Task

1. Remove one rule with attribute type as command_line:
   - `sadmin ruleengine remove <ruletype> processname command_line <operation> <REGEX/STRING>`

   This table describes the command's tokens and their functionality in detail.

Token	Possible values	Description
Ruletype	• allow • block • monitor	Allows you to create a rule to allow, block, or monitor execution.
Attributetype	• command_line	Defines the `command_line` argument with which a process is started. The attribute-based rule can be formed on it for decision making in the rule engine.
Operation	• matches • notmatches • equals • notequals	Performs the rule based on operation configured on the attribute of a process. Only `matches` and `notmatches` support REGEX. For others, string is used.
REGEX	A regular expression	Includes a regular expression or a string of characters. It describes a grammar that can be constructed based on ECMA script. See this article for more details.
STRING	Any characters	Defines a string of characters.

2. Remove one rule with `parent_process_name`, `path`, or `user` attribute type:
   - `sadmin ruleengine remove <ruletype> processname <attributetype> <operation> STRING`

   This table describes the command's tokens and their functionality.

Token	Possible values	Description
Ruletype	• allow • block • monitor	Allows you to create a rule to allow, block, or monitor execution.
Attributetype	• user • parent_process_name • path	Defines the attribute type on which attribute-based rules can be formed for decision making in the rule engine.
Operation	• equals • notequals	Performs the rule based on operation configured on the attribute of a process.
STRING	Any characters	Defines a string of characters.

You can use multiple attributes when creating attribute-based rules. Use **AND** as a connector while creating a rule based on two or more attribute types. For example, `sadmin ruleengine remove block powershell.exe command_line matches .*iex* AND user equals "user1"` rule removes the rule that is preventing user1 from running powershell.exe when run with command-line argument that matches regex.`*iex*` in this case.

3. Remove or flush all attribute-based rules defined on the system:
    - `sadmin ruleengine flush`

View attribute-based rules

You can view all attribute-based rules added to your system.

Task

Run this command at the command prompt.

`sadmin rulengine list`

Using certificates with McAfee ePO

What are certificates?

Application Control allows trusted certificates that are associated with software packages to run on a protected system.

After you add a certificate as a trusted or authorized certificate, you can run all software, signed by the certificate on a protected system without entering Update mode. For example, if you add Adobe's code-signing certificate, all software issued by Adobe and signed by Adobe's certificate are allowed to run.

Note

Application Control supports only X.509 certificates.

To allow in-house applications to run on protected systems, you can sign the applications with an internal certificate and define the internal certificate as a trusted certificate. After you do so, all applications signed by the certificate are allowed.

You can also provide updater permissions to the certificate. All applications and binary files that are either added or changed on a system and signed by a certificate that has the updater permissions are automatically added to the whitelist. Use this option carefully because it makes sure that all executable files signed by the certificate acquire updater rights.

Add certificates with McAfee ePO

You can add a certificate before defining rules to permit installation and execution of software signed by the certificate.

To add a certificate, you can follow one of these actions:

- Upload an existing certificate.
- Extract certificates from signed executable files on a network share.
- Schedule a server task to routinely extract certificates from signed executable files on a network share.

Task

1. Upload an existing certificate.
    a. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
    b. On the **Certificates** tab, select **Actions** → **Upload** to open the **Upload Certificate** page.
    c. Browse to and select the certificate file to import, then click **Upload**.
2. Extract certificates.
    a. Select **Menu** → **Configuration** → **Solidcore Rules**.
    b. On the **Certificates** tab, select **Actions** → **Extract Certificates** to open the **Extract Certificate from File** page.
    c. Type the path of the file.
    Make sure that the file path is accessible from the McAfee ePO server.
    d. Type your network credentials to access the specified network location.
    e. Click **Extract**.
3. Schedule extraction: You can schedule and regularly extract the certificates associated with signed executable files on a network share.
    a. Select **Menu** → **Automation** → **Server Tasks**.
    b. On the **Server Tasks** page, click **New Task** to open the **Server Task Builder** wizard.
    c. Type the task name, then click **Next**.
    d. From the **Actions** drop-down list, select **Solidcore: Scan a Software Repository**.

e. Specify the Software Repository Path.

Note

All subfolders in the specified path are also scanned for installers and certificates.

f. Type your network credentials to access the specified network location.
g. Click **Test Connection** to make sure that the specified credentials work.
h. Select **Add extracted certificates and installers to Rule Group** to add the certificates and installers extracted by the task to a user-defined rule group and select the user-defined rule group from the list.

Note

You can add extracted certificates and installers only to user-defined rule groups.

i. Click **Next**, specify the schedule for the task, then click **Next**.
j. Review the task summary, then click **Save**.

4. (Optional) Specify an alias or friendly name for a certificate.
   a. Select **Menu** → **Configuration** → **Solidcore Rules**.
   b. On the **Certificates** tab, select a certificate.
   c. Click **Actions** → **Edit** to open the **Edit** window.
   d. Enter the friendly name, then click **OK**.

Search for a certificate

You can add a certificate to permit installation and execution of software signed by the certificate.

You can search for a certificate based on its category.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
2. On the **Certificates** tab, under **Search Certificate**, select a category to sort the listed certificates.
   - **Issued To** — Sorts the list by the name of the organization that publishes the certificate.
   - **Issued By** — Sorts the list by the name of the signing authority.
   - **Extracted From** — Sorts the list by the path of the file from which the certificate was extracted.
   - **Friendly Name** — Sorts the list by the friendly name of the certificate.
3. Type the string to search for and click **Search**.

Verify assignments for a certificate

You can verify if each certificate is assigned to the appropriate policies and rule groups.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
2. On the **Certificates** tab, select a certificate, then click **Actions** → **Check Assignments**.

Results

The **Certificate Assignments** dialog box lists the rule groups and policies where the selected certificate is assigned.

Add a certificate to a policy or rule group

After you add a certificate to McAfee ePO, you can assign it to a policy or rule group. After you add a certificate as trusted or authorized, you can run all software, signed by the certificate on a protected system without entering Update mode.

Task

1. Assign a certificate to a policy by defining a trusted certificate in a policy.
    a. On the **Rule Groups** tab, locate your **Group Name** and under **Actions**, click **Edit**.
    b. On the **Certificates** tab, click **Add**.
    c. Search for and add the certificate.
    d. (Optional) Select **Add Certificate as Updater** to provide updater rights to the certificate.
    e. Click **OK**.
2. Assign a certificate to an existing rule group.
    a. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
    b. On the **Certificates** tab, select the certificates to add to a rule group.
    c. Click **Actions** → **Add to Rule Group** to open the **Add to Rule Group** dialog box.
    d. Select the user-defined rule group for adding the certificates, then click **OK**.

Using certificates in a standalone environment

Add certificates in a standalone environment

You can add certificates as trusted or authorized certificates to run all software signed by those certificates on a protected system.

Note

Application Control supports only X.509 certificates.

Task

Add a certificate:

`sadmin cert add`

Use an existing certificate or extract certificates from one or more signed files. You can extract certificate from any signed file using ScGetCerts.exe (<Install_dir>\Tools\ScGetCerts\ScGetCerts.exe).

Syntax	Description
`sadmin cert add <certificatename>`	Adds a certificate as a trusted certificate. For example: `sadmin cert add mcafee.cer`
`sadmin cert add -c <certificatecontent>`	Use the `-c` argument to specify the certificate content as trusted. For example: `sadmin cert add -c` `MIIFGjCCBAKgAwIBAgIQbwr3oyE8ytuorcGnG3VhpDANBgkqhkiG9w0BAQUFADCB tDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykwNDEuMCwGA1UEAxMl VmVyaVNpZ24gQ2xhc3MgMyBDb2RlIFNpZ25pbmcgMjAwNCBDQTAeFw0wNTEyMTAw MDAwMDBaFw0wNjEyMTAyMzU5NTlaMIHdMQswCQYDVQQGEwJVUzETMBEGA1UECBMK Q2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxIzAhBgNVBAoUGkFkb2JlIFN5 c3RlbXMgSW5jb3Jwb3JhdGVkMT4wPAYDVQQLEzVEaWdpdGFsIElEIENsYXNzIDMg LSBNaWNyb3NvZnQgU29mdHdhcmUgVmFsaWRhdGlvbiB2MjEcMBoGA1UECxQTSW5m b3JtYXRpb24gU3lzdGVtczEjMCEGA1UEAxQaQWRvYmUgU3lzdGVtcyBJbmNvcnBv cmF0ZWQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJcS8Tyuz/JSB6XlyV5Z d02tIo4iZoXANFxbGVXS3Yg4v7zIR8k2K0Tzzpmz3Y00Qr237nTslDnLb4rMx9Fr +DmH1Fq2CwQBCVTnrwbtdUyv2v977Fc05B09WEJvZmvcm22iNrfpCV5wqd7OTp1F qP2HIMa0ihztWAc3R9cn8xPPAgMBAAGjggF/MIIBezAJBgNVHRMEAjAAMA4GA1Ud DwEB/ wQEAwIHgDBABgNVHR8EOTA3MDWgM6Axhi9odHRwOi8vQ1NDMy0yMDA0LWNy bC52ZXJpc2lnbi5jb20vQ1NDMy0yMDA0LmNybDBEBgNVHSAEPTA7MDkGC2CGSAGG +EUBBxcDMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9y cGEwEwYDVR0lBAwwCgYIKwYBBQUHAwMwdQYIKwYBBQUHAQEEaTBnMCQGCCsGAQUF BzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wPwYIKwYBBQUHMAKGM2h0dHA6 Ly9DU0MzLTIwMDQtYWlhLnZlcmlzaWduLmNvbS9DU0MzLTIwMDQtYWlhLmNlcjAf BgNVHSMEGDAWgBQI9VHo+/49PWQ2fGjPW3io37nFNzARBglghkgBhvhCAQEEBAMC BBAwFgYKKwYBBAGCNwIBGwQIMAYBAQABAf8wDQYJKoZIhvcNAQEFBQADggEBAFY7 rAYt9WjCDFQ +YNHfnEZxav3zhGhTdTwqGpWZJh/wg9IgLnyRqMnoQNjDFsSCduxf FryGREMwCHI/ PvEYq7hKZsUXSGWRNl+Auuomg0OFGG1ZlBv/rWtQEbwmGKgtwXMD Dm2IYY3t7O7shG3KW4qHg`

Syntax	Description
	`+Tq04pR8VGTGJodwZWEsj9JavErsujI7SFDMkj9xFz4 VD/ilkWF+AyzSLAyUTq797y/ 7TsG5Y1SeMtze49cVbJVRrbGtq3kSzF56adsA4Hv v2CjM379GkYX0Atro74YLEwcfwdAogZ+F +XtOU9CR48bPvkFP5xMLUJ46HPs1u83 Jk2lrr5OYmtMqd7f0`
`sadmin cert add -u <certificatename>`	Add trusted certificates as updaters using the `-u` argument. For example: `sadmin cert add -u mcafee.cer` ⚠ **Caution:** Selecting this option makes sure that all files signed by a certificate acquire updater rights. For example, if you set the Microsoft certificate that signs the Internet Explorer application as an updater, Internet Explorer can download and execute any application from the Internet. In effect, any file added or modified by an application that is signed by the certificate is added to the whitelist automatically.

Extracting certificates

The ScGetCerts utility extracts a certificate from a file. This utility can also run on systems where the whitelist is not created.

The ScGetCerts utility is shipped with the product and it gets installed in the Application Control installation directory. The default location of ScGetCerts is C:\Program Files\McAfee\Solidcore\Tools\ScGetCerts.

Here is the syntax of the command to extract certificates.

```
scgetcerts.exe [<FILEPATH: filename|directory>] [OUTPUT PATH] [--cab] <-A> <-O> <-n|-c> [<DOMAIN>] [<USERNAME>] [<PASSWORD>]
```

To extract certificate from a file, specify the file path with the file name or the directory path where the file is located. If you specify a directory name, certificate, or installer information, certificates are extracted recursively from all files to the specified directory. Also, specify the output directory path where you want to store the extracted certificates, installer information, or both.

This table describes the supported parameters:

Parameter	Description
--cab	It extracts certificate from a cab file. When you specify the --cab parameter, you must specify the -O parameter with it.

Parameter	Description
-A	It extracts all certificates from a file. By default, only the root certificate is extracted.
-O	Specify this optional parameter if only the certificates are required to be extracted and not the additional information. But, this parameter is not optional if --cab parameter is also specified.
-c	It checks if the path of the file is accessible on the network.
-n	It provides authentication to the directory path on the network. The -n option is specified only when you specify the directory path.

Note

Mention the domain, user name, and password when –n or –c parameter is used.

View certificates

You can view certificates in the Application Control certificate store to verify that the trusted certificates are added to the system.

Task

Run these commands at the command prompt.

Syntax	Description
`sadmin cert list`	Lists the SHA-1 and SHA-256 of certificates that are added as trusted or authorized certificate in the Application Control certificate store.
`sadmin cert list -d`	Lists details of the issuer and subject of the certificates added to the system.
`sadmin cert list -u`	Lists all certificates with updater permissions.

Remove certificates

You can delete certificates from the Application Control certificate store to remove their trusted or authorized status. Such certificates cannot run the software signed by the trusted certificates on a protected system.

Task

Run this command at the command prompt.

```
sadmin cert remove
```

Syntax	Description
`sadmin cert remove <SHA-1 or SHA-256>`	Removes a certificate that is added as a trusted certificate using the SHA-1 or SHA-256 value. Specify the SHA-1 or SHA-256 value of the certificate to remove the certificate from the Application Control certificate store. For example: `sadmin cert remove 7ecf2b6d72d8604cf6217c34a4d9974be6453dff`
`sadmin cert remove –c <certificatecontent>`	Use the –c argument to remove specified certificate content from the Application Control certificate store. For example: `sadmin cert remove –c MIIFGjCCBAKgAwIBAgIQbwr3oyE8ytuorcGnG3VhpDANBgkqhkiG9w0BAQUFADCB tDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykwNDEuMCwGA1UEAxMl VmVyaVNpZ24gQ2xhc3MgMyBDb2RlIFNpZ25pbmcgMjAwNCBDQTAeFw0wNTEyMTAw MDAwMDBaFw0wNjEyMTAyMzU5NTlaMIHdMQswCQYDVQQGEwJVUzETMBEGA1UECBMK Q2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxIzAhBgNVBAoUGkFkb2JlIFN5 c3RlbXMgSW5jb3Jwb3JhdGVkMT4wPAYDVQQLEzVEaWdpdGFsIElEIENsYXNzIDMg LSBNaWNyb3NvZnQgU29mdHdhcmUgVmFsaWRhdGlvbiB2MjEcMBoGA1UECxQTSW5m b3JtYXRpb24gU3lzdGVtczEjMCEGA1UEAxQaQWRvYmUgU3lzdGVtcyBJbmNvcnBv cmF0ZWQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJcS8Tyuz/JSB6XlyV5Z d02tIo4iZoXANFxbGVXS3Yg4v7zIR8k2K0Tzzpmz3Y00Qr237nTslDnLb4rMx9Fr +DmH1Fq2CwQBCVTnrwbtdUyv2v977Fc05B09WEJvZmvcm22iNrfpCV5wqd7OTp1F qP2HIMa0ihztWAc3R9cn8xPPAgMBAAGjggF/MIIBezAJBgNVHRMEAjAAMA4GA1Ud DwEB/ wQEAwIHgDBABgNVHR8EOTA3MDWgM6Axhi9odHRwOi8vQ1NDMy0yMDA0LWNy bC52ZXJpc2lnbi5jb20vQ1NDMy0yMDA0LmNybDBEBgNVHSAEPTA7MDkGC2CGSAGG +EUBBxcDMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9y cGEwEwYDVR0lBAwwCgYIKwYBBQUHAwMwdQYIKwYBBQUHAQEEaTBnMCQGCCsGAQUF BzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wPwYIKwYBBQUHMAKGM2h0dHA6 Ly9DU0MzLTIwMDQtYWlhLnZlcmlzaWduLmNvbS9DU0MzLTIwMDQtYWlhLmNlcjAf BgNVHSMEGDAWgBQI9VHo+/49PWQ2fGjPW3io37nFNzARBglghkgBhvhCAQEEBAMC BBAwFgYKKwYBBAGCNwIBGwQIMAYBAQABAf8wDQYJKoZIhvcNAQEFBQADggEBAFY7 rAYt9WjCDFQ`

Syntax	Description
	`+YNHfnEZxav3zhGhTdTwqGpWZJh/wg9IgLnyRqMnoQNjDFsSCduxf FryGREMwCHI/ PvEYq7hKZsUXSGWRNl+Auuomg0OFGG1ZlBv/rWtQEbwmGKgtwXMD Dm2IYY3t7O7shG3KW4qHg +Tq04pR8VGTGJodwZWEsj9JavErsujI7SFDMkj9xFz4 VD/ilkWF+AyzSLAyUTq797y/ 7TsG5Y1SeMtze49cVbJVRrbGtq3kSzF56adsA4Hv v2CjM379GkYX0Atro74YLEwcfwdAogZ+F +XtOU9CR48bPvkFP5xMLUJ46HPs1u83 Jk2lrr5OYmtMqd7f0`
`sadmin cert flush`	Removes all certificates from the Application Control certificate store.

Using updaters

What are updaters?

Updaters are authorized components that are allowed to make changes to the system.

If a program is configured as an updater, it can install new software and update existing software. By default, if you provide updater rights to a component, the child component automatically inherits the same rights.

Updaters work at a global-level and aren't application-specific or license-specific. When a program is defined as an updater, it can change any protected file.

An updater isn't authorized automatically. To be authorized, an updater must be in the whitelist or given explicit authorization.

⚠ Caution

We advise caution when assigning updater rights to executable files. If you set an executable as an updater and invoke any executable from it, it can perform any change on the protected endpoints.

You can also add scripts as updaters. This feature is called Script as Updaters (SAU) and it gives updater rights to scripts (such as .bat, .vbs, and .py). When enabling Application Control, the SAU feature is available by default after the endpoint is restarted.

Application Control also includes predefined default updater rights for commonly used applications that might need to update the systems frequently. These applications are known as *default updaters*.

Script as Updater feature

If a program is configured as an updater, it can install new software and update existing software. With the Script as Updaters (SAU) feature, you can give updater rights to scripts (such as .bat, .vbs, and .py).

Script as Updater (SAU) and Memory-protection (MP) features are enabled by default. But when you perform a clean installation and enable Application Control, you can permanently disable these features.

Important

These features can be permanently disabled only when installing Application Control in a managed McAfee ePO environment. In standalone mode, the SAU feature is available by default after the endpoint is restarted.

Disabling SAU and MP features in the **Initial Feature configuration** is permanent. You can't enable them again after installation. Any change of MP or SAU status through a policy is ignored by the endpoint.

Permanently disable SAU

When you perform a clean installation and enable Application Control, you can permanently disable Script as Updater (SAU) and Memory-protection (MP) features.

Important

This initial feature configuration is available only in a clean install. If you upgrade from a previous version, the SAU feature is enabled. If after the upgrade you want to disable SAU, you must introduce the change with a policy.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Select a group or an endpoint and go to **Actions** → **Agent** → **Run Client Task Now**.
    a. Under **Product**, Select **Solidcore 8.2.0**.
    b. Under **Task Type**, select **SC: Enable**.
    c. Under **Task Name**, click **Create New Task**.
3. On the **Run Client Task Now** page:
    a. Choose the Platform and Sub Platform.
    b. Under **Enable**, select **Application Control**.
4. For **Initial Feature configuration**, you can select:
    a. MP disabled
    b. SAU disabled
5. Select an option for activation:
    a. Limited Feature Activation
    b. Full Feature Activation
6. (Optional) Select **Start Observe Mode** to place the endpoints in Observe mode.
7. (Optional) Select **Pull Inventory** to manage the inventory with McAfee ePO.
8. Click **Run Task Now**.

Results

Important

Disabling SAU and MP features in the **Initial Feature configuration** is permanent. You can't enable them again after installation. Any change of MP or SAU status through a policy is ignored by the endpoint.

Add feature columns to the System Tree

On McAfee ePO, you can configure the columns on the **System Tree** page to see the status of the features.

You can see the status of the features (SAU, MP, and others) in all endpoints by adding the corresponding feature columns. These columns allow you to filter all endpoints depending on the status of the features.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Select the endpoints and go to **Actions** → **Choose Columns**.
3. On the left pane, go to **Application Control Features Status** and select the columns you want to add to the **System Tree**.
4. Click **Save**.

Disable SAU after upgrading the software

If you upgrade from a previous version, the Script as Updater (SAU) feature is enabled by default. If after the upgrade you want to disable SAU, you must introduce the change with a policy.

Task

1. Go to **Menu** → **Policy** → **Policy Catalog**.
    a. Select the **Solidcore 8.2.0: Application Control** product.
    b. Select **Application Control Options (Windows)** category.
2. Choose **McAfee Default** or **My Default** policy and click **Duplicate**.
3. Once the policy is duplicated, click the name of the policy and go to the **Features** tab.
    a. Select **Enforce feature control from McAfee ePO**.
    b. Select or deselect the features you want to disable.
    c. Click **Save**.
4. To implement the policy, go to **System Tree** and select the endpoint.
5. Go to **Actions** → **Agent** → **Set Policy & Inheritance**.
    a. Select the **Product**, **Category**, and **Policy**.
    b. Click **Save**.
6. Select the endpoint and click **Wake up Agent**.

a. Complete the information on the **Wake Up McAfee Agent** page.
b. Select **Force complete policy and task update**.
c. Click **OK**.

7. Reboot the endpoints to implement the policy.

Manage updaters in a managed environment

If a program is configured as an updater, it can install new software and update existing software. You can add, edit, or remove updaters.

Task

1. Manage updaters in rule groups.
   a. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
   b. Locate the rule group and under **Actions**, click **View**.
   c. On the **Updater Processes** tab, you can **Add**, **Edit**, or **Remove** an updater.
2. Manage updaters in policies.
   a. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
   b. On the **Policy Catalog** page, select the product and category from the list.
   c. Click the selected policy.
3. Complete the addition of an updater to a rule group or policy.
   a. On the **Updater Processes** tab, click **Add**.
   b. Specify whether to add the updater based on the file name, SHA-1, or SHA-256.
      If you add the updater by name, the updater is not authorized automatically. The file must be added to the whitelist.
   c. Enter the location of the file (when adding by name), or the SHA-1 or SHA-256 value of the executable file.
   d. Specify an identification updater label for the program.
   e. When adding an updater by name, specify conditions that the file must meet to run as an updater.
      - Select condition **None** to allow the file to run as an updater without any conditions.
      - Select condition **Library** to allow the file to run as updater only when it has loaded the specified library. For example, when configuring iexplore.exe as an updater to allow Windows Updates using Internet Explorer, specify wuweb.dll as the library. This makes sure that the iexplore.exe program has updater rights only until the web control library (wuweb.dll) is loaded.
      - Select condition **Parent** to allow the file to run as an updater only if it is started by the specified parent. For example, when configuring updater.exe as an updater to allow changes to Mozilla Firefox, specify firefox.exe as the parent. Although updater.exe is a generic name that can be part of any installed application, using the parent makes sure that only the correct program is allowed to run as an updater.
   f. When adding an updater by name, indicate whether to disable inheritance for the updater.
      For example, if Process A (that is set as an updater) starts Process B, disabling inheritance for Process A makes sure that Process B does not become an updater.

g. When adding an updater by name, indicate whether to suppress events generated for the actions performed by the updater. Typically, when an updater changes a protected file, a File Modified event is generated for the file. If you select this option, no events are generated for changes made by the updater.
h. Click **OK**.

Manage updaters in an unmanaged environment

If a program is configured as an updater, it can install new software and update existing software. You can add, edit, or remove updaters.

Task

1. Add updaters.
    - Add files as updaters:

      ```
      sadmin updaters add <filename>
      ```

    - Add installers as updaters:

      ```
      sadmin updaters add file.exe
      ```

    - Add scripts as updaters:

      ```
      sadmin updaters add <scriptname>
      ```

    - Add users as updaters:

      ```
      sadmin updaters add -u <username>
      ```

    - Add certificates as updaters:

      ```
      sadmin cert add -u <certfilename>
      ```

    Note

    All components signed by these certificates are allowed to change binaries on the system and start new applications.

Argument	Description

-d	Excludes the child process of the file from inheriting updater permissions.
	`sadmin updaters add -d <filename>`
	`sadmin updaters add -d winlogon.exe`

Argument	Description

-n	Disables event logging for a file to be added as an updater.
	`sadmin updaters add -n <filename>`
	`sadmin updaters add -n winlogon.exe`

-l	Adds an execution file as an updater only when the specified library name is loaded for the execution file.
	`sadmin updaters add -l <associated libraryname> <filename>`
	`sadmin updaters add -l system32\wuauserv.dll svchost.exe`

-t	• Includes the tags for a file to be added as an updater.
	`sadmin updaters add -t <associated tag> -l <associated libraryname> <filename>`
	`sadmin updaters add -t Win_up_schedule1 -l system32\wuauserv.dll svchost.exe`
	• Adds a user with a tag name as an updater.
	`sadmin updaters add -t <tagname> -u <username>`
	`sadmin updaters add -t McAfee001 -u john_smith`

-p	Adds a file as an updater, only when its parent execution file is running.
	`sadmin updaters add -p <parentname> <filename>`
	`sadmin updaters add -p svchost.exe iexplore.exe`

-u	Adds a user as an updater. All update operations by the specified user name are allowed. **Note:** When you specify the `-u` argument, other arguments, such as `-l`, `-p`, `-d`, and `-n` are not applicable. `sadmin updaters add -u <username>` Here's are the types of user names that can be added as updaters. • Simple name For example, john_smith.

Argument	Description
	If you specify a simple name, users with this name in all domains are added as updaters. • Domain name (username@domain name) For example, john_smith@mycompany.com. • Hierarchical domain name (domain name\user name) For example, mydomain\john_smith. If you right-click a file and select **Run as <updater user name>**, the file can run as an updater only if the file is added to the whitelist and authorized to run.

2. View all updaters:
   `sadmin updaters list`
3. Remove updaters.
   - Delete all components from the updaters list:

     `sadmin updaters flush`
   - Remove a specific component from the updaters list:

     `sadmin updaters remove <filename>`

Discover potential updaters

You can identify a list of possible updaters that can be added in a Windows system. In the feature list, this is identified as discover-updaters.

When running in Enabled mode, Application Control protection can prevent a legitimate application from running (if the required rules are not defined). The software tracks all failed attempts made by authorized executable to change protected files or run other executable files. You can review the information of failed attempts to identify update rules to allow legitimate applications to run.

Task

1. Get a list of components that can be added as updaters: `sadmin diag`

   Note

   Review the list to ensure that no restricted program or programs with generic names such as, setup.exe, are set as authorized updaters.

   The output of executing this command displays these configuration parameters.

Symbol	Configuration Rules
!	The configuration for the program exists. The existing configuration is displayed on the next line.
*****	The configuration is for a *restricted* program, which can provide capability to change the system. Hence, such programs must have restricted configuration.
***** and **!**	The configuration of the program exists but some changes are required in the configuration to execute the program successfully.

2. Apply the diagnosed configuration changes: `sadmin diag fix`
3. Apply the diagnosed configuration changes for restricted programs: `sadmin diag fix -f`
   Restricted programs are Windows critical programs. For example, services.exe, winlogon.exe, svchost.exe, and explorer.exe.

Configure processes and certificates

On the McAfee ePO console, you can configure updaters by editing the list of generic launcher processes and restricted certificate names.

You can configure these settings:

- **Generic launcher processes** — Certain processes on the Windows operating system, such as explorer.exe and iexplore.exe, start other processes and can be used to start any software. Such processes are referred to as generic launcher processes and must never be configured as updaters. A predefined list of such processes is available on the Application Control configuration interface. You can review and edit the list of generic launcher processes. No updater rules are generated for generic launcher processes at the endpoints.
- **Restricted certificate names** — Certificates from certain vendors such as Microsoft are associated with multiple commonly used applications. They should not be used to define rules based on the certificate. A predefined list of such certificates is available on the Application Control configuration interface. You can review and edit the list of restricted certificate names. If the file in a request is signed by one of these certificates, you can't create rules based on the certificate associated with the file.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Server Settings** → **Solidcore**.
2. Review and edit the list of generic launcher processes.
   a. Review the processes listed in the **Generic launcher processes** field.
   b. Click **Edit** to update the list.
   c. Add the process name to the end of this list (separated by a comma), then click **Save**.
3. Review and edit the list of restricted certificates.

a. Review the names listed in the **Restricted certificate names** field.
b. Click **Edit** to update the list.
c. Add the vendor name to the end of this list (separated by a comma), then click **Save**.
   For example, to prevent creation of rules based on the Microsoft certificate, add `Microsoft` to the list. Use the value listed in the ISSUED TO field of the certificate.

Using interpreters

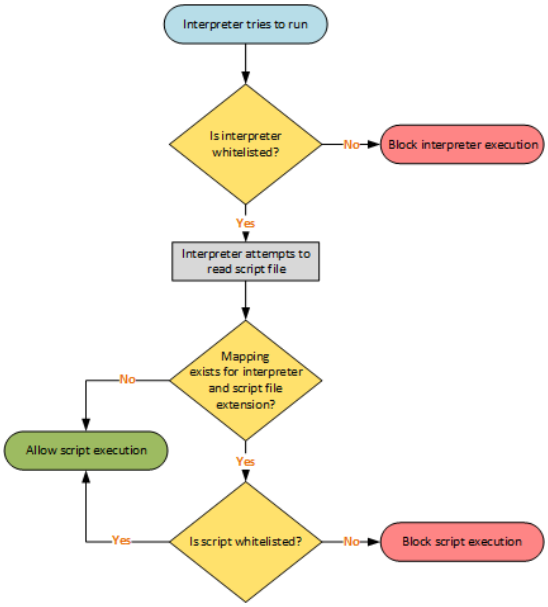
You can configure interpreters to control the execution of additional scripts.

Unlike executables, a script needs an interpreter to read and execute the instructions written in a scripting language. To manage execution of scripts in your setup:

1. Check that relevant interpreters and scripts are whitelisted.
2. Map appropriate file extensions of scripts with specific interpreters.

On the Windows platform, by default, if no interpreter is associated with a script file, the script is allowed to execute because Application Control doesn't treat it as a script file. By default, the software supports standard interpreters and script files that are integrated with Windows operating system, such as batch files (.bat), command interpreter (.cmd), script files (.vbs), PowerShell files (.ps1), and Command files (.com).

When you execute an interpreter to run a script file, these checks that are performed.



Configure interpreters

You can configure interpreters to control the execution of additional scripts.

Task

1. Map an interpreter with a file or script extension:

   `sadmin scripts add extension interpreter1 [interpreter2]...`

   `sadmin scripts add .vbs wscript.exe cscript.exe`

   This command enables Application Control to enforce that wscript.exe and cscript.exe can execute a .vbs script (when the script file and interpreters are whitelisted). After the association is defined, wscript.exe and cscript.exe can also execute other script files (provided the interpreter can read and understand the instructions in the script file). The association is effective immediately and applies to all new interpreter instances initiated after running this command.

   If needed, you can associate additional interpreters with a script or file type. For example:

   `sadmin scripts add .vbs zscript.exe`

   If you try to add an interpreter that is already associated with a file or extension type, no action is taken.

   Note

   Application Control supports a special tag 16 Bits as a synthetic extension for the 16-bit binaries. To control execution for the 16-bit binaries, execute these commands.

   - `sadmin scripts add 16Bit wowexec.exe`
   - `sadmin scripts add 16Bit ntvdm.exe`

2. View interpreter and file extension associations

   `sadmin scripts list`

   Sample output appears like this:

```
.ps1     "powershell.exe"
.bat     "cmd.exe"
.cmd     "cmd.exe"
.pif     "ntvdm.exe"
.sys     "ntvdm.exe"
.vbe     "cscript.exe" "wscript.exe"
16Bit    "ntvdm.exe" "wowexec.exe"
.vbs     "cscript.exe" "wscript.exe"
.exe     "ntvdm.exe"
```

3. Remove interpreter and file extension associations.

   - `sadmin scripts remove extension [interpreter1 [interpreter2]]...` — Removes the specified interpreter associations for the file or script type.
   - `sadmin scripts remove extension` — Removes all interpreter associations for the specified file or script type.

Using installers in a managed environment

What are installers?

On a McAfee ePO console, when a program is configured as an authorized installer, it gets attributes of authorized executable and updater. It can execute and update software on the endpoint.

An authorized installer is allowed based on its SHA-1 or SHA-256 which is specified while configuring the policy. Regardless of the source of the installer, if the SHA-1 or SHA-256 matches, the installer is allowed to run. But, if the reputation of the installer is malicious, its execution is blocked. The reputation of the installer is determined based on the SHA-1 value of an executable file. Reputation sources, such as McAfee GTI and TIE server don't support SHA-256 reputation-based workflows. For example, if you add the installer for the Microsoft Office 2010 suite as an installer and if the SHA-1 or SHA-256 matches, the installer can install the Microsoft Office suite on the protected endpoints.

Control installation and uninstallation

You can manage the installation and uninstallation of software packages using the *Package Control* feature.

This feature allows or denies installation, uninstallation, upgrade, and repair actions for software packages. It also prevents any unauthorized installation and uninstallation.

Package Control is identified as `pkg-ctrl` in the features list and it supports all types of installers on the Windows platform. By default, this feature is enabled and it allows or blocks the installation based on the reputation information and defined rules.

- If the reputation information is available, this feature allows or blocks installation of software packages based on these conditions.

Installer type	Description	Condition
Microsoft Installers (MSI)	This installer type includes multiple variants such as .msp, .mst, and .msm.	If the reputation of the certificate (that has signed the installer file) is trusted, installation of software packages is allowed.
EXE-based installer	This installer includes MSI files embedded with the installer.	If the installer file is configured as an updater, the reputation of the installer file is trusted, or if the reputation of any associated certificate is trusted, installation of software packages is allowed.
Non-MSI-based installers	This installer does not include an MSI file embedded with it.	Package Control considers these conditions to allow or block installation:

Installer type	Description	Condition
		• It considers the reputation of the installer file or the reputation of the certificate. The reputation must be trusted. • It uses a heuristics-based identification for the installer file. • It considers whether the installer file is included or excluded from the list of generic launcher processes, such as explorer.exe and svchost.exe.

- If the reputation information isn't available, installation is allowed or blocked based on the defined rules such as updater by name or path, users, directories, certificate as an updater, SHA-1 or SHA-256 as an updater.

When this feature is disabled, software installation and uninstallation are blocked.

Package Control includes these subfeatures.

Subfeature	Description
Allow Uninstallation	It controls the uninstallation of software packages. When this feature is enabled, software uninstallation, upgrade, and repair actions are allowed. By default, this feature is enabled and identified as *pkg-ctrl-allow-uninstall* in the features list.
Bypass Package Control	This feature controls bypassing from the Package Control feature. When this feature is enabled, Package Control feature is bypassed and software installation and uninstallation is allowed. By default, this feature is disabled and identified as *pkg-ctrl-bypass* in the features list.

By default, the Package Control and Allow Uninstallation features are enabled. You can uninstall any software from the system. But, if the reputation of the uninstall file is malicious (Known Malicious, Most Likely Malicious, or Might be Malicious), software uninstallation isn't allowed regardless of the Package Control configuration. If the reputation of the installer file or MSI file is malicious, software installation isn't allowed regardless of the Package Control configuration. Use this default configuration for desktop and System Center Configuration Manager (SCCM)-managed environments. This configuration allows change, repair, remove, or upgrade operations for software that are useful in these scenarios.

- Explicit software upgrades.
- Software upgrades through Windows update mechanisms.
- Software upgrades of existing software while installing new software packages in chained installations.
- Rollback if there is a power failure or if you restart your system during installation. This is called a suspended installation. The installer tracks the installation that is in progress. When resumed, you can roll back the suspended installation or continue the suspended installation.

If needed, you can also change the default configuration to:

- Disable the Allow Uninstallation feature — Prevents you from uninstalling software from the system. Use this configuration for fixed-function devices and server environments for all actions except upgrades. For upgrading software in server environments, you must switch to the default configuration because it blocks change, repair, remove, or upgrade operations for software.
- Enable the Bypass Package Control feature — Allows software installation and uninstallation on the system except when the file has malicious reputation.
- Disable the Package Control feature — Prevents software installation and uninstallation on the system.
- Place the system in Update mode — this configuration allows software installation and uninstallation on the system except when the file has malicious reputation.

Add an installer in a managed environment

Before defining rules to permit an installer to install or update software on managed endpoints, you must add the installer. You can add an executable or script file.

Use one of these methods to add an installer.

Task

1. Add an existing installer.
   a. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
   b. On the **Installers** tab, select **Actions** → **Add Installer** to open the **Add Installer** page.
   c. Enter the installer details.
   d. Click **Add**.
2. Schedule a server task to routinely add installers.
   a. Select **Menu** → **Automation** → **Server Tasks**.
   b. Click **New Task** to open the **Server Task Builder** wizard.
   c. Type the task name, then click **Next**.
   d. Select **Solidcore: Scan a Software Repository** from the **Actions** drop-down list.
   e. Specify the repository path.
   All subfolders in the specified path are also scanned for installers and certificates.
   f. Specify the network credentials to access the specified network location.
   g. Click **Test Connection** to make sure that the specified credentials work.
   h. Select **Add extracted certificates and installers to Rule Group** to add the certificates and installers extracted by the task to a user-defined rule group and select the user-defined rule group from the list.

   Note

   You can add extracted certificates and installers only to user-defined rule groups.

   i. Click **Next**.

j. Specify the schedule for the task.
k. Click **Next** to open the **Summary** page.
l. Review the task summary, then click **Save**.

Add an installer to a policy or rule group

After you add an installer, you can assign it to a policy or rule group to allow users to install new software and update the software components on a protected endpoint.

Task

1. On the McAfee ePO console, create or change an Application Control policy or rule group.

   Note

   To create a rule group, see *Create a rule group*.

2. On the **Rule Groups** tab, locate your **Group Name** and under **Actions**, click **Edit**.
3. On the **Installers** tab, click **Add**.
4. Search for and add the installer.
5. Specify an identification label for the installer.
6. Click **OK**.

Verify assignments for an installer

This feature provides a convenient way to verify if each installer is assigned to the relevant policies and rule groups.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Solidcore Rules**.
2. On the **Installers** tab, select an installer, then click **Actions** → **Check Assignments**.
   The **Installer Assignments** dialog box lists the rule groups and policies where the selected installer is assigned.
3. Click **OK**.

Configure Package Control

You can configure Package Control to control the installation and uninstallation of software packages on a system.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.x.x: Application Control** product.

3. Select the **Application Control Options (Windows)** category.
4. Click the **My Default** policy to edit it.

   Note

   By default, the **My Default** policy is applied to all endpoints in your enterprise. To configure the feature for selected endpoints, duplicate the **My Default** policy, edit the settings, and apply the policy to only the relevant endpoints.

5. On the **Features** tab:
   a. Select **Enforce feature control from McAfee ePO**.
   By default, the **Package Control** and **Allow Uninstallation** options are selected.
   b. Select an option for configuring Package Control.

Option	Action	Description
Package Control	Enable	When enabled, all subfeatures revert to their default state. But, if you enable the Bypass Package Control subfeature, disable and re-enable Package Control, the Bypass Package Control subfeature is still enabled and in effect.
	Disable	Disabling this feature also disables all its subfeatures.
Allow Uninstallation	Enable	When enabled, this feature allows uninstallation of software packages on endpoints.
	Disable	When disabled, it prevents uninstallation of software packages on endpoints.
Bypass Package Control	Enable	When enabled, Package Control is bypassed and you can't control the installation and uninstallation of software packages.
	Disable	Disables the feature.

Using events

What are events?

Any action to change or execute an unauthorized file or program on a protected system causes Application Control to prevent the action and generate a corresponding event on the endpoint.

When using the software in a standalone environment, you can review the event list by reviewing the product logs.

All events for managed systems are sent to the McAfee ePO server. You can review and manage the generated events to monitor the status of the managed endpoints.

Solidcore Events severity is classified as Info, Minor, Warning, Major, Critical, and Fatal. This classification is done based on the McAfee ePO common threat event severity, numbered from 1–7.

Note

Categories such as Info, Minor, Warning, Major, Critical, and Fatal are displayed on the Threat Events Log page. The severity is displayed in numbers on the Solidcore Events page.

Windows Event viewer is categorized as:

- Information — Info, Minor
- Warning — Warning
- Error — Major, Critical, Fatal

When an event is generated, Solidcore Events severity is classified as Info, Minor, Warning, Major, Critical, or Fatal. When it is mapped with Windows Event categories, McAfee ePO Severity is tagged as Information, Warning, or Error.

View and manage events in a managed environment

All generated events for managed systems are sent to the McAfee ePO server. You can review and manage the generated events to monitor the status of the managed endpoints.

Task

1. On the McAfee ePO console, select **Menu** → **Reporting** → **Solidcore Events**.
2. Specify the time duration for which to view events by selecting an option from the **Time Filter** list.
3. Choose the endpoints where you want to view events.
    a. Select the required group in the **System Tree**.
    b. Select an option from the **System Tree Filter** list.
4. View only specific events by applying one or more filters.
    a. Click **Advanced Filters** to open the **Edit Filter Criteria** page.
    b. Select a listed property.
    c. Specify the comparison operator and property value.
    For example, to view only Execution Denied events, select the **Event Display Name** property, set comparison to **Equals**, and select the **Execution Denied** value.
    d. Click **Update Filter**.

Events matching the specified criteria are displayed.

5. Add user comments for one event or multiple events.
    - One event — Click **Add a comment** link.
    - Multiple events — Select the events, click **Actions** → **Add Comments**, then enter your comments and click **OK**.
6. Exclude or ignore events not required to meet compliance requirements.
    a. On the **Solidcore Events** page, select the events to exclude and click **Actions** → **Exclude Events** to open the **Events Exclusion** wizard.
    b. Select the target platform for the rules and the rule group type, then click **Next** to open the **Define Rules** page.
    c. Click **Next** to open the **Select Rule Group** page, add the rule to an existing or new rule group, then click **Save**.
7. Define rules to allow the execution of a legitimate application.
    a. On the **Solidcore Events** page, under **Actions**, click **Create Policy** for an event.
    b. On the **Monitoring Events Details** page, click **Create Custom Policy** and define the rules.
    c. Select **Choose existing** to add the rules to an existing rule group or select **Create new** to create a new rule group.
    d. To add the rule group to a policy, select **Add rule group to existing policy**.
    e. Click **Save**.

Processing events

Create relevant rules to process events generated at endpoints. This helps to 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 multiple:

- **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.
- **Write Denied** events — Review the events and define appropriate updater or filter rules. Updater rules are appropriate when the events are for a trusted file. Or, filter (AEF) rules might be relevant if the file is malicious or unknown.
- **Installation Denied** events — Review the events and define appropriate updaters.
- **Execution Denied** events — 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 one host, run an antivirus scan on the system, then resolidify the endpoint.
    - From multiple hosts for the same 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.

Note

Starting with the version 8.0.0 release, you can use the **User Comments** field for each event to record additional information for that event.

List of events in a managed environment

This table provides a detailed list of all Change Control and Application Control events.

Note

Some events might not be present in the Linux version of the product.

Event names with a suffix (_*UPDATE*) indicate that events are generated in Update mode.

In the Event type column, these abbreviations indicate the applicable type for the event.

- **SC** — Solidcore client-related event
- **CC** — Change Control event
- **AC** — Application Control event

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
1	20700	BOOTING_DISABLED	**Booted in Disabled mode**	Warning	Warning	SC
2	20701	BOOTING_ENABLED	**Booted in Enabled mode**	Info	Information	SC
3	20702	BOOTING_UPDATE _MODE	**Booted in Update mode**	Info	Information	SC
4	20703	ENABLED_DEFERRED	**Enabled On Reboot**	Info	Information	SC
5	20704	DISABLED_DEFERRED	**Disabled On Reboot**	Warning	Warning	SC
6	20705	BEGIN_UPDATE	**Opened Update Mode**	Info	Information	SC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
7	20706	END_UPDATE	**Closed Update Mode**	Info	Information	SC
8	20707	COMMAND_EXECUTED	**Command Executed**	Info	Information	SC
15	20714	REG_KEY_CREATED	**Registry Created**	Info	Information	CC
16	20715	REG_KEY_DELETED	**Registry Deleted**	Info	Information	CC
18	20717	REG_VALUE_DELETED	**Registry Deleted**	Info	Information	CC
19	20718	PROCESS_TERMINATED	**Process Terminated**	Major	Error	AC
20	20719	WRITE_DENIED	**File Write Denied**	Major	Error	CC
21	20720	EXECUTION_DENIED	**Execution Denied**	Major	Error	AC
29	20728	PROCESS_TERMINATED _UNAUTH_SYSCALL	**Process Terminated**	Major	Error	AC
30	20729	PROCESS_TERMINATED _UNAUTH_API	**Process Terminated**	Major	Error	AC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
31	20730	MODULE_LOADING _FAILED	**Module Loading Failed**	Major	Error	SC
41	20740	FILE_ATTR_SET	**File Attribute Set**	Info	Information	CC
42	20741	FILE_ATTR_CLEAR	**File Attribute Cleared**	Info	Information	CC
43	20742	FILE_ATTR_SET _UPDATE	**File Attribute Set**	Info	Information	CC
44	20743	FILE_ATTR_CLEAR _UPDATE	**File Attribute Cleared**	Info	Information	CC
49	20748	REG_VALUE_WRITE _DENIED	**Registry Write Denied**	Major	Error	CC
50	20749	REG_KEY_WRITE _DENIED	**Registry Write Denied**	Major	Error	CC
51	20750	REG_KEY_CREATED _UPDATE	**Registry Created**	Info	Information	CC
52	20751	REG_KEY_DELETED _UPDATE	**Registry Deleted**	Info	Information	CC
54	20753	REG_VALUE_DELETED _UPDATE	**Registry Deleted**	Info	Information	CC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
56	20755	OWNER_MODIFIED	**File Ownership Changed**	Info	Information	CC
57	20756	OWNER_MODIFIED _UPDATE	**File Ownership Changed**	Info	Information	CC
61	20760	PROCESS_HIJACKED	**Process Hijack Attempted**	Major	Error	AC
62	20761	INVENTORY_CORRUPT	**Inventory Corrupted**	Critical	Critical	AC
63	20762	BOOTING_DISABLED _SAFEMODE	**Booted in Disabled mode**	Warning	Warning	SC
64	20763	BOOTING_DISABLED _INTERNAL_ERROR	**Booted in Disabled mode**	Critical	Critical	SC
70	20769	FILE_CREATED	**File Created**	Info	Information	CC
71	20770	FILE_DELETED	**File Deleted**	Info	Information	CC
72	20771	FILE_MODIFIED	**File Modified**	Info	Information	CC
73	20772	FILE_ATTR_MODIFIED	**File Attribute Modified**	Info	Information	CC
74	20773	FILE_RENAMED	**File Renamed**	Info	Information	CC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
75	20774	FILE_CREATED _UPDATE	**File Created**	Info	Information	CC
76	20775	FILE_DELETED _UPDATE	**File Deleted**	Info	Information	CC
77	20776	FILE_MODIFIED _UPDATE	**File Modified**	Info	Information	CC
78	20777	FILE_ATTR_MODIFIED _UPDATE	**File Attribute Modified**	Info	Information	CC
79	20778	FILE_RENAMED _UPDATE	**File Renamed**	Info	Information	CC
80	20779	FILE_SOLIDIFIED	**File Solidified**	Info	Information	AC
82	20781	FILE_UNSOLIDIFIED	**File Unsolidified**	Info	Information	AC
84	20783	ACL_MODIFIED	**File Acl Modified**	Info	Information	CC
85	20784	ACL_MODIFIED_UPDATE	**File Acl Modified**	Info	Information	CC
86	20785	PROCESS_STARTED	**Process Started**	Info	Information	CC
87	20786	PROCESS_EXITED	**Process Exited**	Info	Information	CC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
88	20787	TRIAL_EXPIRED	**Trial license expired**	Major	Error	SC
89	20788	READ_DENIED	**File Read Denied**	Major	Error	CC
90	20789	USER_LOGON _SUCCESS	**User Logged On**	Info	Information	CC
91	20790	USER_LOGON_FAIL	**User Logon Failed**	Info	Information	CC
92	20791	USER_LOGOFF	**User Logged Off**	Info	Information	CC
93	20792	USER_ACCOUNT _CREATED	**User Account Created**	Info	Information	CC
94	20793	USER_ACCOUNT _DELETED	**User Account Deleted**	Info	Information	CC
95	20794	USER_ACCOUNT _MODIFIED	**User Account Modified**	Info	Information	CC
96	20795	PKG_MODIFICATION _PREVENTED	**Installation Denied**	Critical	Critical	AC
97	20796	PKG_MODIFICATION _ALLOWED_UPDATE	**Installation Allowed**	Info	Information	AC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
98	20797	PKG_MODIFICATION _PREVENTED_2	**Installation Denied**	Critical	Critical	AC
99	20798	NX_VIOLATION _DETECTED	**Nx Violation Detected**	Critical	Critical	AC
100	20799	REG_VALUE _MODIFIED	**Registry Modified**	Info	Information	CC
101	20800	REG_VALUE_MODIFIED _UPDATE	**Registry Modified**	Info	Information	CC
102	20801	UPDATE_MODE _DEFERRED	**Update Mode On Reboot**	Info	Information	SC
103	20802	FILE_READ_UPDATE	**File read in update mode**	Info	Information	CC
106	20805	STREAM_CREATED	**Alternate Data Stream Created**	Info	Information	CC
107	20806	STREAM_DELETED	**Alternate Data Stream Deleted**	Info	Information	CC
108	20807	STREAM_MODIFIED	**Alternate Data Stream Modified**	Info	Information	CC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
109	20808	STREAM_ATTR _MODIFIED	**Attribute Modified in Data Stream**	Info	Information	CC
110	20809	STREAM_CREATED _UPDATE	**Alternate Data Stream Created**	Info	Information	CC
111	20810	STREAM_DELETED _UPDATE	**Alternate Data Stream Deleted**	Info	Information	CC
112	20811	STREAM_MODIFIED _UPDATE	**Alternate Data Stream Modified**	Info	Information	CC
113	20812	STREAM_ATTR _MODIFIED_UPDATE	**Attribute Modified in Data Stream**	Info	Information	CC
114	20813	STREAM_ATTR_SET	**Attribute Added in Data Stream**	Info	Information	CC
115	20814	STREAM_ATTR_CLEAR	**Attribute Cleared in Data Stream**	Info	Information	CC
116	20815	STREAM_ATTR_SET _UPDATE	**Attribute Added in Data Stream**	Info	Information	CC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
117	20816	STREAM_ATTR _CLEAR_UPDATE	**Attribute Cleared in Data Stream**	Info	Information	CC
118	20817	STREAM_RENAMED	**Alternate Data Stream Renamed**	Info	Information	CC
119	20818	STREAM_RENAMED _UPDATE	**Alternate Data Stream Renamed**	Info	Information	CC
120	20819	BEGIN_OBSERVE	**Start Observe Mode**	Info	Information	AC
121	20820	BEGIN_OBSERVE _DEFERRED	**Start Observe Mode On Reboot**	Info	Information	AC
122	20821	END_OBSERVE	**End Observe Mode**	Info	Information	AC
123	20822	END_OBSERVE _DEFERRED	**End Observe Mode On Reboot**	Info	Information	AC
124	20823	INITIAL_SCAN_TASK _COMPLETED	**Initial Scan Completed**	Info	Information	AC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
125	20824	BOOTING_OBSERVE	**Booted in Observe Mode**	Info	Information	AC
126	20825	ACTX_ALLOW_INSTALL	**ActiveX installation Allowed**	Info	Information	AC
127	20826	ACTX_INSTALL _PREVENTED	**ActiveX installation Prevented**	Major	Error	AC
129	20828	VASR_VIOLATION _DETECTED	**VASR Violation Detected**	Critical	Critical	AC
131	20830	THROTTLING_STARTED	**Data Throttled**	Major	Warning	SC
132	20831	THROTTLING_CACHE _FULL	**Data Dropped**	Major	Error	SC
Not applicable (server-side event)	20950	THREAT_DETECTED (1)	**Malicious File Found**	-	Based on reputation. (2)	CC, AC
Not applicable (server-side event)	20951	ASSUMED_THREAT _NOT_PRESENT *	**Malicious File is Trusted**	-	Based on reputation.‡	CC, AC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
Not applicable (server-side event)	20952	OBSERVATION_THRESHOLD _EXCEEDED *	**Observation Threshold Exceeded**	-	Warning	CC, AC
Not applicable (server-side event)	20953	OBSERVATION_REQUEST _THRESHOLD_EXCEEDED *	**Observation Request Threshold Exceeded**	-	Warning	CC, AC
Not applicable (server-side event)	20954	DATA_CONGESTION _DETECTED	**Data Congestion Detected**	-	Warning	CC, AC
Not applicable (server-side event)	20955	CLOGGED_DATA _DELETED	**Clogged Data Deleted**	-	Warning	CC, AC
133	20832	LOCAL_CLI_ACCESS _DISABLED	**Disabled Local CLI Access**	Major	Error	CC, AC
134	20833	LOCAL_CLI_RECOVER _SUCCESS	**Recovered Local CLI**	Info	Information	CC, AC
135	20834	LOCAL_CLI_RECOVER _FAILED	**Unable to Recover Local CLI**	Info	Information	CC, AC
136	20835	OBSERVED_FILE _EXECUTION	**Observed File Execution**	Info	Information	AC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
137	20836	PREVENTED_FILE _EXECUTION	**Prevented File Execution**	Major	Error	AC
138	20837	INVENTORY_RECOVERED	**Recovered Inventory**	Critical	Error	AC
139	20838	INVENTORY_RECOVER _FAILED	**Unable to Recover Inventory**	Critical	Error	AC
140	20839	BLOCKED_PROCESS _INTERACTIVE_MODE	**Blocked Interactive Mode of Process**	Critical	Error	AC
145	20844	PULL_INVENTORY_ENDED	**Pull Inventory Completed**	Information	Information	SC
147	20846	BOOTING_INVENTORY _MODE	**Booted in Inventory Mode**	Information	Information	SC
148	20847	INVENTORY_MODE _DEFERRED	**Inventory Mode on Reboot**	Information	Information	SC
149	20848	END_INVENTORY_MODE _DEFERRED	**Closed Inventory Mode**	Information	Information	SC

1 This event is displayed only on the **Threat Event Log** page.

2 The McAfee ePO severity for this event is based on reputation value. If the reputation value is Known Malicious, Most Likely Malicious, or Might be Malicious, the severity value is Alert, Critical, or Error, respectively. If the reputation value is Unknown, the severity value is Warning. Also, if the reputation value is Might be Trusted, Most Likely Trusted, or Known Trusted, the severity value is Warning, Notice, or Information, respectively.

Customize end-user notifications in a managed environment

If Change Control or Application Control prevent an action on an endpoint, you can choose to display a customized notification message for the event on the endpoint.

You can configure the notification to be displayed on the endpoints for these events.

- **Execution Denied**
- **File Write Denied**
- **File Read Denied**
- **Process Hijack Attempted**
- **Nx Violation Detected**
- **ActiveX Installation Prevented**
- **Installation Denied**
- **VASR Violation Detected**
- **Blocked Interactive Mode of Process**
- **Prevented File Execution**

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.x.x: Application Control** product.
3. Select the **Application Control Options** category and click the **My Default** policy to edit it.
4. Click the **End User Notifications** tab and select **Show the messages dialog box when an event is detected and display the specified text in the message** to display a message box at the endpoint each time any of the earlier mentioned events is generated.
5. Enter the Help Desk information.

Mail To	Represents the email address to which all approval requests are sent.
Mail Subject	Represents the subject of the email message sent for approval requests.
Link to Website	Indicates the website listed in the Application Control and Change Control Events window on the endpoints.

McAfee ePO IP Address and Port	Specifies the McAfee ePO server address and port.

6. Customize the notifications for the various types of events.
   a. Enter the notification message.
      You can use the listed variables to create the message string.
   b. Select **Show Event in Dialog** to make sure that all events of the selected event type (such as Execution Denied) are listed in the **Application and Change Control Events** window on the endpoints.
7. Save the policy and apply to the relevant endpoints.
8. From the endpoints, users can review the notifications for the events and request for approval for certain actions.
   a. Right-click the McAfee Agent icon in the notification area on the endpoint.
   b. Select **Quick Settings** → **Application and Change Control Events**.
      The **Application and Change Control Events** window appears.
   c. Review the events.
   d. Request approval for a certain action by selecting the event and clicking **Request Approval**.

View and manage events in an unmanaged environment

Application Control generates events when an action is taken to change or execute a file on a protected system. You can review and manage events to monitor the status of the managed endpoints.

Task

Go the McAfee Agent icon on your desktop and select **Quick Settings** → **Application and Change Control Events**
You can see a list with all events generated for that endpoint.

List of events in an unmanaged environment

Application Control specific events with the name, event ID, severity, and the description are described in this table.

Note

Some events might not be present in the Linux version of the product.

Event names with a suffix (_*UPDATE*) indicate that events are generated in Update mode.

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
19	20718	PROCESS_TERMINATED	Major	McAfee Solidifier prevented an attempt to hijack the process <string> (Process Id: <string>, User: <string>), by illegally calling the API '<string>'. The process was terminated.
20	20719	WRITE_DENIED	Major	McAfee Solidifier prevented an attempt to change file <string> by process/script <string> (sha1: <string> , md5: <string>, sha256: <string>) (Process Id: <string>, User: <string>).
21	20720	EXECUTION_DENIED	Major	McAfee Solidifier prevented unauthorized execution of '<string>' (sha1: <string>, md5: <string>, sha256: <string>, File Type: <string>) by process <string> (Process Id:<string> , User: <string>) whose parent is process <string> , deny_reason : <string> (deny reason code: <string>) reputation score: <string>.
29	20728	PROCESS_TERMINATED _UNAUTH_SYSCALL	Major	McAfee Solidifier prevented process <string>, run by <string>, from making unauthorized syscall %d (return address %d). The process was terminated.
30	20729	PROCESS_TERMINATED _UNAUTH_API	Major	McAfee Solidifier prevented process <string>, run by <string>, from making unauthorized access to API <string> (return address <string>). The process was terminated

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
49	20748	REG_VALUE_WRITE_DENIED	Major	McAfee Solidifier prevented an attempt to change Registry key '<string>' with value '<string>' by process <string> (Process Id: <string>, User: <string>).
50	20749	REG_KEY_WRITE_DENIED	Major	McAfee Solidifier prevented an attempt to change Registry key '<string>' by process <string> (Process Id: <string>, User: <string>)
51	20750	REG_KEY_CREATED_UPDATE	Info	McAfee Solidifier detected creation of registry key '<string>' by program <string> (User: <string>, Workflow Id: <string>).
52	20751	REG_KEY_DELETED_UPDATE	Info	McAfee Solidifier detected deletion of registry key '<string>' by program <string> (User: <string>, Workflow Id: <string>).
54	20753	REG_VALUE_DELETED_UPDATE	Info	McAfee Solidifier detected deletion of registry value '<string>' under key '<string>' by program <string> (User: <string>, Workflow Id: <string>).
57	20756	OWNER_MODIFIED_UPDATE	Info	McAfee Solidifier detected modification to OWNER of '<string>' by program <string> (User: <string>, Workflow Id: <string>).
61	20760	PROCESS_HIJACKED	Major	McAfee Solidifier detected an attempt to exploit process <string> (sha1: <string>, md5: <string>, sha256: <string>) from address <string>.

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
62	20761	INVENTORY_CORRUPT	Critical	McAfee Solidifier detected that its internal inventory for the volume <string> is corrupt.
75	20774	FILE_CREATED_UPDATE	Info	McAfee Solidifier detected creation of '<string>' by program <string> (User: <string>, Original User: <string>, Workflow Id: <string>).
76	20775	FILE_DELETED_UPDATE	Info	McAfee Solidifier detected deletion of '<string>' by program <string> (User: <string>, Original User: <string>, Workflow Id: <string>).
77	20776	FILE_MODIFIED_UPDATE	Info	McAfee Solidifier detected modification of '<string>' by program <string> (User: <string>, Original User: <string>, Workflow Id: <string>)
79	20778	FILE_RENAMED_UPDATE	Info	McAfee Solidifier detected renaming of '<string>' to '<string>' by program <string> (User: <string>, Original User: <string>, Workflow Id: <string>).
80	20779	FILE_SOLIDIFIED	Info	<string>' was solidified which was created by program <string>(User: <string>, Workflow Id: <string>).
82	20781	FILE_UNSOLIDIFIED	Info	<string>' was unsolidified which was deleted by program <string>(User: <string>, Workflow Id: <string>).

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
89	20788	READ_DENIED	Major	McAfee Solidifier prevented an attempt to read file '<string>' by process <string> (Process Id: <string>, User: <string>).
96	20795	PKG_MODIFICATION _PREVENTED	Critical	McAfee Solidifier prevented package modification by '<string>'(sha1: <string>, md5: <string>, sha256: <string>) by user: '<string>'.
97	20796	PKG_MODIFICATION_ALLOWED _UPDATE	Info	McAfee Solidifier allowed package modification by <string>'(sha1: <string>, md5: <string>, sha256: <string>) by user: '<string>'. (Workflow Id: <string>).
98	20797	PKG_MODIFICATION _PREVENTED_2	Critical	McAfee Solidifier prevented package modification by '<string>' by user: '<string>'.
99	20798	NX_VIOLATION_DETECTED	Critical	McAfee Solidifier prevented an attempt to hijack the process '<string>' (Process Id: '<string>', SHA1: <string>, MD5: <string>, SHA256: <string>, User: '<string>'), by executing code from an address outside of code pages region. Faulting address '<string>'. The process was terminated.
101	20800	REG_VALUE_MODIFIED_UPDATE	Info	McAfeeSolidifier detected modification to registry value '<string>' of type '<string>' under key '<string>' by program '<string>' (User: <string>, Workflow Id: <string>), with data: <string>

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
103	20802	FILE_READ_UPDATE	Info	McAfee Solidifier detected read for '<string>' by program <string> (User: <string>, Original User: <string>, Workflow Id: <string>)
124	20823	INITIAL_SCAN_TASK_COMPLETED	Info	McAfee Solidifier Initial Scan task is complete and Application Control is enforced on the system now.
126	20825	ACTX_ALLOW_INSTALL	Info	McAfee Solidifier allowed installation of ActiveX <string> Workflow Id: <string> by user <string>
127	20826	ACTX_INSTALL_PREVENTED	Major	McAfee Solidifier prevented installation of ActiveX <string> Workflow Id: <string> by user <string>
129	20828	VASR_VIOLATION_DETECTED	Critical	McAfee Solidifier prevented an attempt to hijack the process '<string>' (Process Id: '<string>', sha1: <string>, md5: <string>, sha256: <string>, User: <string>'), by executing code from non-relocatable dll '<string>'. Faulting address <string>. Target address '<string>'.
133	20832	LOCAL_CLI_ACCESS_DISABLED	Major	Local CLI has been disabled due to wrong password attempts and it can be recovered after <string> minutes.
134	20833	LOCAL_CLI_RECOVER _SUCCESS	Info	Local CLI successfully recovered.
135	20834	LOCAL_CLI_RECOVER_FAILED	Info	Failed to recover Local CLI.

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
136	20835	OBSERVED_FILE_EXECUTION	Info	McAfee Solidifier observed start of '<string>'(Process Id: <string>, sha1: <string>, md5: <string>, sha256: <string>, User: <string>, Workflow Id: <mode>: AUTO_2, original_procname: <string> , parent_name = <string>) with command-line: '<string>'.
137	20836	PREVENTED_FILE_EXECUTION	Major	McAfee Solidifier blocked start of '<string>'(Process Id: <string>, sha1: <string>, md5: <string>, sha256: <string>, User: <string>, original_procname: <string>, parent_name = <string>) with command-line: '<string>'.
138	20837	INVENTORY_RECOVERED	Critical	McAfee Solidifier has detected that the inventory for volume <string> is corrupt. The backup dated <string> is loaded.
139	20838	INVENTORY_RECOVER_FAILED	Critical	McAfee Solidifier has detected that the inventory for volume <string> is corrupt. The backup could not be loaded. Review the system and perform solidification to create whitelist.
140	20839	BLOCKED_PROCESS _INTERACTIVE_MODE	Critical	McAfee Solidifier blocked process <string> in interactive mode. (Process Id: <string>, sha1: <string>, md5: <string>, sha256: <string>, User: <string>, original_procname: <string>, parent_name = <string>).

Managing the inventory with McAfee ePO

What is inventory

Inventory is the whitelist created during the initial scan called Solidification.

Inventory information is available on the McAfee ePO console for endpoints. It is updated at regular intervals based on changes made at the endpoints.

Any change to an endpoint's inventory, triggers inventory information to be pushed to the McAfee ePO server after the agent-server communication interval. This keeps the inventory information about the McAfee ePO server updated with changes to inventory at the endpoints. Also, this avoids the need to manually fetch inventory for an endpoint to get the updated inventory.

These changes on an endpoint cause corresponding changes to the inventory information about the McAfee ePO server:

- Addition of a file
- Modification of an existing file
- Rename of a file
- Deletion of a file
- Solidification or Unsolidification of a file

Path of solidified files:

- "<Drive>:Solidcore\Scinv" - Windows
- "\.Solidcore\scinv" - Linux

Note

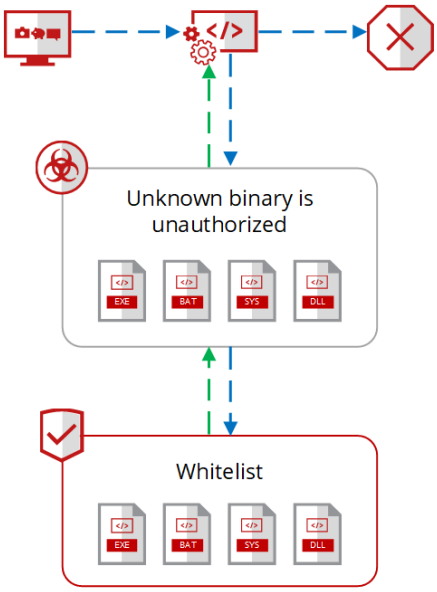
The solidified file is encrypted and can only be decrypted with a special tool from Application Control Engineering. This tool is also version-specific and not available for public use.

What is solidification?

Solidification is the art of creating whitelist for protection.

Whitelist is created during installation by scanning systems for applications, libraries, drivers, and scripts. If a file is solidified, it is allowed to run but is protected from any modifications to be made to it. Whitelisting basics is represented as below:

- Application tries to launch. It can be an executable or operating system component.
- McAfee Application Control verifies the binary code from whitelist.
- Application does not start, if its binaries are not available on whitelist.



Configure inventory updates

Inventory information is updated at regular intervals based on changes made at the endpoints. By default, this configuration is enabled but you can edit this value.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.x.x: General** for the product.
3. In the **Configuration (Client)** category, click **Duplicate** for the **McAfee Default** policy.
4. Specify the policy name, then click **OK**.
5. Open the policy and click the **Miscellaneous** tab.
6. Edit the value for the **Inventory Updates: Configuration** field.
7. Save the policy and apply it to the relevant endpoints.

Configure settings for fetching the inventory

For most enterprises, the default settings configured for fetching the inventory suffice. But, if needed, you can change the default settings.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select **Solidcore 8.x.x: Application Control** for the product and **Application Control Options (Windows)** for the category.
3. Click the **My Default** policy to edit it.

4. Click the **Inventory** tab.
5. Click **Hide Windows OS files** to include the Windows-specific files in the inventory.
   By default, the Windows-specific files are excluded from the inventory. This prevents overwhelming the inventory with legitimate Windows files in the <system drive>\Windows folder (that are signed by the Microsoft certificate) and files in the <system drive>\Windows\winsxs folder.
6. Specify a value for the **Pull Complete Inventory Interval** field. This value indicates the minimum interval (in number of days) between consecutive inventory runs. By default, this value is set to seven days.

   Note

   This value takes precedence over any scheduled tasks to fetch inventory.

7. Specify a value for the **Receive Inventory Updates Interval** field.
   This value indicates the minimum lag (in number of hours) between the generation of consecutive inventory updates. By default, this value is set to three hours.
   Save the policy and apply it to the relevant endpoints.

Fetch the inventory

Although Application Control updates the current inventory for managed endpoints, you can fetch the inventory for one or more managed endpoints, as needed.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Perform one of these actions.
   - To apply a client task to a group, select a group in the **System Tree** and click the **Assigned Client Tasks** tab.
   - To apply a client task to an endpoint, select the endpoint on the **Systems** page, then click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select **Solidcore 8.x.x** for the product and **SC: Pull Inventory** for the task type, then click **Create New Task** to open the **Client Task Catalog** page.
   Specify the task name and add any descriptive information.
5. Click **Save**, then click **Next** to open the **Schedule** page.
6. Specify schedule details, then click **Next**.
7. Review and verify the task details, then click **Save**.

Export SHA-1s

You can use the Offline McAfee GTI tool to fetch ratings for isolated McAfee ePO environments with no access to the internet. You can export SHA-1s of executable files and public key SHA-1s of certificates in the Application Control inventory to a file. The created file is compressed and encrypted.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Inventory**.
2. On the **By Applications** tab, select **Actions** → **Export Inventory for Offline GTI Tool** to create the inventory file.
   The file name is appended with the date and time when the file is created. Here is the syntax of the file name.

   App-Control-Inventory-<year>-<month>-<day>_<hour>-<minute>-<second>.zip

3. Save the inventory file.
   Application Control and Change Control 8.0.x or later versions support SHA-256 values of executable files. Only SHA-1 values of executable files and certificates are exported in the inventory file.
4. Copy the inventory file to a system with access to the internet.

Run the Offline GTI tool

You can use the Offline McAfee GTI tool to fetch ratings for files and certificates with no access to the Internet.

Before you begin

- Make sure that Java Runtime Environment (JRE) 1.6.0_33 or later is installed on the system.
- Verify that the system is connected to the Internet.
- Make sure that you have downloaded and saved the OfflineGTITool.zip file from the McAfee download site.

For all file SHA-1s, File Hash Reputation and File Hash Classification values are fetched from the McAfee GTI file reputation service. Similarly, for public key SHA-1s of certificates, corresponding reputation values are fetched from the McAfee GTI server. The Offline GTI tool fetches the McAfee GTI ratings and saves the information to a result file.

Note

McAfee GTI file reputation service and the server don't support SHA-256 files and public key SHA-256 certificates.

Task

1. Set the GTI_TOOL_JAVA_HOME environment variable.
   a. Open a command window.
   b. Type this command and provide the path to the JRE.

      ```
      set GTI_TOOL_JAVA_HOME=<JRE path>
      ```

      For example:

      ```
      set GTI_TOOL_JAVA_HOME=C:\Program Files\Java\jre6
      ```

2. Run the Offline GTI tool.
   a. Extract the OfflineGTITool.zip file to a system with access to the Internet.

The OfflineGTITool directory is created. This directory contains the readme.txt file that explains the prerequisites, procedure, configuration, and logging details. For detailed information about using the Offline GTI tool, we recommend that you read this file.

b. Change to the OfflineGTITool directory.

```
cd <directory path>
```

Make sure that you specify the absolute path to the OfflineGTITool directory.

c. Verify that the current directory is OfflineGTITool.

```
cd
```

d. Run the tool.

```
runOfflineGTITool.cmd <Inventory file path>
```

Specify the tool name followed by the path to the inventory file that you saved on this system.

For example:

```
runOfflineGTITool.cmd c:\inventory\App-Control-Inventory-yyyy-MM-dd_HH-mm-SS.zip
```

The Offline GTI tool connects to the McAfee GTI server and fetches McAfee GTI ratings for the file SHA-1s and certificate public key SHA-1s. When ratings for all SHA-1s and public key SHA-1s are fetched, a success or failure message is displayed at the command prompt. The created GTI result file contains the McAfee GTI ratings and its contents are encrypted. The file name is appended with the date and time when the file is created.

GTI-Result-<year>-<month>-<day>_<hour>-<minute>-<second>.zip

3. Copy the GTI result file to a system connected to the McAfee ePO server.

Import the GTI result file

You can import the GTI result file to a system connected to the McAfee ePO server to update the Application Control inventory with the fetched McAfee GTI ratings.

Important

After the GTI result file is successfully generated, you must import the McAfee GTI ratings to McAfee ePO in seven days. If you exceed seven days, you can't update the Application Control inventory with the McAfee GTI ratings. Although the default setting is seven days, you can configure it, as needed. To configure this setting, contact McAfee Support.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Inventory**.
2. On the **By Applications** tab, select **Actions** → **Import GTI ratings** to open the Import GTI ratings dialog box.
3. Click **Browse** to select the GTI result file, then click **OK**.
4. Click **OK**.
5. Verify the import:

a. Select **Menu** → **Automation** → **Server Task Log**.
b. Specify the task name **Imports GTI ratings from file to Inventory** in the **Quick find** text box, then click **Apply**.
c. Check that the status of this server task is **Completed**.

Set enterprise reputation for files and certificates

You can change the enterprise reputation for files and certificates on the TIE server to suit your environment. But, changing the enterprise reputation has a global impact on your environment. When you change the enterprise reputation for a file or a certificate, the information is immediately updated in the database and sent to devices in your environment that are listening to TIE change notifications, such as endpoints running Application Control or other clients.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **TIE Reputations**.
2. Click the **File Search** or **Certificate Search** tab.
3. Search for files or certificates, then use the **Actions** menu to set enterprise reputation.

Review the inventory

You can manage and take actions on the software inventory for an endpoint.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Inventory**.
2. Define how to manage the inventory:
    - For all managed endpoints, click the **By Applications** tab.
    - For a selected endpoint, click the **By Systems** tab and click **View** for the relevant endpoint. The inventory for the selected endpoint is listed.
3. Review the applications in the inventory. By default, based on the information received from the configured reputation source, the applications are sorted into **Trusted Applications**, **Malicious Applications**, and **Unknown Applications** categories. The executable files are assigned one of these reputation values.
    - Known Trusted
    - Most Likely Trusted
    - Might be Trusted
    - Unknown
    - Might be Malicious
    - Most Likely Malicious
    - Known Malicious
4. Review application details (only when you review all files sorted by applications).
    a. Click **Inventory Actions** → **Application Details** to open the **Application Details** page.

b. View the details for the application.
c. In the **Executable Files** pane, review the files associated with the selected application.
d. In the **Systems** pane, review the endpoints where the selected application is present.
e. (Optional) Perform any action on the listed endpoints.
f. Click **Close**.

5. Click **Allow** or **Ban** to allow or block the file on an endpoint.

Manage the inventory

Application Control sorts your inventory items based on reputation received from the configured reputation source.

Before you begin

To review and manage inventory items for all systems in your setup, you must be a McAfee ePO administrator. If you are a non-global administrator, you can only review and manage inventory items for systems for which you have the required permissions. If you need permissions to manage enterprise-wide inventory items, contact the McAfee ePO administrator.

Task

1. Define how to manage the inventory:
   - For all managed endpoints, navigate to **Menu → Application Control → Inventory → By Applications**.
   - For a selected endpoint, navigate to **Menu → Application Control → Inventory → By Systems** and click **View** for the relevant endpoint.
2. Prevent malicious executable files or script files from running.
   a. Select the files to block.
   b. Select **Actions → Ban Files** to open the **Allow or Ban Files** wizard.
   c. Specify the rule group for the rules.
      - To add the rules to an existing rule group, select **Add to Existing Rule Group**, select the rule group from the list, and specify the operating system.
      - To create a rule group with the rules, select **Create a New Rule Group**, enter the rule group name, and specify the operating system.

   Note

   You can define rules to allow or ban a file based on both SHA-1 and SHA-256 values of the file.

   d. Click **Next**.
   e. Review the rules, then click **Save**.
3. Allow trusted executable files or script files to run.
   a. Select the files to allow.
   b. Select **Actions → Allow Files** to open the **Allow or Ban Files** wizard.
   c. Perform one of these actions.

- To allow the file only on the selected endpoint, add the file to the whitelist of the endpoint by selecting **Add Files to Whitelist**.
- To allow the file on multiple endpoints, and to add the rules to a rule group, Select **Add to Existing Rule Group** or **Create a New Rule Group**.

d. Click **Next**.
e. Review the rules, then click **Save**.

4. Recategorize an unknown executable file or script file as a trusted file by editing the reputation by Application Control for the file.
   a. Select the files.
   b. Select **Actions** → **Set Reputation by Application Control** to open **Set Reputation by Application Control**.
   c. Select the reputation value.
5. Add the updated rule group to the policies applied to the endpoints.

Define filters for inventory data

Specify advanced exclusion filters to exclude non-meaningful inventory data from the endpoints.

Task

1. On the McAfee ePO console, create or change an Application Control policy or rule group.
2. Select the **Filters** tab and expand **Inventory**.
3. Click **Add Rule**.

   A new filter row appears. You can create filters based on file, file type, application, application version, application vendor, and file signed by certificate (Microsoft certificate only).

   Note

   When you create a filter to exclude inventory items based on the application name, version, or vendor, the filter works on the embedded values associated with the application.

4. Edit the settings to specify the filter.
5. Click **+** or **Add Rule** to specify more AND or OR conditions, respectively.
6. Click **Save**.

Create an approved repository of known applications

You can set the base image for your enterprise to create an approved repository of known applications.

If the inventory for an endpoint in your setup includes known and trusted applications, you can set it as a base image for your enterprise. This creates an approved repository of known applications, including internally developed, recognized, or trusted (from a reputed vendor) applications. Also, this makes management of desktop systems easier by verifying the corporate applications.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Inventory** → **By Systems** to display the endpoints in your setup.
2. Navigate to the endpoint where the known and trusted applications exist.
3. Select **Mark Trusted** for the endpoint.
   This recategorizes all unknown executables (binaries, libraries, and drivers) and scripts on the endpoint as trusted files and edits the enterprise trust level for the files. No changes are made to the malicious executable file or script files on the endpoint.

Compare the inventory

Image deviation is used to compare the inventory of an endpoint with the inventory that is fetched from a designated gold system. This helps you to track the inventory present on an endpoint and identify any differences that occur.

Task

1. Fetch the inventory for your gold host.
2. Fetch the inventory for the endpoint.
3. Review the **Menu** → **Automation** → **Solidcore Client Task Log** page to make sure that both client tasks completed successfully.
4. Compare the inventory of gold host with the inventory of the endpoint. This is known as Image Deviation.
5. Review the comparison results.

Run the inventory comparison

Compare the inventory of the gold host with the inventory of an endpoint.

Task

1. On the McAfee ePO console, select **Menu** → **Automation** → **Server Tasks**.
2. Click **Actions** → **New Task** to open the **Server Task Builder** wizard.
   a. Type the task name, then click **Next**.
   b. Select **Solidcore: Run Image Deviation** from the **Actions** drop-down list.
   c. Specify the gold system.
   d. Configure these options to select the endpoint to compare with the gold system.

   - **Systems to compare with Gold System** — Click **Add** to search for the endpoint that you want to compare with the gold system. Type the name of the endpoint in the **System Name** field and click **Search**.
   - **Groups to compare with Gold System** — Click **Add** to search for the group that you want to compare with the gold system. Type the name of the group in the **Group Name** field and click **Search**.

- **Include Systems with Tags** — Click **Add** to search for endpoints based on their tag names. Type the tag name in the **Tag Name** field and click **Search**.
- **Exclude Systems with Tags** — Click **Add** to search for endpoints based on their tag names. Type the tag name in the **Tag Name** field and click **Search**. Select the required tag from the search result. All endpoints with the selected tags are excluded from comparison with the gold system.

3. Click **Next** to open the **Schedule** page.
4. Specify the schedule for the task.
5. Click **Next** to open the **Summary** page.
6. Review the task summary, then click **Save**.
7. Run the server task immediately to instantly review the comparison results.

Review results of inventory comparison

You can review the results of inventory comparison (image deviation).

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Image Deviation**.
2. Locate the comparison of the gold host and endpoint.
   To quickly find the corresponding row, enter the endpoint name in the **Search Target System** field, then click **Search**.
3. Click **Show Deviations**.
4. Review the comparison details.
   - Select the view type. You can organize the results based on applications or executable files.
   - Use the available filters to sort the results. Using the filters, you can view new (added), changed, and removed (missing) files. Use the **Execution Status Mismatch** filter to view files with changes to the execution status. Use the path filter to sort the results based on the file path.

Matching applications using Common Platform Enumeration (CPE)

Using Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE) is a feature that matches applications in the McAfee Application Control inventory with applications registered on the CPE official dictionary or custom CPE dictionary, using different matching methods.

The CPE official dictionary is hosted and maintained by the National Institute of Standards and Technology (NIST). It can be downloaded from https://nvd.nist.gov/products/cpe.

Note

The CPE feature needs Application Control or Integrity Monitor licenses to work.

If the Solidcore extension is upgraded from a previous version that already has inventory populated, the matching runs between the populated inventory and the CPE dictionary. We recommend that you fetch inventory applications again to improve the matching between the inventory and the CPE dictionary.

Specifying matching methods for applications

Different matching methods are specified for inventory applications based on the type of matching.

- **Canonical** — Applications that match with the NIST official dictionary.
- **Custom** — Applications that match with the custom created dictionary.
- **Generated** — Applications that don't match with any of the imported dictionaries. The Solidcore extension creates a CPE name for them.

Dictionary Types

You can import different types of dictionaries to the CPE page.

- **Official dictionary** — Applications that are registered on the NIST CPE page.
- **Custom dictionary** — Applications that don't match the CPE official page. It is exported from CPE names generated on the McAfee ePO Common Platform Enumeration page.
- **Managed Custom dictionary** — Applications that have a CPE-generated name, that is marked as Managed Custom. They are added to a dictionary type that can be edited from the McAfee ePO CPE dictionaries page.

Import the CPE dictionary

You can import the CPE dictionary by selecting an official CPE dictionary or a custom CPE dictionary.

Task

1. Download the NIST CPE dictionary v2.3 (.zip format) or create a custom CPE dictionary (.xml format).
2. On the McAfee ePO console, select **Menu** → **Reporting** → **Common Platform Enumeration**.
3. Import the CPE dictionary file you downloaded.
    a. Click **Actions** → **Import CPE Dictionary**.
    b. On the **Import CPE Dictionary** page, select the downloaded CPE dictionary (.zip file) and click **OK**.
4. Import the custom CPE dictionary file you created.
    a. Click **Actions** → **Import Custom CPE Dictionary**.
    b. On the **Import Custom CPE Dictionary** page, select the custom CPE dictionary (.xml file) and click **OK**.

Results

Create a server task for matching applications

You can run a server task to match applications between the inventory that is populated with system applications in McAfee ePO and the CPE dictionary.

Before you begin

- Inventory is pulled from the endpoints using McAfee ePO.
- The CPE dictionary is imported.

Task

1. On the McAfee ePO console, select **Menu** → **Automation** → **Server Task**.
2. Click **New task**, enter a name for the task, then click **Next**.
3. From **Actions**, select **Solidcore: CPE Matching inventory applications with the latest imported CPE Dictionary** and click **Next**.
4. **Schedule** the task and click **Next**.
5. **Save** the server task.

Results

Run a server task to match applications

You can run a CPE matching application server task to get a list of matched applications.

Before you begin

- The CPE dictionary is imported.
- The CPE matching server task is created.

Task

1. On the McAfee ePO console, select **Menu** → **Automation** → **Server Tasks**.
2. Select the CPE matching server task and click **Run**.
3. Select **Menu** → **Reporting** → **Common Platform Enumeration**.

Results

The list of matched applications is displayed on the page.

Note

If the dictionary is not imported on the CPE page, this matching task generates a new CPE name for all applications in the inventory.

Using dashboards and queries with McAfee ePO

Dashboards

Dashboards help you monitor your environment.

Application Control provides these default dashboards:

- **Solidcore: Inventory** allows you to observe the inventory for the endpoints.
- **Solidcore: Application Control** helps you keep a check on the protected endpoints.
- **Solidcore: Health Monitoring** helps you monitor the health of the protected endpoints in your enterprise.

Available queries

Use the available queries to review information for the endpoints based on the data stored in the McAfee ePO database.

Application Control queries

Query	Description
Alerts	Displays all alerts generated in the last 3 months.
Application Control Agent Status	Displays the status of all endpoints with the Application Control license which are managed by the McAfee ePO server. The pie chart categorizes the information based on the client status. Click a segment to review endpoint information.
Attempted Violations in the Last 24 Hours	Displays the attempted violation events detected during the last 24 hours. The line chart plots data on a per hour basis. Click a value on the chart to review event details.
Attempted Violations in the Last 7 Days	Displays the attempted violation events detected during the last 7 days. The line chart plots data on a per day basis. Click a value on the chart to review event details.
Non Compliant Solidcore Agents	Lists the endpoints that are currently not compliant. The list is sorted based on the reason for noncompliance. An endpoint can be noncompliant if: • It is in Disabled, Observe, or Update mode. • It is operating in limited feature activation mode.

Query	Description
	• The local command line interface (CLI) access is recovered.
Policy Assignments By System	Lists the number of policies applied on the managed endpoints. Click a system to review information about the applied policies.
Policy Discovery Requests for Automatically-Approved Installations	Lists all files that were identified as installers on the endpoints and executed automatically with installer rights in the last 1 month.
Self-Approval Audit Report	Displays a list of all approval requests that are received from the endpoints in the last month.
Solidcore Agent License Report	Indicates the number of Solidcore Agents that are managed by the McAfee ePO server. The information is categorized by the license information and further sorted by the operating system on the endpoint.
Solidcore Agent Status Report	Displays the status of all endpoints managed by the McAfee ePO server. This report combines information for both the Application Control and Change Control licenses. The pie chart categorizes the information based on the client status. Click a segment to review detailed information.
Summary Server Reboot Log - Rolling 30 Days	Displays the reboot log grouped by system name.
Systems for which Inventory Cannot be Fetched Currently	List the systems in your enterprise for which inventory information can't be fetched currently. You can't fetch inventory for a system if the specified interval between consecutive inventory runs hasn't been reached. This interval value is configurable.
Systems for which Inventory Information has not been Fetched for in Last 1 Month	Lists the systems in your enterprise for which inventory hasn't been fetched in the last month. We recommend that you fetch inventory weekly.
Top 10 Application Vendors	Displays the top 10 application vendors in the enterprise with the maximum number of applications. The chart includes a bar for each vendor and lists the applications for each vendor. The bar chart sorts the data in descending order. Click a section on a bar on the chart to review detailed information for the associated application.

Query	Description
Top 10 Systems with Most Violations in the Last 24 Hours	Displays the top 10 systems with the maximum number of violations in the last 24 hours. The chart includes a bar for each system and indicates the number of violations for each system. Click a bar on the chart to review detailed information.
Top 10 Systems with Most Violations in the Last 7 Days	Displays the top 10 systems with the maximum number of violations in the last 7 days. The chart includes a bar for each system and indicates the number of violations for each system. Click a bar on the chart to review detailed information.
Top 10 Users with Most Violations in the Last 7 Days	Displays the top 10 users with the most policy violation attempts in the last 7 days. The chart includes a bar for each user and indicates the number of policy violation attempts for each user. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.
Top 10 Users with Most Violations in the Last 24 Hours	Displays the top 10 users with the most policy violation attempts in the last 24 hours. The chart includes a bar for each user and indicates the number of policy violation attempts for each user. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.

Health Monitoring queries

Query	Description
Client Task Logs Data Congestion Trend in Last 7 Days	Displays the data congestion trend for client task logs on the last 7 days. The line chart plots data on a per day basis. Click a value on the chart to review details.
Inventory Data Congestion Trend in Last 7 Days	Displays the data congestion trend for inventory in the last 7 days. The line chart plots data on a per day basis. Click a value on the chart to review details.
Number of Systems where Throttling Initiated in Last 7 days	Displays the number of systems where Events, Inventory Updates, or Policy Discovery (Observations) throttling is initiated in last 7 days. The summary table sorts the data in descending order.
Observations Data Congestion Trend in Last 7 Days	Displays the data congestion trend for observations in the last 7 days. The line chart plots data on a per day basis. Click a value on the chart to review details.

Query	Description
Self-Approval Data Congestion Trend in Last 7 Days	Displays the data congestion trend for self-approval requests in the last 7 days. The line chart plots data on a per day basis. Click a value on the chart to review details.
Systems with Most Pending Requests Generated in Observe Mode	Displays systems running in Observe mode with pending Policy Discovery requests. The summary table sorts the data in descending order.
Top 10 Events for 10 Most Noisy Systems in Last 7 days	Displays the top 10 events for the most noisy systems in last 7 days. The bar chart sorts the data in descending order. Click a bar on the chart to review detailed information.

View queries

View an Application Control or **Solidcore Health Monitoring** query.

Task

1. On the McAfee ePO console, select **Menu** → **Reporting** → **Queries & Reports**.
2. Select the **Application Control** or **Solidcore Health Monitoring** group under **McAfee Groups**.
3. Review the queries in the list.
4. Navigate to the required query and click **Run**.
   The results for the selected query are displayed.
5. Click **Close** to return to the previous page.

Using trusted users

What are trusted users?

A trusted user is an authorized user with updater permissions to dynamically add to the whitelist.

You can add users as updaters to allow users to perform update operations on a protected system. For example, add administrators as trusted users to allow them to install or update any software. While adding the user information, you can also provide the domain details.

Important

Of all strategies that allow changes to protected systems, this is the least preferred one because it offers minimal security. After a trusted user is added, there are no restrictions on what the user can change or run on the system.

Add trusted users with McAfee ePO

A trusted user is an authorized user with rights to change the whitelist. A trusted user can override protection and perform update operations on protected endpoints.

You can enter user details or import user or group details from an Active Directory.

Task

1. On the McAfee ePO console, create or change an Application Control policy or rule group.
2. On the **Users** tab, click **Add**.
3. Create two rules for each user.
    - With UPN/SAM and domain account name (in *domainName\user* format)
    - With domain netbiosName (in *netbiosName\user* format)
4. Specify a unique identification label for the user.
   For example, if you specify John Doe's Changes as the identification label for the John Doe user, all changes made by the user are tagged with this label.
5. Type the user name.
6. Click **OK**.

Add trusted users in a standalone environment

Add trusted users to allow them to perform update operations on a protected system.

Task

Run this command at the command prompt.

```
sadmin updaters add -u <username>
```

This table lists the supported arguments, descriptions, and examples.

Argument	Description
-u	Specify the `-u` argument to add a user as a trusted user. All update operations by the specified user name are allowed. You can add these types of user names as trusted users.

Argument	Description

	• Simple name
	For example `john_smith`.
	`sadmin updaters add –u john_smith`
	• Domain name
	For example `john_smith@mycompany`.
	`sadmin updaters add –u john_smith@mycompany`
	• Hierarchical domain name (domain name\user name)
	For example `mydomain\john_smith`.
	`sadmin updaters add –u mydomain\john_smith`
	• Hierarchical local group name (local group name\user name)
	For example `mylocalGroup\john_smith`.
	`sadmin updaters add –u mylocalGroup\john_smith`.
	Note: When you specify the –u argument, other arguments supported for sadmin updaters add command, such as -l, -p, -d, and –n are not applicable.

-t	Specify the –t argument to add a user with a tag name as an updater. Tag name is an identification label which is present in the logs for all files processed by this rule.
	`sadmin updaters add –t <tagname> –u <username>`
	`sadmin updaters add –t McAfee001 –u john_smith`

List trusted users

You can view the list of all users who have updater permissions on the system.

Task

Run this command at the command prompt.

`sadmin updaters list`

This command lists all trusted users and other components defined as updaters in the system.

Remove trusted users

When you remove a trusted user, the updater permissions assigned to that user are removed.

Task

Run this command at the command prompt.

`sadmin updaters remove -u <username>`

For example, `sadmin updaters remove -u john_smith`

Note

After using this command, restart the system to remove updater permissions from the users.

Using trusted local group

Trusted local group

Trusted local group is a feature that adds local groups in the trust model.

McAfee Application Control supports trusted users. You can add users as updaters to allow them to perform installations or update operations on a protected system. While adding the user information, you can also provide the domain details.

A local group can contain user accounts from one or more domains and it shares common permissions and rights only within its own domain.

Trusted local group is enabled by default. To disable trusted local group, set the value of this configuration **IsTrustedLocalGroupEnabled** to "0".

Write protection and read protection

What is write protection?

Write protection is a feature that protects the files, directories, and drives from being changed or deleted. It is identified as `deny-write` in the features list. By default, this feature is enabled.

If you write-protect a directory or drive, write protection is applied to all files and subdirectories in that directory or drive . If any file residing in a directory or subdirectory is write-protected, you can't rename, move, or delete its parent directory.

This feature is in effect only when Change Control is operating in Enabled mode.

Any unauthorized attempt to change the contents of a write-protected component is prevented and an event is generated.

Apply write protection

You can write-protect specific files, directories, and drives to prevent unauthorized programs or users from changing them.

Task

1. Run this command at the command prompt.

   `sadmin write-protect [ -i ] pathname1 ... pathnameN`

   Paths can include wildcard characters. When using wildcards, make sure that the specified string matches a limited set of file paths or file names. If the specified string matches many files, we recommend you revise the string.

   - Paths can include the ***** and **?** wildcard characters. When specifying a file path, C:\Test1**\Test.text, C:\?Test* \Test1\Test.txt are allowed while *:\Test1**\Test.txt, *\Test1\Test2\Test.txt, and *:\Test1\Test2\Test.txt are not allowed.

   For example:

   - `sadmin write-protect -i Listener.ora`

   You can also write-protect network file systems by specifying the network path with the `sadmin write-protect` command to prevent any change to the network share.

   This table describes how you can specify the network path with the command.

Syntax	Example
`sadmin write-protect -i \ \server-name\share-name`	Specify the server name that has a network share. Also, specify the name of the network share. For example: `sadmin write-protect -i \\ftpserver\documents`
`sadmin write-protect -i \ \server-ip\share-name`	Specify the IP address of a server and name of the network share. For example: `sadmin write-protect -i \\192.168.0.1\documents`
`sadmin write-protect -i mapped-drive-letter:\`	Specify the drive letter, which is mapped to the server on the client system. For example: `sadmin write-protect -i W:\`

2. You can write-protect registry keys.

   ```
   sadmin write-protect-reg [ -i ] registrykeyname1 ... registrykeynameN
   ```

   Paths used in registry key-based rules can include the wildcard character (*****). But, it can only represent one path component in the registry path. Don't use the character for the component at the end of the complete registry path (if used at the end, the path filter isn't in effect). For example, registry path HKEY_LOCAL_MACHINE*\Microsoft is allowed while HKEY_LOCAL_MACHINE* or HKEY_LOCAL_MACHINE** isn't allowed.

   Tip

   Write-protect only the HKEY_LOCAL_MACHINE\SOFTWARE registry key cluster to protect the Windows components. Do not write-protect other registry key clusters.

   Specify registry key names as parameters with the write-protect-reg (wpr) command to apply write protection to registry keys. For example:

   ```
   sadmin write-protect-reg -i HKEY_LOCAL_MACHINE\SOFTWARE
   ```

Exclude components from write protection

You can exclude specific components from a write-protected directory or drive.

Task

1. Run this command at the command prompt.

   ```
   sadmin write-protect -e pathname1 ... pathnameN
   ```

   When you specify a file path to be excluded from a write-protected component, write protection is removed from only that specific file.

   Specify the complete path for the components to be excluded from write protection. For example:

   - `sadmin write-protect -e Listener.ora`

2. Exclude registry keys from write protection.

   ```
   sadmin write-protect-reg -e registrykeyname1 ... registrykeynameN
   ```

   Specify the registry key names as parameters with this command and the exclude argument to exclude registry keys from being write-protected.

   For example:

   - `sadmin write-protect-reg -e HKEY_LOCAL_MACHINE\SOFTWARE`

View write-protected components

You can view the complete list of write-protected components.

Task

1. Run this command at the command prompt.
   `sadmin write-protect -l`
2. View all write-protected registry keys.
   `sadmin write-protect-reg -l`

Remove write protection

When you remove write protection, components are no longer protected from unauthorized changes.

Task

1. Run this command at the command prompt.
   `sadmin write-protect [ -r ] pathname1 ... pathnameN`

   When you specify the file path, write protection applied to all files in the specified path is removed.

   For example:

   - `sadmin write-protect -r Listener.ora`

2. Remove write protection from specific registry keys.
   `sadmin write-protect-reg [ -r ] registrykeyname1 ... registrykeynameN`
   For example:

   - `sadmin write-protect-reg -r HKEY_LOCAL_MACHINE\SOFTWARE`

3. Flush write protection from all components.
   `sadmin write-protect -f`
4. Flush write protection from all registry keys.
   `sadmin write-protect-reg -f`

What is read protection?

Read protection is a feature that protects the files, directories, and drives by preventing the data in the files from being read. This feature is identified as `deny-read` in the features list.

Read protection is disabled by default and can be enabled by using the command `sadmin features enable deny-read` and it works only when the software is in Enabled mode.

If you read-protect a component, the whitelisted files in that component aren't allowed to run. Also, if you create a file in a read-protected component, the file can't be added to the whitelist. If a read-protected file or directory is moved to a different path, it is no longer read-protected.

Tip

Make sure that read-protected files are also write-protected. This ensures that the content of the files can't be read by renaming or moving the files. A read-protected file that isn't write-protected becomes readable if it's renamed or moved to another location.

Apply read protection

The read protection feature prevents unauthorized programs or users from reading protected data.

You can read-protect specific components to prevent unauthorized programs or users from reading the data. These components can't be compressed or encrypted.

Task

Run this command at the command prompt.

```
sadmin read-protect [ -i ] pathname1 ... pathnameN
```

Specify the full path for each component to be read-protected.

Paths can include wildcard characters. When using wildcards, make sure that the specified string matches a limited set of file paths or file names. If the specified string matches many files, we recommend you revise the string.

- Paths can include the ***** and **?** wildcard characters. When specifying a file path, C:\Test1**\Test.text, C:\?Test*\Test1\Test.txt are allowed while*:\Test1**\Test.txt, *\Test1\Test2\Test.txt, and *:\Test1\Test2\Test.txt are not.

For example:

- `sadmin read-protect -i password.docx`

You can apply read protection over mounted network file system components by specifying the network paths with the `sadmin read-protect` command.

Exclude specific components from read protection

Exclude specific components from a read-protected directory or drive.

Task

Exclude specific components.

```
sadmin read-protect -e pathname1 ... pathnameN
```

Specify the complete path for the components to be excluded from read protection.

For example:

- `sadmin read-protect -e password.docx`

View read-protected components

You can view the complete list of components that are read-protected.

Task

List all read-protected components.

`sadmin read-protect -l`

Remove read protection

Removing read protection allows users or unauthorized programs to read data from the components, putting critical data at risk.

Task

1. Remove read protection applied to specific components.

   `sadmin read-protect [ -r ] pathname1 ... pathnameN`

   Specify the complete path for the components to be removed from read protection.

   For example:

   - `sadmin read-protect -r confidential.docx`

2. Flush read protection applied to all components.

   `sadmin read-protect -f`

Optimizing your software

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.
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.

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 collect data for a consolidated report. To regularly collect 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.
	• Routinely purge data for inventory, events, client task logs, alerts, and observations. We recommend that you purge:
	  • Events older than 3 or 6 months (based on your auditing needs).
	  • Client task logs older than 30 days.
	
	Note: 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

Applying Windows updates at the earliest is a good practice to keep your operating system secure.

Dynamic whitelisting and Windows update installation process is represented as below:

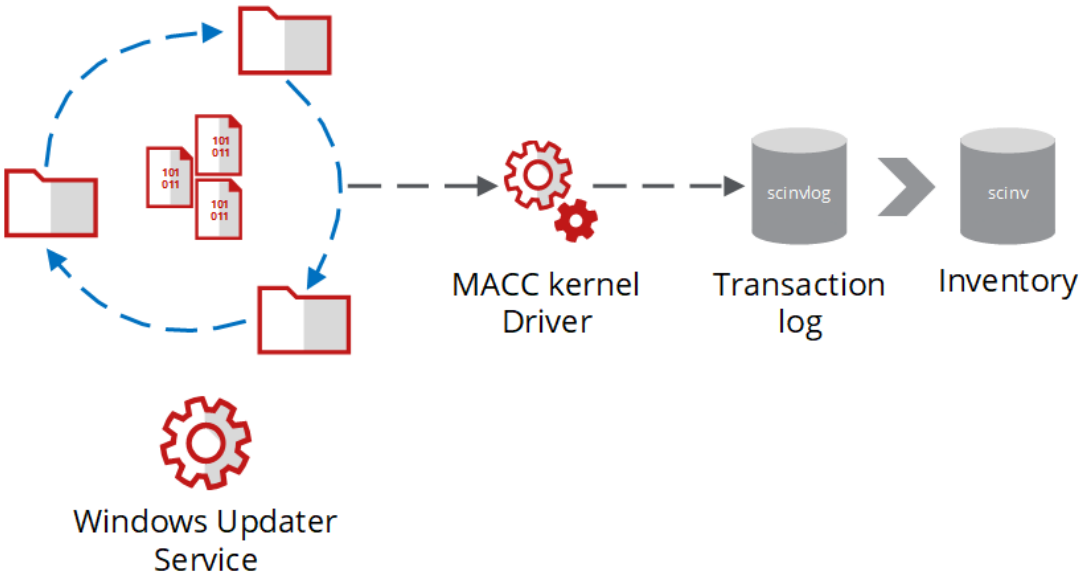
- New binary files are added to the system.

Note

Temporary binaries are not solidified but tracked for security.

Processes identified as updaters are allowed to modify protected files.

- Transaction log (scinvlog) is updated every time a file is modified. Some folders are ignored for solidification because Windows is not meant to execute any binary from that location.
- Transaction log is merged periodically into the inventory (scinv), which is only accessed from user-space.



Here are some considerations and expected behaviors to be reviewed before applying Windows updates in your enterprise environment with Windows Update Services or third-party patching applications.

Using the latest version of McAfee Application and Change Control

Make sure you are running the latest version of the software and extensions (client 8.2.1.435 or later and extension 8.2.6.103 or later).

- Hard link issues are fixed with clients and client configurations are updated for updates with latest versions.
- If you are upgrading the software from an earlier version to 8.2.1.435 or later, you must first resolidify your system to fix the hard links in your inventory.

Note

Resolidification is only needed on upgrade to version 8.2.1.435 or later from an earlier version. Resolidification is not needed if you are upgrading the software from version 8.2.1.435 to a later version.

Applying Windows updates in different modes

If you are running the latest version of McAfee Application and Change Control, you can apply Windows updates in enable mode, disable mode, observe mode, update mode, or inventory mode.

Note

The inventory mode is available on version 8.3.0 or later only.

- Minor security updates, get automatically installed in any mode and do not require any additional steps.
- Feature upgrades need clients to be resolidified after applying major upgrades.

Note

Resolidification must be performed in update mode.

How to resolidify your system after upgrades and major releases

Create a Client Task using these commands:

Note

You need not include *sadmin* to run these commands.

1. bu
2. config set SoPriority=2
3. config set MaplCommLostRestart=0
4. so
5. config set MaplCommLostRestart=5
6. config set SoPriority=1
7. eu

Important

Resolidify the system after performing Windows updates.

McAfee Application and Change Control 8.x and McAfee Agent 5.0.3 are the minimum versions supported to run in a Windows 10 Version 1703 (Creators Update) environment. After upgrading your system with the minimum supported version of MACC and McAfee Agent, follow these steps:

1. Switch McAfee Application and Change Control to the Update mode.
2. Upgrade to Windows 10.
3. Run the solidification task.
4. End the Update mode.

Steps to be followed when upgrading to Windows 10

For information about upgrading to Windows 10 with McAfee Application and Change Control deployed, see KB86551.

Long-term Windows update integration with SCCM

In an enterprise environment with SCCM present, task sequences can be built to automate the update process including major releases. For more information, see KB93343.

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 performing optimally. For more information about maintaining your McAfee ePO server, see *McAfee ePolicy Orchestrator Product Guide*.
- Set up Windows Performance Monitor (PerfMon) to gather performance counters. For information about setting up PerfMon, see the Performance Monitor page on the Microsoft Developer Network website. Collect data for these counters to determine if any services are consuming more 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 Product Guide*.
- Estimate and adjust the agent-server communication interval (ASCI) for your environment. For information about adjusting ASCI, see *McAfee ePolicy Orchestrator Product Guide*.
- Maintain your SQL database to make sure that there is optimal performance. For more information, see *McAfee ePolicy Orchestrator Product Guide*.

Participating in the MACC Product Improvement Program

The Product Improvement Program (PIP) capability or the secure product telemetry framework, when enabled allows McAfee to collect data. You can choose to participate in the MACC Product Improvement Program and allow McAfee to collect data through McAfee Agent.

To learn more about McAfee Product Improvement Program, see https://www.mcafee.com/enterprise/en-us/products/technologies/product-improvement-program.html.

Purpose

McAfee uses the MACC data that is collected through McAfee Agent. The data collected is:

- Analyzed by McAfee to improve product features and customers' experience with the product.
- Used by McAfee Technical Support for troubleshooting.

Privacy protection

The MACC data collected by McAfee Agent is only for product improvement and Technical Support. The system-specific data is filtered or used in aggregate form, unless it is needed for Technical Support. For details about McAfee Privacy Notice, see https://www.mcafee.com/enterprise/en-us/about/legal/privacy.html.

Enable Product Improvement Program to collect data

You can configure the McAfee ePO server settings to enable Product Improvement Program capability.

Task

1. Click **Menu** → **Configuration** → **Server Settings**, select **Product Improvement Program** from the **Setting Categories**, then click **Edit**.
2. Select **Yes** to allow McAfee to collect anonymous diagnostic and usage data, then click **Save**.

Enforce policy to enable the Product Improvement Program capability on MACC

You can manage Product Improvement Program on MACC using the McAfee Agent PIP policy.

Before you begin

Make sure you enable the Product Improvement Program server settings before enforcing the policies.

Task

1. Click **Menu** → **Systems** → **System Tree**, then select a group in the **System Tree**.
   All systems within this group (but not its subgroups) appear in the details pane.
2. Select systems as needed, then click **Actions** → **Agent** → **Set Policy & Inheritance**.
3. Select **McAfee Agent** as the **Product**, **Product Improvement Program** as the **Category**, then select the **Policy** as needed.

   See the McAfee ePO product documentation for more information about creating and editing policies.

4. Select whether to **Reset inheritance** or **Break inheritance**, then click **Save**.

Using the software in virtual environment

McAfee Application and Change Control might not detect hard drives when using a virtual host due to the type of hardware driver it uses.

Sometimes, virtual system detects hard drives as removable media. McAfee Application and Change Control does not solidify removable drives. Follow these steps to allow removable media to be detected correctly.

To enable virtual disk support, change the **CustomerConfig** value as follows:

To enable this feature on a local system:

1. Open an **Administrative Command Prompt** (cmd.exe) using **Run as administrator**.
2. Recover the Application Control command line interface (CLI) using `sadmin recover`.
3. Enter the CLI password.
4. Run this command:

```
sadmin config set customerconfig=65690
```

5. To see the CustomerConfig value, run this command:

```
sadmin config show customerconfig
```

Note

The correct value is: **CustomerConfig 65690 (0x1009a)**.

6. Lock down the CLI using `sadmin lockdown`.
7. Reboot the system.
8. Attempt to solidify the system using the **SC:Enable** task or the `sadmin so` command.

To enable this feature using McAfee ePO client task:

1. Make sure the CLI on the client is locked down.
2. On the McAfee ePO console, select **Menu → Client Tasks → Client Task Catalog**.
3. On the **Client Task Catalog** page, select **Solidcore 8.x.x → SC: Run Commands**, and create a task with the value of **config set customerconfig=65690**.
4. Run the task.
5. Reboot the system when the CustomerConfig value change is in effect.
6. Run the **SC: Enable** task to solidify the system.

If you are deploying to Virtual Desktop Infrastructure (VDI), the VDI template must have Application Control deployed, configured, and protected in the same way as any endpoint. This protected image must then be used as the VDI template to spawn virtual machines. Once your template is ready, you can launch your VDI image in the protection mode (Enabled mode).

Recommended steps to create a VDI template for any software:

1. Create your virtual machine.
2. Install BASE operating system and applications.
3. Apply operating system updates.
4. Install McAfee Agent and place in VDI mode.
5. Install Application Control.
6. Solidify and place system in update mode.

7. Create the template.

When you deploy the system, have it check in to McAfee ePO as it gets a new GUID for McAfee Agent and then it can run the task to lock down and protect.

Using the software with third-party tools

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

For information about configuring Application Control for use in a Microsoft System Center Configuration Manager environment, see KB87830.

- 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 Application and Change Control Installation Guide* for standalone configuration.

Upgrading the software

Follow the recommended upgrade path to successfully upgrade the software.

Solidcore client upgrade supported paths for windows:

Upgrade from version	Upgrade to Solidcore version						
	6.2.x	**7.0.x**	**8.0.x**	**8.1.x**	**8.2.1.x**	**8.2.6**	**8.3.x**
6.1.0 and below	Yes	**No**	**No**	**No**	**No**	**No**	**No**
6.1.0 to 6.1.4	Yes	Yes	**No**	**No**	**No**	**No**	**No**
6.2.x	Yes	Yes	**No**	**No**	**No**	**No**	**No**
7.0.x	N/A	Yes	Yes	Yes	Yes	Yes	Yes

Upgrade from version	Upgrade to Solidcore version						
	6.2.x	7.0.x	8.0.x	8.1.x	8.2.1.x	8.2.6	8.3.x
8.0.x	N/A	N/A	Yes	Yes	Yes	Yes	Yes
8.1.x	N/A	N/A	N/A	Yes	Yes	Yes	Yes
8.2.x	N/A	N/A	N/A	N/A	Yes	Yes	Yes
8.3.x	N/A	N/A	N/A	N/A	N/A	N/A	Yes

Important

You must reboot your system after upgrading to a newer version.

- If upgrading from Solidcore version 6.1.2 or earlier to version 6.2.0.567 or later, you need to first upgrade to Solidcore version 6.1.3 or any version until 6.2.0.555.
-

If upgrading from Solidcore version 8.2.1.143 or earlier to version 8.2.1.435 or later, **Re-Solidification is required**. For more information, see KB91257.

- **Reboot required status** is not updated, if upgraded in **Disable mode** and rebooted before the mode is changed.
-

For more information about how to know if Solidcore needs reboot, see KB92408.

- MACC installer enables you to upgrade on any version but these are recommended paths by support or engineering.
  - Inventory architectural changes are done from version 6.x to 7.x and then to 8.x. Hence, it is recommended not to upgrade directly from version 6.x to 8.x.
- When upgrading from version 6.x to 8.x, features enabled or disabled do not retain current status in some situations.

Note

You must upgrade the Solidcore extension before upgrading the Solidcore client. Review the Solidcore extension use guidelines before upgrading.

Guideline	Example
You can't use an old version of the Solidcore extension with a new version of the Solidcore client.	Solidcore 8.3.0 client can't run with the Solidcore 6.2.0 extension.

Guideline	Example
You can use a new version of the Solidcore extension with an old version of the Solidcore client.	Solidcore 6.2.0 client can run with the Solidcore 8.3.0 extension.

Use these modes for upgrading the Solidcore client.

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

McAfee Secure Policy

McAfee Secure Policy in Policy Catalog under Application Control Rules (Windows) and Configuration (client) are added to make sure only required policies are applied to the end points for secure/restricted product functionality.

This includes predefined rules having limited updaters and skip lists in it to make sure the system is more secure. This Policy is not the default policy. This policy prioritizes security over usability. Lot of rules that allow applications to run have been removed, and this may cause failures in third party applications, this policy must be tested thoroughly before deploying to production environments.

Note

McAfee Secure Policy is compatible only with MACC 8.3.3 and above.

McAfee Secure Policy Under Application Control Rules (Windows) contains these rules from McAfee Default Rules

- Default List
- Execution Control Rules
- Internet Printing
- Local User
- McAfee
- McAfee DLP Agent
- McAfee Exclusion Filters
- McAfee Group Shields
- McAfee Publisher
- SCCM/SMS ClientRestricted - (CcmExec.exe, SMSCliUI.exe, ScanWrapper.exe, CcmSetup.exe, windowsupdatebox.exe. Only these updaters are added as secure)

- System Information
- Terminal Server
- USB Plug and Play
- Windows AD server
- Windows Component(secure) - sysocmgr.exe, cleanmgr.exe, shrpubw.exe, wmiadap.exe, compmgmtlauncher.exe, ServerManagerLauncher.exe, SMSS.exe
- Windows Defender
- Windows Metro App
- Windows Secure - Windows rule group has been changed. Add Windows Secure by making only system32\Wsqmcons.exe as an updater.
- Windows Server Update 2.0 sp1
- Windows Update(Secure) - GWXConfigManager.exe, System32\LogonUI.exe, svchost.exe with library as system32\wups.dll, and svchost.exe with library as system32\wups2.dll, TiWorker.exe, wusa.exe, searchUI.exe, onedrivestandaloneupdater.exe, msdt.exe, iexplore.exe are removed from the updaters list.

McAfee Secure Policy Under Configuration (Client) contains `PathsWritableOnlyByUpdater` config. This configuration changes cannot be made from policy. If you apply this configuration, policy client gets updated with below paths and these paths will be write protected after system reboot:

c:\windows\ccmsetup;c:\windows\ccmcache;c:\windows\system32\ccm\setup;c:\windows\system32\ccm\cache;c:\windows\syswow64\ccm\setup;c:\windows\syswow64\ccm\cache

c:\windows\ccmsetup;c:\windows\ccmcache;c:\windows\system32\ccm\setup;c:\windows\system32\ccm\cache;c:\windows\syswow64\ccm\setup;c:\windows\syswow64\ccm\cache;c:\windows\ccm\systemtemp

Note

Only updater process are allowed to make modification on these write protected path. This setting overrides trusted volume rules.

Client Configuration for MACC

Configuration Name	Summary	Details	Customer configuration associated	Versi intro
ServiceStartFinetune	This configuration handles boot performance issues faced in few of the	ServiceStartFinetune=7 settings can be configured on system to minimize the boot performance issues (if any). This can be configured using client task from McAfee ePO using SC:Run command or	NA	8.3.3

Configuration Name	Summary	Details	Customer configuration associated	Versi intro
	operating systems.	command-line interface on standalone systems.		
UsernameRetryCountInUMode	This configuration handles boot performance issues happening due to username retrial.	User-mode lookup for the username will be retried only after a first successful resolution of the username. This ensures that Solidcore are not retrying the username unnecessarily and thereby delaying the boot. A configuration that specifies the number of retries is also added. UsernameRetryCountInUMode default value is 4 and it is configurable with client task from McAfee ePO using SC:Run command or command-line interface in standalone systems.	CustomerConfig2 bit (8) need to be configured to revert back to the original behavior where username is retried based on the retry count configured even after unsuccessful resolutions of username many times. **Example:** If customerConfig2 value is 0, the CustomerConfig2 value in this case is decimal 256. This value varies based on default customerconfig2 value set. 8th bit needs to be added to default value.	8.3.3
PackageControlCmdlineFull MatchBinaries	This configuration is introduced as a generic option to fine-tune package control and resolve	This configuration can be configured from McAfee ePO as client task using SC:Run command or from command-line in standalone systems. You must reboot the client for this configuration to take place.	NA	8.3.3

Configuration Name	Summary	Details	Customer configuration associated	Versi intro
	performance issues related to installation package.			
PackageControlFinetune1	This configuration is introduced as a generic option to fine-tune package control and resolve performance issues related to installation package.	This configuration can be configured from McAfee ePO as client task using SC:Run Command or from command-line interface in standalone systems. For resolving slow performance issue during install when McAfee GTI is enabled, the configuration PackageControlFineTune1 bit introduced is 29 decimal equivalent 536870912.	NA	8.3.3
InventoryCaseSensitivity Enabled	This configuration is introduced to enable/ disable case-sensitivity on inventory. After turning on case-sensitivity, cleaning inventory and re-solidification are required.	This configuration can be configured from McAfee ePO as client task using SC:Run command or from command-line in standalone systems. InventoryCaseSensitivity Enabled=1 for Enabling Case sensitivity for McAfee Application and Change Control. InventoryCaseSensitivity Enabled=0 for Disabling Case Sensitivity for McAfee Application and Change Control.	NA	8.3.3

Configuration Name	Summary	Details	Customer configuration associated	Versi intro
PathsWritableOnlyByUpdater	Paths added under this configuration will be write protected and only updater process can do updates to this path. This is applicable for trusted directories as well.	Refer to the secure Policy Section for default values, this can be configured from McAfee ePO as client task using SC:Run Command or from command-line interface in standalone systems. You must reboot the client for this configuration to take place.	Setting bit (14) (decimal 16384) will make the paths under PathsWritableOnlyBy Updater write-protected even if they are in trusted directory.	8.3.3
PackageControlCopyBinaries	This configuration prevents observation and event generation when a new msi file is created.	By default, this configuration prevents observation and event generation for three processes - explorer.exe, xcopy, and robocopy.	NA	8.3.5
PackageControlDisableInstallerObservations	This configuration prevents only observation generation for all processes when a new msi file is created.	To stop generating these observations, you need to set the value of this config as `1`.	NA	8.3.5

Configuration Name	Summary	Details	Customer configuration associated	Versi intro
CksumCalcMode	This configuration handles MACC checksum calculation when you create any process.	When you set CksumCalcMode to 0, it takes checksum from MPT cache and does not calculate checksum always on process creation. If set to 1, the checksum stored in inventory compares with the calculated checksum. If there is a mismatch, MACC denies the process execution.	NA	8.2.x

Using Application Control in Observe mode

Observe mode indicates that Application Control is running but it only monitors and logs observations. When running in Observe mode, the application doesn't prevent any execution or changes made to the endpoints. Instead, it monitors execution activities and it compares them with the local inventory and predefined rules.

Note

Observe mode is available only in a McAfee ePO managed environment.

Observe mode also supports reputation-based execution. When you execute a file, Application Control fetches its reputation and that of all certificates associated with the file to determine whether to allow or ban the file execution. When running in Observe mode, Application Control emulates Enabled mode but only logs observations.

All files that are allowed to execute in Observe mode are automatically added to the whitelist, if not already present in the whitelist. An observation event is logged that corresponds to the action Application Control takes in Enabled mode. For example, if not authorized, the execution of Adobe Reader is prevented in Enabled mode. In Observe mode, the file is allowed to execute unless banned by a specific rule or has malicious reputation.

Observe mode offers two benefits.

- It helps you develop policies and determine rules that allow applications to run in Enabled mode.
- It performs a dry run for the product to run or install software without any blockages.

What is Observe mode?

In Observe mode, Application Control records execution, installation, and removal activities for managed endpoints.

In Observe mode, a file is allowed to execute unless it is banned by a specific rule or has malicious reputation. All observations generated on an endpoint are sent to the McAfee ePO server after agent-server communication intervals (ASCI). When an endpoint is in Observe mode, no Application Control events are generated for the endpoint.

Activating Observe mode involves these high-level steps:

1. Identifying the staging or test endpoints for deployment.

   If you have multiple types of endpoints in your setup, group similar types of endpoints to roll out Observe mode. This allows you to analyze product impact on each group of endpoints, discover policy groups, and validate the policies that apply to each group of endpoints.

2. Placing Application Control in Observe mode for a few days and perform day-to-day tasks on the endpoints.

   If a reputation source is available and configured, you can review the reputation of files and certificates in your enterprise. This helps you make informed decisions for the received requests. The settings configured for your enterprise determine the reputation values that are allowed and banned.

Requests are created based on observations generated for the endpoints. These requests allow you to discover Application Control policy rules for the software installed on the endpoints.

3. Periodically reviewing and creating rules for the received requests.
4. Validating the recently added policies by running frequently used workflows. This helps you verify if more requests are received for the applications.
5. When the number of requests received reduces considerably, exit Observe mode and place the endpoints in Enabled mode.

Observe mode also supports reputation-based execution. When you execute a file at an endpoint, the software fetches its reputation and reputation of all certificates associated with the file to determine whether to allow or ban the file execution.

- **Trusted files** — The file is allowed to run, unless blocked by a predefined ban rule. No corresponding observation or event is generated.
- **Malicious files** — The file isn't allowed to execute and no corresponding observation is generated. A corresponding event is generated and displayed on the **Solidcore Events** page. The settings configured for your enterprise determine the reputation value that is banned. You can choose to ban only Known Malicious, Most Likely Malicious, Might be Malicious files, or all such files.
- **Unknown** — Reputation isn't used to determine execution. Application Control performs multiple other checks to determine whether to allow or block the file.

Note

Regardless of the file's reputation, if a ban by name, SHA-1, or SHA-256 rule exists for an executable file, its execution is banned. No corresponding observation is generated. A corresponding event is generated and displayed on the **Solidcore Events** page.

For all processes without updater rights, these observations are generated in Enabled mode and Observe mode.

Observations generated in Observe mode

Scenario	Event generated in Observe mode	Event type in Observe mode (Agent events folder)	Activity (on the McAfee ePO Policy Discovery page)
Execution denied	No		
Write denied	Yes	WRITE_DENIED	File Modification
Installation denied	Yes	PACKAGE_MODIFICATION_PREVENTED	Software Installation
NX violation detected	No		

Scenario	Event generated in Observe mode	Event type in Observe mode (Agent events folder)	Activity (on the McAfee ePO Policy Discovery page)
Process hijack attempted	No		
ActiveX installation prevented	No		

Observations generated in Enabled mode

Scenario	Event generated in Enabled mode	Event type in Enabled mode (Agent events folder)	Event display name (on the McAfee ePOSolidcore Events page)
Execution denied	Yes	EXECUTION_DENIED	Execution Denied
Write denied	Yes	WRITE_DENIED	File Write Denied
Installation denied	Yes	PACKAGE_MODIFICATION_PREVENTED	Installation Denied
NX violation detected	Yes	NX_VIOLATION_DETECTED	Nx Violation Detected
Process hijack attempted	Yes	PROCESS_HIJACKED	Process Hijack Attempted
ActiveX installation prevented	No		

For all processes with updater rights, these observations are generated for memory protection-related operations in Enabled mode and Observe mode.

- Process Hijack Attempted
- Nx Violation Detected

Deployment strategy

You can deploy the software on endpoints in incremental phases to reduce the performance impact.

Phase 1 (Pilot phase)

A pilot phase must not include more than 200 endpoints. Create a basic policy to establish a baseline for your enterprise. Perform day to day tasks on these endpoints. Endpoints in security operations are normally a good place to start as any adverse activities are observed. During this time, run the standard cycle of 2 weeks in observe mode and evaluate the total number of policy discovery events to make sure legitimate software has been added to a policy. New events must not exceed more than 2 per day before enabling. MACC events must not exceed more than 200 events per day to make sure minimal performance impact.

Phase 2 (Group 1)

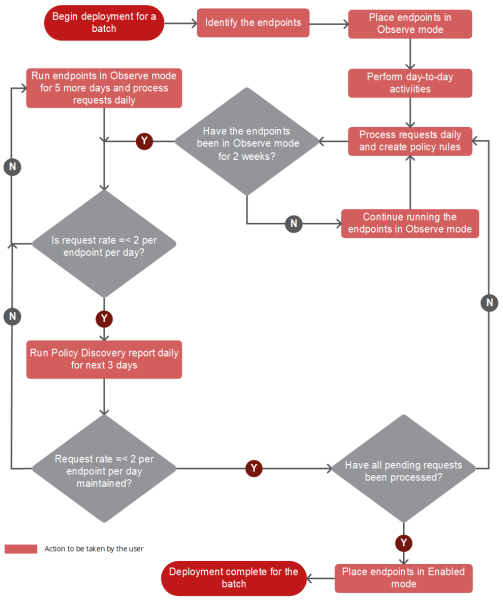
Group 1 must only be deployed when the pilot group is stable. Depending on the target systems, this group must not contain more than 1000 systems if they are low risk endpoints, or 100 systems if assets are considered critical to your environment. You must monitor policy discovery and MACC events daily. Make sure numbers do not exceed 200 events per day and all policy discovery events are reconciled before enabling.

Phase 3 (and beyond)

After deploying group 1 successfully, continue deploying as needed. Further groups must not exceed more than 10,000 as more than 10,000 endpoints in observe mode can cause significant performance degradation to McAfee ePO.

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 the software 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 needed rules.	Deployment	Identify endpoints in pilot phase.
	Number of endpoints	Total number must not exceed 200, use criteria discussed under "deployment strategy".
	Pre-deployment tasks	Complete these activities for your endpoints: • Run an on-demand scan. • Update 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.	Pulling inventory	If a software inventory is needed by your organization, make sure to select the box within the **SC:Enable** client task to collect an inventory.
	Verifying placement	Verifying placement runs the **Application Control Agent Status** query to verify that selected endpoints are placed in Observe mode.
	Number of endpoints	Total number must not exceed 200, use criteria discussed under "deployment strategy". At any point, only 2 batches can run simultaneously in Observe mode.
	Determining scan priority	The scan priority determines the priority of the thread that creates the whitelist on the endpoints. For most scenarios, we recommend that you set the scan priority to **Low**. For systems that are in the Production mode, use **Low** priority to make sure there is minimal impact. Also, you must use **Low** priority if the system can't be restarted. If you can restart the system and you want the initial scan to be completed as soon as possible, select **High** priority.

Task	Recommendation	Description
	Selecting activation	Wherever possible, use **Full Feature Activation** to make sure 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 antivirus or McAfee® Host Intrusion Prevention software.
Perform day-to-day operations and tasks to generate corresponding requests.	Based on the requests, you can define relevant rules needed 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 Application Control is optimally configured for your setup.	Specifying processing ownership	The McAfee ePO administrator must process requests. Based on your setup, you might need to make sure there is collaboration between global and site administrators.
	Determining frequency	• Process requests daily and define needed rules. • Run reports every week 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 request and verify 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.

<table>
<tr><th>Task</th><th>Recommendation</th><th colspan="3">Description</th></tr>
<tr><td rowspan="11"></td><td>Running reports</td><td colspan="3">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.</td></tr>
<tr><td>User Comments</td><td colspan="3">You can record additional information for each request. For example, add a similar piece of information inside User Comments field for a few requests for request identification.</td></tr>
<tr><td rowspan="10">Rule identification</td><td colspan="3">Rules are identified for requests based on event and activity type.</td></tr>
<tr><td>Event type</td><td>Activity type</td><td>Rule type</td></tr>
<tr><td>File Write Denied</td><td>File Modification</td><td>Updater process rule</td></tr>
<tr><td>Installation Denied</td><td>Software Installation</td><td>Installers rule</td></tr>
<tr><td>ActiveX Installation Prevented</td><td>ActiveX Installation</td><td>Certificates rule</td></tr>
<tr><td>NX Violation Detected</td><td>Memory Protection Violation</td><td>Exclusions rule</td></tr>
<tr><td>Process Hijack Attempted</td><td>Memory Protection Violation</td><td>Exclusions rule</td></tr>
<tr><td>VASR Violation Detected</td><td>Memory Protection Violation</td><td>Exclusions rule</td></tr>
<tr><td>Execution Denied</td><td>Software Installation</td><td>Installer rule</td></tr>
<tr><td>Execution Denied</td><td>Application Execution</td><td>Executable file rule to allow execution or allow locally to add to whitelist</td></tr>
<tr><td>File Write Denied</td><td>File Addition</td><td>Updater rule</td></tr>
</table>

Configure processes and certificates

On the McAfee ePO console, you can configure updaters by editing the list of generic launcher processes and restricted certificate names.

You can configure these settings:

- **Generic launcher processes** — Certain processes on the Windows operating system, such as explorer.exe and iexplore.exe, start other processes and can be used to start any software. Such processes are referred to as generic launcher processes and must never be configured as updaters. A predefined list of such processes is available on the Application Control configuration interface. You can review and edit the list of generic launcher processes. No updater rules are generated for generic launcher processes at the endpoints.
- **Restricted certificate names** — Certificates from certain vendors such as Microsoft are associated with multiple commonly used applications. They should not be used to define rules based on the certificate. A predefined list of such certificates is available on the Application Control configuration interface. You can review and edit the list of restricted certificate names. If the file in a request is signed by one of these certificates, you can't create rules based on the certificate associated with the file.

Task

1. On the McAfee ePO console, select **Menu → Configuration → Server Settings → Solidcore**.
2. Review and edit the list of generic launcher processes.
   a. Review the processes listed in the **Generic launcher processes** field.
   b. Click **Edit** to update the list.
   c. Add the process name to the end of this list (separated by a comma), then click **Save**.
3. Review and edit the list of restricted certificates.
   a. Review the names listed in the **Restricted certificate names** field.
   b. Click **Edit** to update the list.
   c. Add the vendor name to the end of this list (separated by a comma), then click **Save**.
   For example, to prevent creation of rules based on the Microsoft certificate, add `Microsoft` to the list. Use the value listed in the ISSUED TO field of the certificate.

Place endpoints in Observe mode

After installation, we recommend placing selected endpoints in Observe mode to perform a test run for the Application Control product.

Select at least one endpoint for each type you have in your environment. Use one of these client tasks to place the endpoints in Observe mode.

- **SC: Enable** — Use this client task to place the endpoints in Observe mode after fresh installation of Application Control.
- **SC: Observe Mode** — Use this client task to place the existing endpoints (running in Enabled mode) in Observe mode.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Perform one of these actions.
   - Group — Select the group in the **System Tree** and click the **Assigned Client Tasks** tab.
   - Endpoint — Select the endpoint on the **Systems** page and click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select **Solidcore 8.x.x** → **SC: Enable**, then click **Create New Task** to open the **Client Task Catalog** page.
   a. Specify the task name and add any descriptive information.
   b. Select **Windows** for the platform, **All except NT/2000** for the subplatform, then select **Application Control**.
   c. Specify the scan priority.
   The set scan priority determines the priority of the thread that is run to create the whitelist on the endpoints. We recommend setting the scan priority to **Low**. This makes sure that Application Control causes minimal performance impact on the endpoints but might take longer (than when you set the priority to **High**) to create the whitelist.
   d. Specify the activation option.
      - **Limited Feature Activation** — Endpoints are not restarted, whitelist created, and limited features of Application Control are activated. Memory protection and Script As Updater (SAU) features are available only after the endpoint is restarted.
      - **Full Feature Activation** — Endpoints are restarted, whitelist created, and all features of Application Control including memory protection are active. Restarting the endpoints is needed to enable the memory protection features. The endpoint is restarted 5 minutes after the client task is received at the endpoint. A pop-up message is displayed on the endpoint before the endpoint is restarted.
   e. Select **Start Observe Mode**.
   f. (Optional) Select **Pull Inventory**.
   If you select this option, the inventory (including the created whitelist) is sent to McAfee ePO. Select this option because inventory information is used in multiple workflows available from McAfee ePO.
   g. Click **Save**.
5. Click **Next** to open the **Schedule** page.
6. Specify scheduling details, then click **Next**.
7. Review and verify the task details, then click **Save**.
8. (Optional) Wake up the agent to send your client task to the endpoint immediately.

Policy discovery permissions

By default, non-global administrators can view, manage, and delete requests generated only by endpoints in their associated group (in **My Organization**).

If you review request details about the **Request Details** page, the number of requests listed in the **Enterprise Level Activity** pane might be less than the value displayed in the **Global Prevalence** column on the **Policy Discovery** page. This is because the **Global Prevalence** column indicates the enterprise-wide prevalence for the requests regardless of any groups. For example, if a request is generated by two systems in different groups across the enterprise, the value in the **Global Prevalence** is 2. But, because non-global administrators can only view the requests generated for their group, the non-global administrator might see only one request generated by the system in their group in the **Enterprise Level Activity** pane.

Note

The McAfee ePO administrator can review and manage all requests generated in the enterprise (**My Organization**). Also, McAfee ePO administrator can add rules to any rule group, and provide permissions to all non-global administrators to review and take custom actions on the requests generated in the enterprise.

If you are a non-global administrator, you can add rules (for a request) to only the rule groups that you own. Rule groups that you don't own are not displayed on the **Policy Discovery: Custom Rules** page. Also, if you take an action for a request, the action doesn't impact the same request generated by the system in a different group.

Allow non-global administrators to manage enterprise-wide requests

If you are a McAfee ePO administrator, you can assign permissions to all non-global administrators (who have access to groups in **My Organization**) to review and manage requests generated in your enterprise.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Server Settings**.
2. From the **Setting Categories** pane, select **Solidcore**, then click **Edit** to open the **Edit Solidcore** page.
3. Change the value of **Allow group administrators to manage Policy Discovery requests for entire System Tree** to **Yes (overrides System Tree group access permissions)**.
4. Click **Save**.

Results

All non-global administrators are allowed to review and take custom actions on enterprise-wide requests. Non-global administrators can't perform global actions.

Managing requests

Review requests

You can review the requests received from endpoints.

Note

Some fields don't apply to Linux endpoints.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Review the listed requests using one of these methods.
   - **Specific interval** — Select an option from the **Time Filter** list, then click **Update Results** to view requests received during a specific interval.
   - **Request status** — Select a value for the request status from the **Approval Status** list, then click **Update Results** to view requests that match the selected status.
   - **Activity** — Click **Additional filters** and select a value from the **Activity** list. Click **Update Results** to view requests for a certain activity.
   - **Reputation** — Click **Additional filters** and select a value from the **Final Reputation** list. Click **Update Results** to view requests for files that match the selected reputation value. For more information about how the software determines final reputation for files or certificates, click **What's Final Reputation**.
   - **Specific endpoint** — Click **Additional filters** and enter an endpoint name in the **System Name** field. Click **Update Results** to view requests received from the endpoint. Make sure that you specify the complete system name because no partial matches are performed.
   - **Multiple criteria** — Specify values for the **Time Filter**, **Approval Status**, **Activity**, **Final Reputation**, and **System Name** fields, as needed, then click **Update Results** to perform a search based on the specified criteria.
   - **Specific search string** — Enter a search string in the **Quick find** field for **Object Name**, **Application Name**, **Certificates**, and **User Comments**, then click **Apply** to view requests that match the specified search string. Partial matches are performed based on the text you specify.
   - **Sort** — Sort the list based on the global prevalence, final reputation, reputation source, execution time, activity, object name, application name, certificate, or user comments by clicking the column heading.
   - **Selected requests** — Select requests of interest, then click **Show selected rows** to review only the selected requests.

   Note

   The **Policy Discovery** page lists only the requests for which the McAfee ePO administrator can make rules. To view other requests, such as those for installers with trusted reputation, run the **Policy Discovery Requests for Automatically-Approved Installations** query. The query lists all files with trusted reputation that were executed automatically on the endpoints with installer permission in the last one month.

3. (Optional) Add user comments for one or multiple events:
   - One event – click **Add a comment**.
   - Multiple events – select the requests and click **Actions** → **Add Comments**, then enter your comments and click **OK**.
4. Review individual requests that make up a collated request and detailed information for the file.
   a. Click a row to open the **Request Details** page.

b. Review file details, such as name, version, path, parent process, files changed, final reputation, and user comments, if any.
c. Review the checksum information for the file.
d. Click the file SHA-1 value to review file details about the **File Details** page.
e. Review the certificate vendor name for the file. The certificate vendor name for a file is color coded to indicate trusted (green), malicious (red), or unknown (orange) reputation.
f. Click certificate name to view certificate details, such as issuer, certificate reputation, reputation source, public key algorithm, public key length, public key hash, certificate hash, valid from, and valid to.
g. Review the individual requests that make up the collated request in the **Enterprise Level Activity** pane.
h. Click **Close**.

Allow a file on all endpoints

You can define rules to allow an application or executable file to run on all endpoints in the enterprise.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the requests where you want to define rules.
3. Click **Actions** → **Allow File Globally**.
   The **Allow File Globally** dialog box provides details and prompts you to confirm the action.
4. Click **OK**.

Results

Rules are created for the files associated with the selected requests and added to the Global Rules rule group included in the **McAfee Default** policy.

Allow a file by certificate

You can define rules to allow an application, executable file, or ActiveX control to run on all endpoints in the enterprise based on the certificate associated with the file.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the request where you want to define rules.
3. Click **Actions** → **Allow by Certificate Globally**.
   The **Allow by Certificate Globally** dialog box provides details and prompts you to confirm the action. Based on the file associated with a selected request, the certificate is assigned or not assigned updater privileges. If the certificate has

updater privileges, allowing based on certificate allows all applications signed by the certificate to make changes to existing executable files or start new applications on the endpoints.

4. Click **OK**.

Note

The **Allow by Certificate Globally** action is unavailable if the main executable associated with the request is signed by a certificate included in the Restricted certificate names list.

Allow network files on all endpoints

You can define rules to allow a network file (file placed on a network path) to run on all endpoints in the enterprise.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the request where you want to define rules.
3. Click **Actions** → **Allow Trusted Path Globally**.
   The **Allow Trusted Path Globally** dialog box provides details and prompts you to confirm the action. Based on the network path associated with a selected request, suggested alternate paths (sorted based on path length) and corresponding number of matching requests that are pending for each suggested path are displayed.

   Caution

   When you allow the path, updater rights are provided to all software present in that network path and its subdirectories. Use caution and carefully add the trusted path.

   When a request from a network path is approved globally, no further requests for the approved network path and its subdirectories are received at McAfee ePO.
4. Click **OK**.

Results

Rules to allow the specified network path (with updater rights to all software present in that network path and its subdirectories) are added to the Global Rules rule group included in the **McAfee Default** policy.

Ban by SHA-1 or SHA-256 on all endpoints

You can define rules to ban an application or executable file from running on all endpoints in the enterprise based on the SHA-1 or SHA-256 value of the file.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the requests where you want to define rules.
3. Click **Actions** → **Ban File Globally**.
   The **Ban File Globally** dialog box provides details and prompts you to confirm the action.
4. Click **OK**.
   Rules are created for the files associated with the selected requests and added to the Global Rules rule group included in the **McAfee Default** policy.
5. Ban the files that have already been added to the endpoint.
   a. Click the application name link.
      The **Files** page lists all executable files installed on the endpoint.
   b. Select all listed files.
   c. Click **Actions** → **Ban Files** to open the **Allow or Ban Files** wizard.
   d. Specify the rule group for the rules.
      - To add the rules to an existing rule group, select **Add to Existing Rule Group**, select the rule group from the list, and specify the operating system.
      - To create a rule group with the rules, select **Create a New Rule Group**, enter the rule group name, and specify the operating system.
   e. Make sure that the rule group where you add the rules is added to a policy that is applied on the endpoint where the request was received.
   f. Click **Next**.
   g. Review the rules, then click **Save**.

Define rules for specific endpoints

If you are a McAfee ePO administrator, you can add prepopulated rules to allow or ban an application or executable file for specific endpoints in your administered groups. Or, you can define custom rules for specific endpoints or groups, as needed.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the request where you want to define custom rules.
3. Click **Actions** → **Create Custom Policy** to open the **Policy Discovery: Custom Rules** page.
4. You can review rules or define custom rules:
   - **Review or add rules** — Select **Approve Request**, **Ban Request**, **Allow By Certificate**, **Allow Trusted Path**, or **Bypass Memory Protection**, then review or add more rules as needed.
   - **Define custom rules** — Select **Clear and define Rules**, then review the request details and define relevant rules as needed.
5. Specify the rule group for the rules.

- To add the rules to an existing rule group, select **Choose existing** and select the rule group from the list.

Note

When adding rules to allow a network path, select your rule group carefully. If you add rules to the **Global Rules** rule group, all future requests received from that network path are automatically approved. Or, if you add your rules to a custom rule group, future requests from that network path aren't automatically approved.

- To create a rule group with the rules, select **Create new** and enter the rule group name.

6. (Optional) Add the changed or created rule group to a policy.
   a. Select **Add rule group to existing policy**.
   b. Select the policy where you want to add the rule group.
7. Click **Save**.
   This approves all grouped requests. For requests received from network paths, when you click **Save**, the **Approve Requests for Subdirectories** pop-up window appears that includes a checkbox to approve all related requests. If needed, select the checkbox, then click **OK** to approve all requests received from the network path and its subdirectories.

Allow by adding to whitelist for specific endpoints

You can add one or more executable files to the whitelist to allow the files to run on the endpoint.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Click a row to review request details in the **Request Details** page.
   Each row in the **Enterprise level activity** pane represents an executable file and endpoint combination.
3. Click **Allow Locally** for a row.
   The **Allow Locally** dialog box lists one or more paths to add to the whitelist.

Note

The **Allow Locally** action is available only for requests that are generated when you execute an application that isn't in the whitelist (Application Execution activity).

4. Review and customize the listed paths.

   For example, if you execute proc.exe for an endpoint, these paths might be listed.

   C:\Program Files\<App Name>\proc.exe

   C:\Program Files\<App Name>\a.dll

   C:\Program Files\<App Name>\b.dll

   To avoid redundancy, add only the C:\Program Files\App Name path.

5. Click **OK**.

Results

The specified paths are added to the whitelist and allowed to run on the endpoint.

Define bypass rules for all endpoints

You can define rules to allow an application or executable file to bypass applied memory protection and other techniques.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the request where you want to define bypass rules.
3. Click **Actions** → **Bypass Memory Protection Globally**.
4. When prompted to confirm, click **OK**.

Results

Rules are created for file associated with the selected request and added to the **Global Rules** rule group included in the **McAfee Default** policy.

Change file reputation

Application Control works with multiple sources to fetch reputation information. The software regularly synchronizes with TIE and McAfee GTI. You can review or edit the reputation for a file on the **TIE Reputations** page.

Task

1. Select **Menu** → **Application Control** → **Policy Discovery**.
2. On the **Policy Discovery** page, select a request and click **Actions** → **More** → **Change File Reputation (TIE)**
3. Review the file information about the **TIE Reputations** page.
4. (Optional) Edit file reputation: click **Actions**, then select an action.

Delete requests

You can remove requests from the **Policy Discovery** page and database.

Note

For optimal performance, the **Solidcore: Auto Purge Policy Discovery Requests** server task is run weekly to remove policy discovery requests older than three months.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the requests to delete.
3. Click **Actions** → **Delete Requests**.
4. When prompted to confirm, click **OK**.

Results

All selected collated requests and contained individual requests are deleted from the page and database.

Define filters for observations and events

You can specify advanced exclusion filters to exclude non-meaningful observations and events from the endpoints.

Task

1. On the McAfee ePO console, create or change an Application Control policy or rule group.
2. Select the **Filters** tab and expand **Observations & Events**.
3. Click **Add Rule** to add a filter row.
   You can create filters based on files, events, programs, registry keys, and users. By default, all defined filters are applied to observations.
4. Edit the settings to specify the filter.
5. Click **+** or **Add Rule** to specify additional AND or OR conditions, respectively.
6. Select **Apply rule to events also** for a set of rules to apply the filter rules to events.
   You can also define advanced exclusion filters from the **Solidcore Events** page.

Define filters for user comments

You can apply a filter on user comments to view the requests and identify which requests are to be processed. Only the requests matching the specified filter criteria are displayed.

Task

1. On the McAfee ePO console, select **Menu** → **Reporting** → **Queries & Reports**, then click **New Query** to open the **Query Builder** page.
2. Select **ePO** → **Solidcore** → **Policy Discovery Collated Requests**, then click **Next** to open the Chart tab and the filters tab.

3. Select **User Comments** from the available properties and define the comparison and value.
4. Click **Run** to apply the filter.
   Requests matching the specified criteria are displayed.
5. Click the**Activity** bar on the chart or click a row to open the **Request Details** page.
6. Click **Back** to return to the previous page or Click **Save** to save the query.
7. Click **Save** to save the query.
   This query is saved to the Query Group.

Throttling observations

Frequently reviewing and managing requests for the generated observations allows you to define the relevant rules for your setup. If you don't process observations in a timely manner, you continue to get similar and repeated observations from endpoints.

Also, if you place additional endpoints in Observe mode or perform multiple activities simultaneously on existing endpoints (in Observe mode), the absence of relevant rules might result in excessive generation of observations. If a high number of observations are received at the McAfee ePO server from the endpoints, the McAfee ePO interface might become sluggish.

Observation throttling helps you take care of the non-responsiveness of the McAfee ePO interface. When the number of observations received at the McAfee ePO server reaches the defined threshold, observation throttling is initiated. When observation throttling starts, Application Control performs these actions:

- It stops further processing of observations at McAfee ePO to prevent non-responsiveness of the McAfee ePO interface.
- It applies the **Throttling Rules** policy to the **My Organization** group to prevent the generation of observations on all endpoints after agent-server communication interval.
- It generates the **Observation Request Threshold Exceeded** event. This event is displayed on the **Threat Event Log** page and can be used to create an automatic response.
- It displays a warning message on the **Policy Discovery** page stating that observation generation has stopped.

Define the threshold value for throttling

By default, Application Control can process 100,000 observations in 24 hours. You can configure this setting to define the threshold value for your enterprise.

When the number of observations received at the McAfee ePO server in the last 24 hours reaches the defined threshold, observation throttling is initiated.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Server Settings**.
2. From the **Setting Categories** pane, select **Solidcore**.
3. Change the value of **Threshold count at which to initiate throttling and suspend observation generation (6.1.1 and older endpoints)** setting.

Review filter rules for throttling

To implement throttling, rules that filter and stop observations are added to the **Stop Observation Requests** rule group.

This rule group is read only and is assigned to the default read-only **Throttling Rules** policy. Initially, this policy isn't assigned to any system or group. When the number of observations reaches the defined threshold, this policy is applied to **My Organization** (all systems and groups in your organization).

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select **Solidcore 8.x.x: Application Control** for the product.
3. Click the **Throttling Rules** policy.
4. From the **Rule Groups** pane, select **Stop Observation Requests**.
5. Select the **Filters** tab.
6. Review the listed rules.

Restart observation generation for throttling

After you process existing requests and define rules for the accumulated requests, restart observation generation at endpoints.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery**.

   The **Policy Discovery** page displays a message stating that the observation generation has stopped.

2. In the warning message, click **Enable Observation Generation**.

Exit Observe mode

Once you are done monitoring the system and logging observations, you must exit Observe Mode.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. You can apply a client task to a group or an endpoint:
   - Group — Select the group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
   - Endpoint — Select the endpoint on the **Systems** page and click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select **Solidcore 8.x.x** → **SC: Observe Mode** and click **Create New Task** to open the **Client Task Catalog** page.

a. Specify the task name and add any descriptive information.
b. Select **End Observe Mode** and choose to place the endpoints in Enabled or Disabled mode.

5. Click **Save**, then click **Next** to open the **Schedule** page.
6. Specify scheduling details, click **Next**, then click **Save**.
7. (Optional) Wake up the agent to send your client task to the endpoint immediately.

Using Application Control in Inventory mode

What is Inventory mode?

Inventory mode creates the inventory that contains information about the executable and script files present on the endpoint. The information includes complete file name, file size, SHA-1, SHA-256, file reputation, file type, embedded application name, certificate details, and version.

Inventory mode tracks and records each change made to an endpoint's inventory. Also, it dynamically updates the inventory to make sure that the changed or added binaries and files are included in the inventory.

In Inventory mode, initial solidification process is needed to create the inventory that is sent to the McAfee ePO server.

Important

When an endpoint is in Inventory Mode, Application Control is not protecting your system. It does not prevent the execution of not whitelisted scripts. Only error, status transition, and pull inventory events are generated and sent to the McAfee ePO server.

Place endpoints in Inventory mode

You can place the endpoints in Inventory mode after a fresh installation or after an upgrade.

After a fresh installation, you can select **Start Inventory mode** when enabling the product with Application Control license.

Important

When you select **Start Inventory mode**, the system is resolidified automatically.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Select a group or an endpoint:
    - Group — Go to **System Tree** and click the **Assigned Client Tasks** tab.
    - Endpoint — On the **Systems** tab, select the endpoint you want to work with and click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
    a. For **Product**, select **Solidcore 8.3.x** (or later).
    b. For **Task Type**, select **SC: Enable**.
    c. Click **Create New Task** to open the **Client Task Catalog** page.
    d. Enter the task name and add any descriptive information.
    e. Select **Windows** for the platform, **All except NT/2000** for the sub-platform, then select **Application Control**.

f. Specify the activation option.

- **Limited Feature Activation** — If Application Control is not in Disabled mode, endpoints must be restarted manually.
- **Full Feature Activation** — Endpoints are restarted.

g. Select **Start Inventory Mode**.

h. Click **Save**.

4. Schedule the task, then click **Save**.
5. (Optional) Click **Wake Up Agents** to send the client task to the endpoint immediately.

What to do next

Important

You can also place the endpoints in Inventory mode by choosing the task **SC: Begin Inventory Mode**. You must solidify the system manually after running this task.

Exit Inventory mode

You can exit Inventory mode by switching to Disabled mode.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Select a group or an endpoint.
3. Click **Actions** → **Agent** → **Run Client Task Now**.
4. Select **Solidcore 8.3.x** (or later) for the product, then select one of these task types:
   - **SC: Disable** — Click **Create New Task**, then select **Reboot endpoint**.
   - **SC: End Inventory mode**.
5. Click **Run Task Now**.

What to do next

Important

If you choose the task **SC: End Inventory mode**, you must reboot the system manually after running the task.

Inventory mode events in McAfee ePO

This table provides a detailed list of all Inventory mode events.

Event ID on endpoints	Threat Event ID on McAfee ePO	Event Name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
147	20846	BOOTING_INVENTORY_MODE	Booted in Inventory Mode	Information	Information	SC
148	20847	INVENTORY_MODE_DEFERRED	Inventory Mode on Reboot	Information	Information	SC
149	20848	END_INVENTORY_MODE_DEFERRED	Closed Inventory Mode	Information	Information	SC
145	20844	PULL_INVENTORY_ENDED	Pull Inventory Completed	Information	Information	SC

Self-approval requests

What is self-approval?

Application Control prevents any new or unknown applications from running on protected endpoints. When the self-approval feature is enabled and users try to run an unknown or new application on a protected endpoint, they are prompted to approve or deny the application execution.

Important

Self-approval is available only in a McAfee ePO managed environment.

When a user approves the application execution, the business need or justification, if any, provided by the user for running the application is sent to the McAfee ePO administrator. The administrator reviews the approval request and can define rules to allow or ban the application for one or all endpoints in the enterprise.

The rules that are applied through policies have precedence over the self-approval feature. For example, if the self-approval feature is enabled and the user tries to run an application that is banned through a policy, the user isn't prompted to take action. Also, you can't self-approve and perform any actions that are prevented by Application Control memory-protection techniques.

The self-approval feature is available for binary or executable files, scripts, installers, ActiveX controls, and supported files that you run from network shares and removable devices. This feature is available on all supported Windows platforms except Windows NT, Windows 2000, and Windows 2003 (IA-64 platform).

Note

Although the self-approval feature is available in Limited Feature Activation mode, use this feature in Full Feature Activation mode (after restarting the endpoints). This feature requires patching of some system libraries and patching might require a restart to work effectively.

Enable self-approval on endpoints

By default, the self-approval feature is disabled on endpoints. You can configure a policy to enable this feature on selected endpoints.

After the feature is enabled, users can approve an unknown or new application on a protected endpoint and run it.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select **Solidcore 8.x.x: Application Control** for the product.
3. Select **Application Control Options (Windows)** for the category.
4. Click the **My Default** policy to edit it.

Note

By default, the **My Default** policy is applied to all endpoints in your enterprise. To enable the self-approval feature for selected endpoints, duplicate the **My Default** policy, edit the settings, and apply the policy to only the relevant endpoints.

5. Select **Enable Self-Approval**.
6. (Optional) Specify the message to display to the users on the endpoints when they try to run a new or unknown application. This specified text is displayed on the endpoint in the **McAfee Application Control - Self-Approval** dialog box.
7. Specify a timeout value for the user to take an action when the **McAfee Application Control – Self-Approval** dialog box is displayed.
   If the user doesn't take action in the specified time, the attempted action is automatically denied and the dialog box closes.
8. Specify whether it is mandatory or optional for the user to provide a business need while allowing an action on the endpoint.
9. (Optional) Specify the advanced options.
   If you select this option, all applications that run on the system while it is booting or when an interactive session is unavailable are allowed to execute.
10. Save the policy and apply to endpoints.
    After the policy is applied, the self-approval feature is enabled on the endpoints.

Self-approval dialog box

When users try to run a new application on the endpoints, the **McAfee Application Control - Self-Approval** dialog box indicates that execution of the application has been detected and prompts the user to take action.

For trusted and malicious executable files and certificates, execution is determined based on reputation received from the configured reputation source. So, the **McAfee Application Control - Self-Approval** dialog box isn't displayed for trusted and malicious files. But, if the file or certificate reputation is unknown, the **McAfee Application Control - Self-Approval** dialog box prompts the user to take action. Perform one of these tasks:

- Provide a justification (if mandatory) and click **Allow** to allow the action immediately. When you choose to self-approve the action, an approval request is sent to the administrator who reviews the provided justification to determine whether to allow or ban the action for one or more endpoints in the enterprise. The McAfee ePO administrator allows the action only if it is in accordance with the corporate policies and the application is trusted and known.
- Click **Deny** to deny the action. Users can deny the action when it isn't user-initiated or the changes seem irrelevant. The deny action is event-specific. If the same event is generated again, the user is prompted again to take an action.
  Users can review the event notifications and request approval for certain actions.
  - Right-click the McAfee Agent icon in the notification area on the endpoint.
  - Select **Quick Settings** → **Application and Change Control Events**.
  - Request approval for an action from the McAfee ePO administrator by selecting the event and clicking **Request Approval**. The McAfee ePO administrator receives an email including all relevant event details and a link. The administrator can click the link to open the needed event in the **Solidcore Events** page and define needed rules.

Policy discovery permissions

By default, non-global administrators can view, manage, and delete requests generated only by endpoints in their associated group (in **My Organization**).

If you review request details about the **Request Details** page, the number of requests listed in the **Enterprise Level Activity** pane might be less than the value displayed in the **Global Prevalence** column on the **Policy Discovery** page. This is because the **Global Prevalence** column indicates the enterprise-wide prevalence for the requests regardless of any groups. For example, if a request is generated by two systems in different groups across the enterprise, the value in the **Global Prevalence** is 2. But, because non-global administrators can only view the requests generated for their group, the non-global administrator might see only one request generated by the system in their group in the **Enterprise Level Activity** pane.

Note

The McAfee ePO administrator can review and manage all requests generated in the enterprise (**My Organization**). Also, McAfee ePO administrator can add rules to any rule group, and provide permissions to all non-global administrators to review and take custom actions on the requests generated in the enterprise.

If you are a non-global administrator, you can add rules (for a request) to only the rule groups that you own. Rule groups that you don't own are not displayed on the **Policy Discovery: Custom Rules** page. Also, if you take an action for a request, the action doesn't impact the same request generated by the system in a different group.

Allow non-global administrators to manage enterprise-wide requests

If you are a McAfee ePO administrator, you can assign permissions to all non-global administrators (who have access to groups in **My Organization**) to review and manage requests generated in your enterprise.

Task

1. On the McAfee ePO console, select **Menu** → **Configuration** → **Server Settings**.
2. From the **Setting Categories** pane, select **Solidcore**, then click **Edit** to open the **Edit Solidcore** page.
3. Change the value of **Allow group administrators to manage Policy Discovery requests for entire System Tree** to **Yes (overrides System Tree group access permissions)**.
4. Click **Save**.

Results

All non-global administrators are allowed to review and take custom actions on enterprise-wide requests. Non-global administrators can't perform global actions.

Review approval requests

Review the requests received from the endpoints.

On the **Solidcore: Health Monitoring** dashboard, check the **Top 10 Pending Policy Discovery Requests** monitor to take notice of the data that might require immediate action.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page. After the requests are received from the endpoints, Application Control collates and groups requests based on these parameters.
    - SHA-1 value of the executable file or .cab file (if there is a request for an ActiveX control) where the request is received.

      Note

      Although Application Control supports SHA-256 value of files, only SHA-1 values are used for collating and grouping requests on the **Policy Discovery** page.

    - Status of the request.

   Note

   The **Activity** field for each request indicates the action performed by the user on the endpoint. For example, if the user installs MSI-based software, the **Activity** field lists Software Installation for the request.

2. Review the listed requests using one of these methods.
    - **Specific interval** — Select an option from the **Time Filter** list and click **Update Results** to view requests received in a specific interval.
    - **Request status** — Select a value for the request status from the **Approval Status** list and click **Update Results** to view requests that match the selected status.
    - **Activity** — Select a value from the **Activity** list and click **Update Results** to view requests for a certain activity.
    - **Reputation** — Select a value from the **Final Reputation** list and click **Update Results** to view requests for files that match the selected reputation level. For more information about how the software determines final reputation for files or certificates, click **What's Final Reputation**.
    - **Specific endpoint** — Enter an endpoint name in the **System Name** field and click **Update Results** to view requests received from the endpoint. Make sure that you specify the complete system name because no partial matches are performed.
    - **Multiple criteria** — Specify values for the **Time Filter**, **Approval Status**, **Activity**, **Final Reputation**, and **System Name** fields, as needed, and click **Update Results** to perform a search based on multiple criteria.
    - **Specific search string** — Enter a search string in the **Quick find** field and click **Apply** to view requests that match the specified search string. Partial matches are performed based on the text you specify.

Note

You can enter **User Comments** field value as a search string.

- **Sort** — Sort the list based on the global prevalence, execution time, activity, object name, application name, certificate, final reputation, or reputation source by clicking the column heading.
- **Selected requests** — Select requests of interest and click **Show selected rows** to review only the selected requests.

Note

The **Policy Discovery** page lists only the requests for which the McAfee ePO administrator can make rules. To view other requests, such as those for software uninstall, run the **Self-Approval Audit Report** query. This report lists all requests received from the endpoints in the last month.

3. Review individual requests that make up a collated request and detailed information for the file.
   a. Click a row to open the **Request Details** page.
   b. Review file details, such as name, version, path, parent process, files changed, and final reputation.
   c. Review the SHA-1, SHA-256, and MD5 information for the file.
   d. Click the file SHA-1 to review file details about the **File Details** page.
   e. Review the certificate vendor name for the file. The certificate vendor name for a file is color coded to indicate trusted (green), malicious (red), or unknown (orange) reputation.
   f. Click certificate name to view certificate details, such as issuer, certificate reputation, reputation source, public key algorithm, public key length, public key hash, certificate hash, valid from, and valid to.
   g. Review the individual requests that make up the collated request in the **Enterprise Level Activity** pane.
   h. Click **Close**.

Process approval requests

When the self-approval feature is enabled, administrators receive approval requests from users. Administrators review the requests and can define rules for one or all endpoints.

The reputation value for a file is color-coded to indicate trusted, malicious, and unknown reputation:

- Values in green indicate that the file is **Known Trusted**, **Most Likely Trusted**, or **Might be Trusted**.
- Values in orange indicate that the file is unknown.
- Values in red indicate that the file is **Known Malicious**, **Most Likely Malicious**, or **Might be Malicious**.
- Values in grey indicate that reputation value is Not applicable (only for network path execution requests).

The reputation source indicates the source from where the reputation is fetched. Possible values for reputation source are **TIE**, **GTI**, **Application Control**, **Not synchronized**, or **Not Applicable**. If you click the TIE value, it opens the **TIE Reputations** page where you can view relevant details for the selected file.

Allow a file on all endpoints

You can define rules to allow an application or executable file to run on all endpoints in the enterprise.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the requests where you want to define rules.
3. Click **Actions** → **Allow File Globally**.
   The **Allow File Globally** dialog box provides details and prompts you to confirm the action.
4. Click **OK**.

Results

Rules are created for the files associated with the selected requests and added to the Global Rules rule group included in the **McAfee Default** policy.

Allow a file by certificate

You can define rules to allow an application, executable file, or ActiveX control to run on all endpoints in the enterprise based on the certificate associated with the file.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the request where you want to define rules.
3. Click **Actions** → **Allow by Certificate Globally**.
4. The **Allow by Certificate Globally** dialog box provides details and prompts you to confirm the action. Based on the file associated with a selected request, the certificate is assigned or not assigned updater privileges. If the certificate has updater privileges, allowing based on certificate allows all applications signed by the certificate to make changes to existing executable files or start new applications on the endpoints.
5. Click **OK**.

   Note

   The **Allow by Certificate Globally** action is unavailable if the main executable associated with the request is signed by a certificate included in the Restricted certificate names list.

Ban by SHA-1 or SHA-256 on all endpoints

You can define rules to ban an application or executable file from running on all endpoints in the enterprise based on the SHA-1 or SHA-256 value of the file.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the requests where you want to define rules.
3. Click **Actions** → **Ban File Globally**.
   The **Ban File Globally** dialog box provides details and prompts you to confirm the action.
4. Click **OK**.
   Rules are created for the files associated with the selected requests and added to the Global Rules rule group included in the **McAfee Default** policy.
5. Ban the files that have already been added to the endpoint.
   a. Click the application name link.
      The **Files** page lists all executable files installed on the endpoint.
   b. Select all listed files.
   c. Click **Actions** → **Ban Files** to open the **Allow or Ban Files** wizard.
   d. Specify the rule group for the rules.
      - To add the rules to an existing rule group, select **Add to Existing Rule Group**, select the rule group from the list, and specify the operating system.
      - To create a rule group with the rules, select **Create a New Rule Group**, enter the rule group name, and specify the operating system.
   e. Make sure that the rule group where you add the rules is added to a policy that is applied on the endpoint where the request was received.
   f. Click **Next**.
   g. Review the rules, then click **Save**.

Define rules for specific endpoints

You can add prepopulated rules to allow or ban an application, executable file, or ActiveX control for specific endpoints in your administered groups. Or, you can define custom rules for specific endpoints or groups, as needed.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the request where you want to define custom rules.
3. Click **Actions** → **Create Custom Policy** to open the **Policy Discovery: Custom Rules** page.
4. You can review rules or define rules:
   - **Review and add prepopulated rules** – Select **Approve Request**, **Ban Request**, or **Allow By Certificate**.
   - **Define custom rules** – Select **Clear and define Rules**.
5. Specify the rule group for the rules.
   - To add the rules to an existing rule group, select **Choose existing** and select the rule group from the list.
   - To create a rule group with the rules, select **Create new** and enter the rule group name.

6. (Optional) Add the changed or created rule group to a policy.
    a. Select **Add rule group to existing policy**.
    b. Select the policy where you want to add the rule group.
7. Click **Save**.

Results

This approves all grouped requests.

Allow by adding to whitelist for specific endpoints

You can add one or more executable files to the whitelist to allow the files to run on the endpoint.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Click a row to review request details in the **Request Details** page.
   Each row in the **Enterprise level activity** pane represents an executable file and endpoint combination.
3. Click **Allow Locally** for a row.
   The **Allow Locally** dialog box lists one or more paths to add to the whitelist.

   Note

   The **Allow Locally** action is available only for requests that are generated when you execute an application that isn't in the whitelist (Application Execution activity).

4. Review and customize the listed paths.

   For example, if you execute proc.exe for an endpoint, these paths might be listed.

   C:\Program Files\<App Name>\proc.exe

   C:\Program Files\<App Name>\a.dll

   C:\Program Files\<App Name>\b.dll

   To avoid redundancy, add only the C:\Program Files\App Name path.

5. Click **OK**.

Results

The specified paths are added to the whitelist and allowed to run on the endpoint.

Change file reputation

Application Control works with multiple sources to fetch reputation information. The software regularly synchronizes with TIE and McAfee GTI. You can review or edit the reputation for a file on the **TIE Reputations** page.

Task

1. Select **Menu** → **Application Control** → **Policy Discovery**.
2. On the **Policy Discovery** page, select a request and click **Actions** → **More** → **Change File Reputation (TIE)**
3. Review the file information about the **TIE Reputations** page.
4. (Optional) Edit file reputation: click **Actions**, then select an action.

Delete requests

You can remove requests from the **Policy Discovery** page and database.

Note

For optimal performance, the **Solidcore: Auto Purge Policy Discovery Requests** server task is run weekly to remove policy discovery requests older than three months.

Task

1. On the McAfee ePO console, select **Menu** → **Application Control** → **Policy Discovery** to open the **Policy Discovery** page.
2. Select the requests to delete.
3. Click **Actions** → **Delete Requests**.
4. When prompted to confirm, click **OK**.

Results

All selected collated requests and contained individual requests are deleted from the page and database.

Maintaining your system in a managed environment

Monitoring enterprise health

You can monitor the health of the protected endpoints in the enterprise. The **Solidcore: Health Monitoring** dashboard provides health status at-a-glance.

The **Solidcore: Health Monitoring** dashboard includes specific monitors to indicate congestion levels for inventory items and observations on the McAfee ePO console. You can also add more monitors to review congestion for self-approval requests and client task logs. Possible values for the congestion levels are **No congestion**, **Low**, **Moderate**, **High**, and **Data deleted**.

Congestion level value	Value for trend monitors	Description
No congestion	0	This value indicates that no congestion is present in the McAfee ePO database.
Low	1	This value indicates that data older than 5 days is present in the McAfee ePO database and is yet to be parsed by the software. Typically, **Low** congestion levels are automatically resolved. When congestion begins, the **Data Congestion Detected** event is generated to notify the user.
Moderate	2	This value indicates that data older than 5 days is still present in the McAfee ePO database and is yet to be parsed by the software. You might experience sluggish responses from the user interface at this stage. When congestion levels reach **Moderate**, the **Data Congestion Detected** event is generated to notify the user.
High	3	This value indicates that data older than 5 days is still not parsed by the software and the McAfee ePO database is choked. If the congestion level reaches **High**, old data is deleted from the McAfee ePO database to resolve congestion. When congestion levels reach **High**, the **Data Congestion Detected** event is generated to notify the user.
Data deleted	3	This value indicates that data pending for parsing for the feature has been deleted from endpoints to resolve congestion. When data is deleted from the McAfee ePO database, the **Clogged Data Deleted** event is generated to notify the user.

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 displays 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 environment. 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 displays 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.

Review congestion status and trend

You can review the monitors on the **Solidcore: Health Monitoring** dashboard to assess enterprise health status and trend.

Task

1. Select **Menu** → **Reporting** → **Dashboards**.
2. Select the **Solidcore: Health Monitoring** dashboard from the **Dashboard** list.

You can review the overall health of the enterprise.

3. Review congestion levels for inventory items:
    - Review the **Inventory Data Congestion Level** monitor to validate if congestion is present for inventory items in the McAfee ePO database.
    - Check the **Inventory Data Congestion Trend in Last 7 Days** monitor to review the weekly trend.
4. Review observation requests:
    - Review the **Observations Data Congestion Level** monitor to validate if congestion is present for observations in the McAfee ePO database.
    - Check the **Observations Data Congestion Trend in Last 7 Days** monitor to review the weekly trend.
5. (Optional) Review congestion levels for self-approval requests and client task logs.
    a. From the McAfee ePO console, select **Dashboard Actions** → **Duplicate** for **Solidcore: Health Monitoring** dashboard, click **OK** in the **Duplicate Dashboard** dialog box, then click **Add Monitor**.
    b. Select **Solidcore** from the **Category** list.
    c. Click and drag the **Self-Approval Data Congestion Level** and **Client Task Logs Data Congestion Level** monitors.
    d. Select **Queries** from the **Category** list.
    e. Click and drag the **Queries** monitor.
    f. In the **New Monitor** dialog box, click the **Monitor Content** drop-down list.
    g. Navigate to the **McAfee Groups - Solidcore Health Monitoring** section (McAfee ePO console), select the **Self-Approval Data Congestion Trend in Last 7 Days** query, and click **OK**.
    h. Repeat steps d through g for the **Client Task Logs Data Congestion Trend in Last 7 Days** query.
    i. Review the **Self-Approval Data Congestion Level** and the **Self-Approval Data Congestion Trend in Last 7 Days** to review the weekly trend.
    j. Review the **Client Task Logs Data Congestion Level** and the **Client Task Logs Data Congestion Trend in Last 7 Days** monitor to review the weekly trend.

Why to configure notifications?

Configure alerts or automatic responses to receive notifications about important incidents such as bad binary detected, data throttled, or data congestion detected in your environment.

- To receive notifications for Known Malicious and Might be Malicious files or certificates encountered in your setup, enable the **Bad Binary has been detected in Enterprise** automatic response from the **Menu** → **Automation** → **Automatic Responses** page.
- 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 notifications

You can configure alerts or automatic responses to receive a notification when data congestion begins for your environment.

To receive a notification when congestion begins for your setup, you can configure an alert for the **Data Congestion Detected** event. Similarly, to receive a notification when data is deleted from the McAfee ePO database to resolve congestion, you can configure an alert for the **Clogged Data Deleted** event.

Task

1. Select **Menu** → **Automation** → **Automatic Responses**.
2. Click **Actions** → **New Response**, then enter the alert name.
3. Select the **ePO Notification Events** group and **Threat** event type.
4. Select **Enabled**, then click **Next** to open the **Filter** page.
5. Select **My Organization** for the **Defined at** property, then Select **Threat Name** from the **Available Properties** pane.
6. Include this information in the **Value** field:
    a. Type `DATA_CONGESTION_DETECTED` and click **+**.
    b. Type `CLOGGED_DATA_DELETED` and click **Next**.
7. Specify aggregation details, then click **Next** to open the **Actions** page.
8. Select **Send Email**, specify the email details, and click **Next** to open the **Summary** page, then review the details and click **Save**.

Making emergency changes

To implement an emergency change, you can create a change window that overrides all protection and tamper proofing that is in effect. Use a change window only when the other available mechanisms can't be used.

Place the endpoints in Update mode, then make the required emergency changes and place the endpoints in Enabled mode.

Switch to Update mode

Place the endpoints in Update mode to make emergency changes.

Task

1. Select **Menu** → **Systems** → **System Tree**.
2. Perform one of these actions.
    - Group — Select a group in the **System Tree** and click the **Assigned Client Tasks** tab.
    - Endpoint — Select the endpoint on the **Systems** page, then click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.

4. Select **Solidcore 8.x.x** for the product, **SC: Begin Update Mode** task type, then click **Create New Task** to open the **Client Task Catalog** page.
    a. Specify the task name and add any descriptive information.
    b. Enter the Workflow ID and any comments you want.
    c. Click **Save**.
5. Click **Next** to open the **Schedule** page.
6. Specify scheduling details, then click **Next**.
7. Review and verify the task details, then click **Save**.

Exit Update mode

Place the endpoints back in Enabled mode after you complete the required changes in Update mode.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Perform one of these actions.
    - To apply the client task to a group, select a group in the **System Tree** and click the **Assigned Client Tasks** tab.
    - To apply the client task to an endpoint, select the endpoint on the **Systems** page, then click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
    a. Select **Solidcore 8.x.x** for the product, **SC: End Update Mode** for the task type, then click **Create New Task** to open the **Client Task Catalog** page.
    b. Specify the task name and add any information you want.
    c. Click **Save**, then click **Next**.
    d. Specify the task name and add any information you want.
    e. Specify scheduling details, then click **Next**.
    f. Review and verify the task details, then click **Save**.
4. (Optional) Wake up the agent to send your client task to the endpoint immediately.

Administering throttling for your enterprise

When several events, policy discovery requests (observations), or inventory updates are received on the McAfee ePO server, the McAfee ePO interface might become unresponsive or sluggish. The throttling feature helps avoid such scenarios.

You can control the flow of events, policy discovery requests, and inventory updates. When the data sent to the McAfee ePO server reaches the defined threshold for an endpoint, throttling is initiated and these actions are taken.

1. Data is no longer sent to the McAfee ePO server.
2. Data is stored in a cache at the endpoints. When the cache is full, data starts dropping with the oldest.

Note

Data is stored in the cache only for event and policy discovery requests. The inventory data isn't stored in the cache; instead, it is updated at the endpoints locally.

3. Throttling is reset no less than 24 hours after the first event, policy discovery request, or inventory update for the day.

   Note

   When throttling of inventory updates is initiated, the **Pull Inventory** client task is disabled. This indicates that you can't fetch inventory until throttling resets.

4. Data stored in the cache is sent to the McAfee ePO server in batches (starting with the oldest data).

After throttling resets for events and policy discovery requests, further generated data is stored in the cache and not sent to the McAfee ePO server until the cache is empty.

The throttling feature is available on all supported Windows platforms. You can manage throttling by identifying the endpoints where throttling is initiated and taking remedial actions. If needed, you can configure throttling for your enterprise.

Set up throttling

By default, the throttling feature is enabled for events, inventory updates, and policy discovery requests.

Enabling or disabling this feature also enables or disables all its subfeatures.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.x.x: General** product.
3. In the **Configuration (Client)** category, click **Duplicate** for the **McAfee Default** policy.
4. Specify the policy name, then click **OK**.
5. Open the policy and click the **Throttling** tab.
6. Enable or disable throttling by clicking **Enable Throttling**.
   This enables or disables the throttling feature for events, inventory updates, and policy discovery requests.
7. (Optional) Disable the throttling feature selectively for **Events**, **Inventory Updates**, and **Policy Discovery (Observations)**.
   When the throttling feature is enabled, you can disable one or more types of throttling by deselecting the corresponding checkbox.
8. Save the policy and apply it to the relevant endpoints.

Configure throttling values

For most enterprises, the default settings for the throttling feature are enough. But, if needed, you can change the default configuration for the feature.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select **Solidcore 8.x.x: General** for the product.
3. In the **Configuration (Client)** category, click **Duplicate** for the **McAfee Default** policy.
4. Specify the policy name, then click **OK**.
5. Open the policy and click the **Throttling** tab.
6. Edit the values for events, inventory updates, and policy discovery requests, as needed.

Value	Description
Events	The value for threshold and cache size is defined in number of event XML files. By default, 2000 XML files can be processed per endpoint in 24 hours. Also, the default event cache size is set to 7000 XML files per endpoint.
Inventory Updates	The value for threshold is defined in number of file elements containing inventory updates. By default, 15000 files elements can be processed per endpoint in 24 hours.
Policy Discovery (Observations)	The value for threshold and cache size is defined in number of request XML files. By default, 100 XML files can be processed per endpoint in 24 hours. Also, the default event cache size is set to 700 XML files per endpoint.

7. Save the policy and apply it to the relevant endpoints.

Manage throttling

You can determine if throttling is initiated for any endpoint in your setup and you can take action to manage the feature.

On the **Solidcore: Health Monitoring** dashboard, check the **Number of Systems where Throttling Initiated in Last 7 days** monitor to take notice of the systems that might require immediate action.

Task

1. Determine if throttling is initiated and identify the affected endpoints.

Event	Description
Data Throttled	Generated for an endpoint when event or policy discovery request throttling is initiated. After throttling resets, this event is generated daily until the cache is empty.

Event	Description
Data Dropped	Generated in 2 scenarios for an endpoint. • When the cache is full and the oldest data is dropped from the event or request cache. • When throttling of inventory updates is initiated for the endpoint.

2. Review the throttling status for each affected endpoint.
3. Process data generated for affected endpoints and create relevant rules. You *must* process data quickly to make sure that data isn't dropped.

Identify endpoints where throttling is initiated

You can identify endpoints where **Data Throttled** and **Data Dropped** events are generated.

You can create an automatic response for these events.

Task

1. On the McAfee ePO console, select **Menu** → **Reporting** → **Solidcore Events**.
2. Review the event list and locate endpoints where these events are generated.

Event	Action
Data Throttled	Review the **Object Name** column for information about throttling of events or policy discovery requests (observations) for the corresponding endpoints. Based on the type of throttling, you must immediately review the throttling status and process data for the endpoint to make sure that you don't lose data.
Data Dropped	Review the **Object Name** column for information about throttling of inventory updates. This column also provides information if data has started dropping for events and policy discovery requests (observations). Typically, this occurs when data isn't processed quickly for the endpoint. Based on the type of throttling, you must immediately process data or manage inventory updates.

Review throttling status

For endpoints where throttling is initiated, you can review the throttling status.

Task

1. From the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. On the **Systems** page, click the endpoint where throttling is initiated to view its details.
3. Click the **Products** tab.
4. Click the **Solidcore** row to view product details.
5. Review the values for the listed throttling properties.

Property	Description
Throttling Status: Events	Provides this information. • **Cache usage** This indicates the percentage of event or request cache that is already used by the stored events or requests. • **Number of dropped events or requests** When the cache usage reaches 100%, events or requests start dropping and the **Data Dropped** event is generated and displayed on the **Threat Event Log** and **Solidcore Events** pages. • Time when the threshold was reached This indicates the time when event or request throttling was initiated.
Throttling Status: Policy Discovery (Observations)	
Inventory Fetch Time (Last)	Indicates the time when the inventory was last fetched. When throttling of inventory updates is initiated, the **Pull Inventory** client task is disabled and you can't fetch the inventory until throttling resets.
Inventory Fetch Time (Next)	Indicates the time when you can fetch the inventory for the endpoint. When throttling of inventory updates resets (24 hours after the first inventory update was generated), the **Pull Inventory** client task is enabled again to allow you to fetch the inventory. In such scenarios, this property displays the time when throttling resets.

Process data where throttling is initiated

On endpoints where throttling is initiated, you can create relevant rules or filters to process data. This helps you control the flow of data by gradually reducing the amount of received data.

Task

On the McAfee ePO console, take relevant actions based on the type of data.

a. Events — Select **Menu** → **Reporting** → **Solidcore Events**.
   On the identified endpoints where throttling is initiated, review the generated events, then create relevant rules for events based on details such as event type, generation time, and number of occurrences. Define advanced exclusion filters to exclude non-meaningful events from the endpoints.
b. Requests — Create relevant rules to process requests and define advanced exclusion filters to exclude non-meaningful requests from the endpoints.
c. Inventory updates — Define advanced exclusion filters to exclude non-meaningful inventory updates from the endpoints.

Configure CLI breach notifications

Administrators need to be aware of any attempt to recover the CLI with an incorrect password. In case any attempt is made to breach security, the CLI needs to be disabled immediately to thwart the attempt.

You can configure Application Control and Change Control products to notify the administrator of any unsuccessful attempts to recover the CLI on the endpoint.

Note

This feature is available only in McAfee ePO-managed configuration and unavailable in standalone configuration.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select **Solidcore 8.x.x: General** for the product.
3. In the **Configuration (Client)** category, click **Duplicate** for the **McAfee Default** policy.
4. Specify the policy name, then click **OK**.
5. Open the policy and click the **CLI** tab.
6. Enable the feature by clicking **Enable**.
   By default, this feature is disabled.
7. Specify the number of failed attempts and the interval after which to disable the CLI in case of a security breach.
   By default, the CLI is disabled if a user makes three unsuccessful attempts in 30 minutes.
8. Specify how long to disable the CLI if any user makes unsuccessful logon attempts.
   By default the CLI is disabled for 30 minutes.
9. Click **Save**.
10. Apply the policy to the endpoints.

Results

After you enable the feature:

- Each attempt to recover the CLI with the correct password generates the **Recovered Local CLI** event.
- Any attempt to recover the CLI with an incorrect password generates the **Unable to Recover Local CLI** event.

When the user exceeds the permitted number of failed attempts (as defined in the policy), the CLI recovery is disabled to prevent the breach attempt. The **Disabled Local CLI Access** event is generated. This is priority event and is sent immediately to the McAfee ePO console.

Change the CLI password

You can change the default command line interface (CLI) password to prevent others from accessing the CLI.

Task

1. On the McAfee ePO console, select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.x.x: General** product.
3. In the **Configuration (Client)** category, click **Duplicate** for the **McAfee Default** policy.
   The **Duplicate Existing Policy** dialog box appears.
4. Specify the policy name, then click **OK**.
   The policy is created and listed on the **Policy Catalog** page.
5. Click the policy to open it and type the new password in the **CLI** tab.
6. Confirm the password.
7. Click **Save** and apply the policy to the endpoints.

Collect debug information

Before contacting McAfee Support to help you with a Solidcore client issue, collect configuration and debug information for your setup.

This helps McAfee Support quickly identify and resolve the issue. Run the **Collect Debug Info** client task to create an archive with endpoint configuration information and Solidcore client log files. The .zip file is generated on the endpoint and its location is listed on the **Client Task Log** page. Send the .zip file to McAfee Support with details of the encountered issue.

Create a .zip file with configuration and debug information.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Perform one of these actions.
   - Group — Select a group in the **System Tree** and click the **Assigned Client Tasks** tab.
   - Endpoint — Select the endpoint on the **Systems** page, then click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select **Solidcore 8.x.x** for the product, **SC: Collect Debug Info** task type, then click **Create New Task** to open the **Client Task Catalog** page.

5. Specify the task name and add any descriptive information.
6. Click **Save**, then click **Next** to open the **Schedule** page.
7. Specify scheduling details, then click **Next**.
8. Review and verify the task details, then click **Save**.

Place the endpoints in Disabled mode

When you place the endpoints in Disabled mode, the software isn't in effect. Although it is installed, the associated features aren't active.

Task

1. Select **Menu** → **Systems** → **System Tree**.
2. Perform one of these actions.
   - Group — Select a group in the **System Tree** and click the **Assigned Client Tasks** tab.
   - Endpoint — Select the endpoint on the **Systems** page, then click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select **Solidcore 8.x.x** for the product, **SC: Disable** task type, then click **Create New Task** to open the **Client Task Catalog** page.
5. Specify the task name and add any descriptive information.
6. Select **Reboot endpoint**.
7. Click **Save**, then click **Next** to open the **Schedule** page.
8. Specify scheduling details, click **Next**, then click **Save**.
9. (Optional) Wake up the agent to send your client task to the endpoint immediately.

Sending McAfee GTI feedback

Application Control includes seeded server tasks to send feedback to McAfee about your current use of the McAfee GTI and Application Control features.

- **Solidcore: Send Event Feedback to McAfee GTI Server** (disabled by default)
- **Solidcore: Send Policy and Inventory Feedback to McAfee GTI Server** (enabled by default to run daily)
- **Solidcore: Send Policy Discovery Request Feedback to McAfee GTI Server** (enabled by default to run daily)

Note

No information about individual computers or users is sent to McAfee. McAfee stores no data that can be used to track the feedback information to a specific customer or organization.

Server task settings

You can configure the server tasks to send information about how you are currently using one or all these parameters.

Events	Send information, such as file name and SHA-1 for the Execution Denied, Process Hijack Attempted, and Nx Violation Detected events. You can also send information about the number of endpoints where the event occurred with the full path of the file. This information helps McAfee determine how frequently and effectively Application Control blocks actions, and helps to improve product functionality and efficacy.
Policies	Send information about user-editable Change Control, Application Control, and General policies. Information is also sent for the Global Rules and Global Observation Rules (Deprecated) rule groups. This information helps McAfee understand how you are currently using polices and applying rules, and helps to improve the default policies and rules.
Inventory	Send detailed information for files, including base name, application name, application version, file version, and enterprise trust level. You can also send information about the number of endpoints where the file is present, its execution status, and full path of the file. The feedback does not include any information to identify the endpoints, such as system name or IP address. This information helps McAfee determine how you are using (and changing) the File Hash Trust Score (GTI) and File Hash Reputation (GTI) values assigned to files. This information also helps to improve the McAfee GTI file reputation service.
Policy Discovery requests	SenMcAfee GTId information for policy discovery requests and include details about the certificate associated with the file. This information helps McAfee determine the type of requests generated for your setup and identify certificates associated with commonly used applications.
ePO base information	Sends information about the number of nodes managed by McAfee ePO and number of nodes where Application Control is installed.

Configure server tasks

You can configure the server tasks that send feedback, as needed.

Task

1. On the McAfee ePO console, select **Menu** → **Automation** → **Server Tasks**.
2. Select **Edit** for a server task to open the Server Task Builder wizard.

3. Change the schedule status for the task.
4. Click **Save**.

Purge reporting data

You can purge Solidcore reporting data by age or other parameters. When you purge data, the records are permanently deleted.

Task

1. On the McAfee ePO console, select **Menu** → **Automation** → **Server Tasks**.
2. Click **New Task** to open the **Server Task Builder** wizard.
3. Type the task name, then click **Next**.
4. Select **Solidcore: Purge** from the **Actions** list.
5. Configure these options, as needed.
    - **Choose Feature** — Select the reporting feature for which to purge records.
    - **Purge records older than** — Select this option to purge the entries older than the specified age.
    - **Purge by query** — Select this option to purge the records for the selected feature that meet the query criteria. This option is only available for reporting features that support queries in McAfee ePO. Also, this option is supported only for tabular query results.

    Note

    No seeded queries are available for purging. Before purging records, you must create the query from the **Menu** → **Reporting** → **Queries & Reports** page.
6. Click **Next** to open the **Schedule** page.
7. Specify schedule details, then click **Next** open the **Summary** page.
8. Review and verify the details, then click **Save**.

Configuring Case sensitivity on ePO Managed Solidcore Client

McAfee Application and Change Control supports case sensitivity.

You can solidify and un-solidify files having the same name but with different case.

Note

Case sensitivity support is disabled by default on Windows 10 or below. When McAfee Application and Change Control is getting installed on Window 11, case sensitivity turns on by default.

Task

1. Follow these steps to enable case sensitivity on Windows 10:
   a. Disable **Solidcore** and reboot systems if **Solidcore** is in **Enable** mode.
   b. In McAfee ePO, go to **Client Task catalog** . Navigate to Solidcore 8.3.x, and click **New Task** and select **SC:Run Commands**.
   c. Enter **Task name** and in run config set:
   `InventoryCaseSensitivityEnabled=1`
   d. Add `Sadmin` clean command `(clean C:\)`.
   e. Send a task to resolidify the system and `Enable`.
2. Follow these steps to disable case sensitivity on Windows 10 and Windows 11:
   a. Disable **Solidcore** and reboot systems if **Solidcore** is in **Enable** mode.
   b. In McAfee ePO, go to **Client Task catalog** . Navigate to Solidcore 8.3.x, and click **New Task** and select **SC:Run Commands**.
   c. Enter **Task name** and in run config set:
   `InventoryCaseSensitivityEnabled=0` for Windows 10 and `InventoryCaseSensitivityEnabled=2` for Windows 11.
   d. Add `Sadmin` clean command `(clean C:\)`.
   e. Send a task to resolidify the system and `Enable`.

Maintaining your system in an unmanaged environment

View product status and version

You can view the status of Application Control, such as operational mode, operational mode after restart, and whitelist status.

You can also view details such as software version and copyright information.

Task

1. View Application Control status:

   `sadmin status [volume]`

   Include `[Volume]` to view details of a single volume.

   A message similar to this example displays the system details.

```
McAfee Solidifier:           Disabled
McAfee Solidifier on reboot: Disabled

ePO Managed:    No
Local CLI access: Recovered

[fstype]           [status]        [driver status]      [volume]
* NTFS        Solidified         Unattached           C:\
```

Status detail	Description
McAfee Solidifier	Specifies the operational mode of Application Control.
McAfee Solidifier on reboot	Specifies the operational mode of Application Control after system restart.
ePO Managed	Displays the connectivity status of Application Control with McAfee ePO. In standalone configuration of the product, this status is *No*.
Local CLI access	Displays the *lockdown* or *recovered* status of the local CLI. In standalone configuration of the product, this status is *Recovered*.
fstype	Displays the supported file systems for a volume.
status	Displays the current whitelist status for all supported volumes on a system. If a volume name is specified, only the whitelist status for that volume is displayed.

Status detail	Description
driver status	Displays whether the Application Control driver is loaded on a volume. If the driver is loaded on a volume, status is *attached*; otherwise the status is *unattached*.
volume	Displays the volume names.

2. View version and copyright details of Application Control installed on the system.
   `sadmin version`

Manage the whitelist

Configure whitelist thread priority

The whitelist thread priority (`SoPriority`) determines the usage of system resources and the time required to create the whitelist.

You can configure the whitelist thread priority before creating the initial whitelist. By default, the thread runs on low priority (value of 0) and if you do not specify the thread priority, Application Control considers the default priority to create the whitelist.

Task

Run this command and specify the `SoPriority` value.

- `sadmin config set SoPriority=<value>`

The `SoPriority` value that you specify should be based on your preference. This table describes the `SoPriority` values that you can specify.

Value	Priority	Advantages and disadvantages
0	Low (Recommended)	The low value, takes more time to create the whitelist but causes minimal performance impact on the system.
1	Medium	N/A
2	High	The high value takes less time but uses more system resources and can cause performance impact on the system.

Add and remove components from the whitelist

You can add new components to the initial whitelist to allow their execution on a protected system. If needed, you can remove components from the whitelist.

Task

Specify the components as file names, directory names, or volume names.

Action	Command syntax	Description
Add components to the whitelist.	`sadmin solidify [<arguments> <components>]`	After the initial whitelist is created, execution is blocked for the components that are not included in the whitelist. If needed, add more components to the whitelist.
Remove all components from the whitelist.	`sadmin unsolidify`	Remove all components from the whitelist using this command. When you remove components from the whitelist, they are no longer protected by Application Control.
Remove selected components from the whitelist.	`sadmin unsolidify [<arguments> <components>]`	Specify the components that you want to remove from the whitelist.

You can add or remove components from the whitelist as described in this table.

Component	Description
File name	Add files to the whitelist. For example, `sadmin solidify filename1 ... filenameN`
	Remove files from the whitelist. For example, `sadmin unsolidify filename1 ... filenameN`
Directory name	Add all supported files (recursively) under specified directories to the whitelist. For example, `sadmin solidify directoryname1 ... directorynameN`
	Remove all supported files in one or more directories from the whitelist. For example,

Component	Description
	`sadmin unsolidify directoryname1 ... directorynameN`
Volume name	Add all supported files (recursively) under specified system volumes to the whitelist. For example, `sadmin solidify volumename1 ... volumenameN`
	Remove all supported files in one or more system volumes from the whitelist. For example, `sadmin unsolidify volumename1 ... volumenameN`
File name Directory name Volume name	Optionally, you can specify supported arguments with the command. • **Add** — `sadmin solidify [ -q | -v ] filename1 ... filenameN | directoryname1 ... directorynameN | volumename1 ... volumenameN` • **Remove** — `sadmin unsolidify [ -v ] filename1 ... filenameN | directoryname1 ... directorynameN | volumename1 ... volumenameN` Here are the arguments descriptions: • The `-q` argument displays only error messages. • The `-v` argument displays all messages.

View whitelisted files

You can view lists of all whitelisted and non-whitelisted files, directories, and drives/volumes on your system.

Task

1. List all whitelisted components.
   - `sadmin list-solidified`
2. List all non-whitelisted components.
   - `sadmin list-unsolidified`

You can narrow the results by specifying components as described in this table.

Component	Description
File name	List all whitelisted files. If only one file name is specified, this command shows the file name only if it is whitelisted. `sadmin list-solidified filename1 ... filenameN`

Component	Description
	List all non-whitelisted files. If only one file name is specified, this command shows the file only if it is not whitelisted. `sadmin list-unsolidified filename1 ... filenameN`
Directory name	List all whitelisted files present in the specified directories. `sadmin list-solidified directoryname1...directorynameN`
	List all non-whitelisted files present in the specified directories. `sadmin list-unsolidified directoryname1...directorynameN`
Volume name	List all whitelisted files present in the specified drives/volumes. `sadmin list-solidified volumename1...volumenameN`
	List all non-whitelisted files present in specified volumes. `sadmin list-unsolidified volumename1...volumenameN`
File name Directory name Volume name	List details about the files, such as file type, file path, and file checksum. `sadmin list-solidified [ -l ] filename1 ... filenameN | directoryname1...directorynameN | volumename1...volumenameN`

Check and update the status of whitelisted components

You can compare the current whitelist status and checksum values of whitelisted files, directories, and volumes with the status and values stored in the whitelist. If they are not current, you can update the whitelist and fix inconsistencies.

If the components in the whitelist are changed or removed and the whitelist is not updated, the execution of these components is blocked. This results in inconsistencies in the whitelist.

Task

Run this command at the command prompt.

```
sadmin check [ -r ] file | directory | volume
```

You can narrow the results by specifying the names of files, directories, and drive/volumes with this command.

Also, you can specify the `-r` argument with this command. This argument fixes inconsistencies by updating the whitelist with the latest checksum values of the components and adds the components to the whitelist, if the components are not already present. If you don't specify a component, inconsistencies in all supported drives/volumes are fixed.

Review product features

You can review the list of all Application Control features and their status (enabled or disabled) on your system.

Task

Run this command at the command prompt.

```
sadmin features list
```

The features list is displayed on the screen.

Note

Starting from the Application Control 6.0.0 release, the features list has been minimized to show only the features that require changes regularly.

Feature	Description	Default status	Supported Operating System
activex	It installs and runs ActiveX controls on the protected system. Only the Internet Explorer browser is supported for the ActiveX control installations. Simultaneous installation of ActiveX controls using multiple tabs of Internet Explorer is not supported.	Enabled	Windows
checksum	It compares the checksum of the file to be executed with the checksum stored in the whitelist.	Enabled	Windows and Linux
deny-read	It read-protects the specified components. When this feature is applied on components, they cannot be read. Read protection works only when Application Control is running in Enabled mode.	Disabled	Windows and Linux
deny-write	It write-protects the specified components. When this feature is applied on the components, they are rendered as read-only to protect your data.	Enabled	Windows and Linux

Feature	Description	Default status	Supported Operating System
discover-updaters	It generates a list of potential updaters that can be included in the system. It tracks all failed attempts made by authorized executable to change protected files or run other executable files. It also generates a list of possible updaters that can be configured on the system to perform an update.	Enabled	Windows
enduser-notification	It displays a customized notification message on the system when Application Control prevents an action on the system. This feature is supported only in the McAfee ePO-managed configuration.	Enabled	Windows
execution-control	It defines attribute-based rules using one or more attributes of a process to allow, block, or monitor the process.	Enabled	Windows
integrity	This feature: • Protects Application Control files and registry keys from unauthorized tampering. • Allows the product code to run even when the components are not present in the whitelist. • Ensures that all product components are protected. • Prevents accidental or malicious removal of components from the whitelist to ensure that the product doesn't become unusable. • Is disabled in update mode to facilitate product upgrades.	Enabled	Windows and Linux
mp	It protects running processes from hijacking attempts. Unauthorized code injected into a running process is trapped, halted, and logged. It also attempts to gain control of the system through buffer overflow and similar exploits are rendered ineffective.	Enabled	Windows
mp-casp	It renders useless code that is running from the non-code area, which happens due to a buffer overflow being exploited on 32-bit Windows platforms.	Enabled	Windows

Feature	Description	Default status	Supported Operating System
mp-vasr mp-vasr-forced-relocation	It forces relocation of those dynamic-link libraries (DLLs) that have opted out of the Windows native ASLR feature. Some malware relies on these DLLs always being loaded at the same and known addresses. By relocating such DLLs, these attacks are prevented.	Enabled	Windows
network-tracking	It tracks files over network directories and blocks the execution of scripts over network directories. By default, this feature is enabled and prevents the execution of scripts over network directories. When this feature is disabled, execution of scripts over network directories is allowed. Also, write-protecting or read-protecting components over a network directory is not effective.	Enabled	Windows
pkg-ctrl	It manages installation and uninstallation of MSI-based and non-MSI-based installers.	Enabled	Windows
script-auth	It prevents the execution of supported script files that are not in the whitelist. Only whitelisted script files are allowed to execute on the system. For example, supported script files such as .bat, .cmd, .vbs (on Windows), and script files with #! (hash exclamation point) for supported local file systems (on Linux) are added to the whitelist and are allowed to run.	Enabled	Windows and Linux
throttle	It controls the flow of data (events, policy discovery requests, and inventory updates) from each system to the McAfee ePO server. **Note:** This feature is available only in a McAfee ePO managed environment.	Enabled	Windows

Enable or disable features

You can change the default status of a feature by enabling or disabling features. After disabling a feature, the system is no longer protected by that feature.

Caution

Contact Technical Support before enabling or disabling a feature. It can affect the core functionality of the product and make your system vulnerable to security threats.

Task

Run these commands to enable and disable features.

Task	Command
Enable a feature.	`sadmin features enable <featurename>`
Disable a feature.	`sadmin features disable <featurename>`

Package Control feature

You can manage the installation and uninstallation of software packages using the Package Control feature.

This feature allows or denies installation, uninstallation, and upgrade or repair actions for software packages. It prevents any unauthorized installation and uninstallation.

Package Control feature supports these types of installers.

- MSI installers — Include multiple variants such as .msp, .mst, and .msm.
- EXE-based installers — Include MSI files embedded with the installer.
- Non-MSI-based installers — Don't include an MSI file embedded with the installer.

This feature is identified as *pkg-ctrl* in the features list. By default, this feature is enabled and allows installation of software packages by adding rules, such as updater and trusted user. When this feature is disabled, software installation and uninstallation are blocked.

Package Control includes these subfeatures.

Subfeature	Description
Allow Uninstallation	Controls uninstallation of software packages. When this feature is enabled, software uninstallation is allowed. By default, this feature is enabled and identified as *pkg-ctrl-allow-uninstall* in the features list.

Subfeature	Description
Bypass Package Control	Controls bypassing from the Package Control feature. When this feature is enabled, Package Control feature is bypassed and software installation and uninstallation is allowed. By default, this feature is disabled and identified as *pkg-ctrl-bypass* in the features list.

Configure Package Control

You can configure Package Control to control the installation and uninstallation of software packages on a system.

Task

Use these commands to configure Package Control.

Action	Command	Description
Disable the feature.	`sadmin features disable pkg-ctrl`	When you disable Package Control, all its subfeatures are also disabled.
Enable the feature.	`sadmin features enable pkg-ctrl`	When you enable Package Control, all its subfeatures revert to their default state. But, if you enable the Bypass Package Control subfeature, disable Package Control and re-enable Package Control, the Bypass Package Control subfeature is enabled.

Configure these Package Control subfeatures.

Feature	Default state	Feature configuration	
Allow Uninstallation	Enabled	Disable the feature. Prevent uninstallation of software packages on the system.	`sadmin features disable pkg-ctrl-allow-uninstall`
		Enable the feature.	`sadmin features enable pkg-ctrl-allow-uninstall`

Feature	Default state	Feature configuration	
Bypass Package Control	Disabled	Enable the feature. The Package Control feature is bypassed and you cannot control the installation and uninstallation of software packages.	`sadmin features enable pkg-ctrl-bypass`
		Disable the feature.	`sadmin features disable pkg-ctrl-bypass`

Making emergency changes

Run Application Control in Update mode to perform emergency changes on a protected system.

Use Update mode to make changes that can't be made when Application Control is running in Enabled mode. When possible, use these other methods to allow changes:

- Trusted users
- Trusted directories
- Trusted certificates
- Checksum (SHA-1 or SHA-256)values
- Updaters

In Enabled mode, if you install new software or add new files, the files aren't added to the whitelist or allowed to execute unless you use a trusted method to add them. But, if you install or uninstall software, or add new files in Update mode, changes are tracked and added to the whitelist.

To approve changes to the system, a change window is defined, where users and programs can make changes to the system. Update mode allows you to perform these tasks:

- Schedule software and patch installations.
- Remove or change software.
- Dynamically update the whitelist.

Memory-protection techniques are enabled in Update mode, so that running programs can't be exploited.

From Update mode, you can switch to Enabled or Disabled mode.

Switch to Update mode

Switch Application Control to Update mode to perform scheduled or emergency changes in a system. If the product is in Enabled or Disabled mode, perform these steps to switch to Update mode.

Task

1. Run this command at the command prompt.
   `sadmin bu [workflow-id [comment]]`

   Optionally, specify these arguments with the command.

Attribute	Description
`workflow-id`	Specify a workflow ID for the current Update mode session. This is an identification ID that can be used for a Change Management or Ticketing System. If you don't provide the workflow ID, the workflow ID is set to an automatically generated string, *AUTO_n*, where `n` is a number that is incremented each time an update window is opened.
`comment`	Specify a comment that describes the current Update mode session. This information can be used for a Change Management or Ticketing System.

2. If Application Control is in Disabled mode, restart the system.

   Note

   When using Solidcore client version 6.1.0 or later, restarting the system is not needed to enable the software.

   When you restart the system, the product is switched to Update mode.

Exit Update mode

Exit Update mode after making scheduled or emergency changes, patch installations, or software updates in your system.

Task

Run this command at the command prompt.

`sadmin end-update`

Enable or disable password protection

You can restrict users from running critical `sadmin` commands by enabling password protection. When password protection is enabled, Application Control allows these critical commands to run only when the user enters the correct password.

Passwords are encrypted with the SHA-2 hashing algorithm. To protect password details, a random number is added to the password before the hash is computed. The SHA5012 encryption algorithm, a subset of SHA-2, generates a hash of 512 bits, which protects the password from rainbow table attacks.

If you don't need password protection, remove the password, which allows users to run all `sadmin` commands.

Task

1. Type the `sadmin passwd` command to set a password.
   When you set a password, users can no longer run critical commands without providing the correct password. Only a limited set of non-critical commands can run without the password.

   You can use the `-z` switch to prevent the system from prompting for the password. It can be used in all CLI commands. For example, `sadmin solidify -z <password>` is used for unmanaged CLI operations, and is different from the password for the McAfee ePO administrator used for CLI lockdown.

   - If you already set the password, Application Control prompts you to enter your password. Type the old password and press **Enter**. You are now asked to set the new password and retype it.
   - If you didn't set the password earlier, Application Control prompts you to enter a new password. Set the new password and retype it.
2. Type the `sadmin passwd -d` command to remove password protection.
   This allows users to run all `sadmin` commands without requesting a password.
3. Press **Enter**.

Review changes using events

Configure event sinks

Events are stored at locations called *event sinks*. You can add, view, or remove an event.

You can log events in many types of event sinks, including:

- Operating system log (oslog)
- System controller (sc)

Note

When *sc event sink* is enabled, it sends the events to McAfee ePO.

- Debug output (debuglog)

- Pop-up (Windows only)

You can review the event sinks details and add or remove events as needed.

Task	Command	Description
Add an event	`sadmin event sink -a <event_name> <sink_name>`	Add an event by specifying both the event name and the event sink where you want to log the event. The specified event is added to the event sink.
View the event sink details	`sadmin event sink`	View the event sink details for all events generated in the system. You can view the associated event sinks for each event. Event sink details configured in the system for all events are listed.
Remove an event	`sadmin event sink -r <event_name> <sink_name>`	Remove an event by specifying both the event name and the event sink from where you want to remove the event. Removing an event from an event sink allows you to stop logging the event to that event sink.

Set the event cache size

Set the event cache size to define the buffer limit for the event cache.

Task

Run this command at the command prompt.

`sadmin config set EventCacheSize=<value>`

Include a value for the *EventCacheSize* parameter. This value determines the event cache size.

Define the limits for the event cache

You can set the upper and lower limits for the event cache. When the limits are set, an alert is generated to notify that the cache is about to overflow or has recovered from overflow.

Command	Description
`sadmin config set EventCacheWMHigh=<value>`	This command sets an upper limit.

Command	Description
	Include a value for the *EventCacheWMHigh* parameter. The specified value for this parameter should be between 50% to 100% of the event cache size.
`sadmin config set EventCacheWMLow=<value>`	This command sets a lower limit. Include a value for the *EventCacheWMLow* parameter. The specified value for this parameter should be above 20% of the event cache size. The value of the low watermark level must always be less than the value of the high watermark level.

View events

You can view events specific to Application Control to track changes related to the product.

Task

1. Open the **Event Viewer** application:
   - Windows Server 2008 — Select **Start** → **Run** and type `eventvwr`.
   - Windows 7 — Select **Start** → **Search** and type `eventvwr`.
   - Windows 8, 8.1, Server 2012, and Windows 10 — Press [**Windows**] + [**R**] on the keyboard, then type `eventvwr`.
2. Press **Enter**.
3. Perform these steps based on your platform:
   - Windows Server 2008 — From the navigation pane, select **Application** and under the **Source** column, double-click **McAfee Solidifier** event to view its description.

     All application events categorized by type, date, time, source, category, event, user, and computer columns are displayed. Events are listed by order of occurrence, with most recent first.

   - Windows 7 and later — From the navigation pane, expand **Window Logs** and select **Application**. Under the **Source** column, look for the **McAfee Solidifier** events.

     Double-click an event to view its description.

Configuring log files

Application Control generates log messages for all actions and errors related to the product. These log messages are stored in log files that are used for troubleshooting errors.

Log file	Operating system	Path	Description
solidcore.log	Windows Server 2008	<system drive>\Documents and Settings\All users\Application Data\McAfee\Solidcore\Logs	After the product is deployed on a system, a log file named solidcore.log is created in the Logs foder. This file is also known as debuglog. You can configure the solidcore.log file size and number of solidcore.log files that you want to create on the system. **Note:** Configuring log files is applicable only to the solidcore.log file. You can't change the configuration of any other log file.
s3diag.log	Windows Server 2008	<system drive>\Documents and Settings\All users\Application Data\McAfee\Solidcore\Logs	s3diag.log file stores logs for all operations performed on the supported files.
Solidcore_Installer.log and solidcore_setup.log	Windows (all supported versions)	<system drive>\Windows	Application Control installation logs are stored in this file.

Switch to Disabled mode

Switch to Disabled mode to deactivate the features of the software.

Task

1. Type the `sadmin disable` command.
2. Press **Enter**.
3. Restart the system.

Configure Case sensitivity on standalone Solidcore Client

Follow these steps to configure case sensitivity support on standalone Solidcore Client.

Task

1. Follow these steps to enable case sensitivity support on standalone Solidcore Client.
    a. Recover CLI.
    b. Disable **Solidcore** and reboot the system if **Solidcore** is in enable mode.
    c. Once the system is up and running, go to Solidcore CLI and use the command sadmin config set:
    `InventoryCaseSensitivityEnabled=1`
    d. Clean inventory using command:
    `sadmin clean C:\`
    e. Resolidify the system and enable **Solidcore**.
2. Follow these steps to disable case sensitivity support on standalone Solidcore Client.
    a. Recover CLI.
    b. Disable **Solidcore** and reboot the system if **Solidcore** is in enable mode.
    c. Once the system is up and running, go to Solidcore CLI and use the command sadmin config set:
    `InventoryCaseSensitivityEnabled=0` for Windows 10 and `InventoryCaseSensitivityEnabled=2` for Windows 11.
    d. Clean inventory using command:
    `sadmin clean C:\`
    e. Resolidify the system and enable **Solidcore**.

Fine-tuning your configuration

Configure a syslog server

You can access more servers by registering them with your McAfee ePO server. Registered servers allow you to integrate your software with other external servers.

Add the syslog server as a registered server and send information (responses or Solidcore events) to the syslog server.

Task

1. Add the syslog server as a registered server.
    a. On the McAfee ePO console, select **Menu** → **Configuration** → **Registered Servers**, then click **New Server** to open the **Registered Server Builder** wizard.
    b. Select **Solidcore Syslog Server** from the **Server type** list.
    c. Specify the server name, add any notes, then click **Next**.
    d. (Optional) Change the syslog server port.
    e. Enter the server address.
    You can choose to specify the DNS name, IPV4 address, or IPv6 address.
    f. Select the type of logs the server is configured to receive by selecting a value from the **Syslog Facility** list.
    g. Click **Test Syslog send** to verify the connection to the server.
    h. Click **Save**.

    You can choose to send specific responses to the syslog server (complete step 2) or use the seeded response to send all Solidcore events to the syslog server (complete step 3).
2. Send responses to the syslog server.
    a. Select **Menu** → **Automation** → **Automatic Responses**.
    b. Click **Actions** → **New Response**.
    c. Enter the alert name.
    d. Select the **ePO Notification Events** group and **Threat** event type.
    e. Select **Enabled**, then click **Next** to open the **Filter** page.
    f. Define the relevant filters, then click **Next** to open the **Aggregation** page.
    g. Specify aggregation details, then click **Next** to open the **Actions** page.
    h. Select the **Send Event To Solidcore Syslog** action.
    i. Specify the severity and message.
    You can use the listed variables to create the message string.
    j. Select the appropriate syslog servers (one or more), then click **Next**.
    k. Review the response details, then click **Save**.
3. Send all Solidcore events to the syslog server.
    Application Control and Change Control include a seeded response that you can configure to automatically send all Solidcore events to the syslog server.
    a. Select **Menu** | **Automation** | **Automatic Responses**.

b. Edit the **Send Solidcore events to Syslog Server** response to configure these options.

- Set the status to **Enabled**.
- Verify that the appropriate syslog server is selected.
- Review the message string.

The message string is based on the Common Exchange format. Contact McAfee Support for assistance in understanding the message string.

c. Save the response.

Using the command-line interface

List of Commands for Application Control and Change Control

When using Application Control and Change Control in a standalone configuration, you can use different commands and arguments to manage the software and its features.

attr

This command changes or lists the software configuration attributes.

Command syntax conventions

- `sadmin attr add -a|-c|-h|-j|-l|-m|-p|-u filename`
- `sadmin attr add -o parent= filename2 -i filename1`
- `sadmin attr add -v filename` (Windows 7 and later)
- `sadmin attr remove -a|-c|-h|-i|-j|-l|-m|-p|-u filename`
- `sadmin attr remove -v filename` (Windows 7 and later)
- `sadmin attr list -a|-c|-h|-i|-j|-l|-m|-p|-u filename`
- `sadmin attr list -v filename`
- `sadmin attr flush -a|-c|-h|-i|-j|-l|-m|-p|-u filename`
- `sadmin attr add -n filename` (Windows 64-bit)
- `sadmin attr remove -n filename` (Windows 64-bit)
- `sadmin attr list -n filename` (Windows 64-bit)
- `sadmin attr flush -n filename` (Windows 64-bit)

auth

This command authorizes an application (whitelist), or unauthorizes it (blacklist). The application (executable or script) can be installed or invoked from a local drive or a network folder.

Command syntax conventions

- `sadmin auth -a [ -t rule id ] [ -u ] -c checksum`
- `sadmin auth -b -c checksum`
- `sadmin auth -b [ -t rule id] -c checksum`
- `sadmin auth -f`
- `sadmin auth -l`
- `sadmin auth -r checksum`

begin-update (bu)

This command initiates Update mode to help perform software updates and installations.

Command syntax conventions

- `sadmin begin-update [workflow-id [ comment]]`

cert

This command manages certificates for digitally signed files. You can add, remove, or list the certificates in the Application Control certificate store, which is a directory in the install directory <instlall_dir>/Certificates

Command syntax conventions

- `sadmin cert add certificate_name`
- `sadmin cert add -u certificate_name`
- `sadmin cert add -c certificate_content`
- `sadmin cert remove SHA-1`
- `sadmin cert remove SHA-256`
- `sadmin cert remove -c certificate_content`
- `sadmin cert list [-d|-u]`
- `sadmin cert flush`

check

This command validates and fixes the attributes of the specified file against the inventory.

Command syntax conventions

- `sadmin check [-r] file name|directory name|volume name`

config

This command exports current configuration settings to a file or imports configuration settings from a file to an existing installation.

Command syntax conventions

- `sadmin config export file`
- `sadmin config import [-a] file`
- `sadmin config set name=value`
- `sadmin config show`

diag

This command runs diagnostics and offers suggestions on programs and applications to authorize (to perform updates).

Command syntax conventions

- `sadmin diag`
- `sadmin diag fix [ -f ]`

disable

This command activates Disabled mode. Restart the system to make sure that the command is applied.

Command syntax conventions

- `sadmin disable`

enable

This command activates Enabled mode. Restart the system to make sure that the command is applied.

Command syntax conventions

- `sadmin enable`

end-update (eu)

This command ends Update mode and activates Enabled mode.

Command syntax conventions

- `sadmin end-update`

event

This command configures the log targets (sinks) for generated events.

Command syntax conventions

- `sadmin event sink [eventname sinkname]`
- `sadmin event sink -a|-r { eventname | ALL } { sinkname | ALL }`

features

This command enables, disables, or lists the features on an existing installation.

Command syntax conventions

- `sadmin features [enable|disable|list] [feature name]`

help

This command provides information about basic commands.

Command syntax conventions

- `sadmin help [command]`

help-advanced

This command provides information about advanced commands.

Command syntax conventions

- `sadmin help-advanced [command]`

license

This command adds or displays licensing information.

Command syntax conventions

- `sadmin license add <license key>`
- `sadmin license list`

list-solidified (ls)

This command lists the whitelisted files, directories, and volumes.

Command syntax conventions

- `sadmin list-solidified [-l] [file name|directory name|volume name]`

list-unsolidified (lu)

This command lists the files, directories, and volumes that are not whitelisted.

Command syntax conventions

- `sadmin list-unsolidified [file name|directory name|volume name]`

lockdown

This command disables the local command line interface. After lockdown, you can only issue the help, help-advanced, status, version, and recover commands.

Command syntax conventions

- `sadmin lockdown`

monitor (mon)

With this command, you can monitor changes to files, user activity and process execution or termination.

Command syntax conventions

- `sadmin monitor file [ -e |-i | -r ] file name|directory name|volume name`

passwd

This command sets a password for the command line interface. If the password is set, you must verify the password before executing critical commands. Using `sadmin passwd -d` command removes the password.

Command syntax conventions

- `sadmin passwd [-d]`

read-protect (rp)

This command displays or changes the read protection rules. You must specify complete file or directory names with this command.

Command syntax conventions

- `read-protect/rp [-e | -i | -r ] path`

recover

This command recovers the local command line interface from locked down state.

Command syntax conventions

- `sadmin recover [-f]`

ruleengine

This command specifies rules on various attributes of a process whose execution is undetermined. This enables the user to allow, block, or monitor its execution. You can combine one or more unique attribute types in one rule using `AND` operator.

Command syntax conventions

- `sadmin ruleengine add allow processname command_line { matches | not matches } regex`
- `sadmin ruleengine add allow processname { command_line | user | parent_process_name | path } { equals | not equals } string`
- `sadmin ruleengine add block processname command_line { matches | not matches } regex`
- `sadmin ruleengine add block processname { command_line | user | parent_process_name | path } { equals | not equals } string`
- `sadmin ruleengine add monitor processname command_line { matches | not matches } regex`
- `sadmin ruleengine add monitor processname { command_line | user | parent_process_name | path } { equals | not equals } string`
- `sadmin ruleengine remove allow processname command_line { matches | not matches } regex`
- `sadmin ruleengine remove allow processname { command_line | user | parent_process_name | path } { equals | not equals } string`
- `sadmin ruleengine remove block processname command_line { matches | not matches } regex`
- `sadmin ruleengine remove block processname { command_line | user | parent_process_name | path } { equals | not equals } string`
- `sadmin ruleengine remove monitor processname command_line { matches | not matches } regex`
- `sadmin ruleengine remove monitor processname { command_line | user | parent_process_name | path } { equals | not equals } string`
- `sadmin ruleengine list`
- `sadmin ruleengine flush`

skiplist

This command bypasses a path component from a feature to remove the protection applied by that feature. You can also define skip rules to skip path components from the whitelist. Use caution and take advice from McAfee Support before applying skiplist rules because doing so can affect the core functionality of the product and can make your system vulnerable to security threats.

Command syntax conventions

- `sadmin skiplist add -c|-d|-f|-i|-r|-s|-v pathname`
- `sadmin skiplist remove -c|-d|-f|-i|-r|-s|-v pathname`
- `sadmin skiplist list -c|-d|-f|-i|-r|-s|-v`
- `sadmin skiplist flush -c|-d|-f|-i|-r|-s|-v`

solidify (so)

This command adds specified files in a directory or system volume to the whitelist.

Command syntax conventions

- `sadmin solidify [-q|-v] [file|directory|volume]`

status

This command displays the status of the software. You can view the operational mode, operational mode on system restart, connectivity with McAfee ePO, access status, and whitelist status of the local CLI.

Command syntax conventions

- `sadmin status`

trusted

This command identifies a local or remote share as a trusted file path, volume, or directory. You can include, exclude, remove, list, or flush the trusted volumes or directories.

Command syntax conventions

- `sadmin trusted -e|-i|-r|-f|-l [path name|volume name]`

unsolidify (unso)

This command removes specified files from the whitelist.

Command syntax conventions

- `sadmin unsolidify [ -v ] [file name|directory name|volume name]`

updaters

This command adds, deletes, lists, or flushes programs from the list of authorized updaters.

Command syntax conventions

- `sadmin updaters add [-d|-n] binaryname`
- `sadmin updaters add [-p parent-binaryname] binaryname`
- `sadmin updaters add [-t rule-id] binaryname`
- `sadmin updaters add [-d] [-n] [-t rule-id] [-p parent-binaryname] binaryname`
- `sadmin updaters add [-l libraryname] binaryname`
- `sadmin updaters remove [-p parent-binaryname] binaryname`
- `sadmin updaters remove [-l libraryname] binaryname`
- `sadmin updaters remove -u username`
- `sadmin updaters list`
- `sadmin updaters flush`

version

This command displays the version of the software that you have installed in your system.

Command syntax conventions

- `sadmin version`

write-protect (wp)

This command write-protects specified files including the whitelisted files. You must specify complete file or directory names with this command.

Command syntax conventions

- `sadmin write-protect -e|-i|-r pathname`
- `sadmin write-protect -f|-l`

write-protect-reg (wpr)

This command write-protects specified registry keys including the whitelisted registry keys.

Command syntax conventions

- `sadmin write-protect-reg -e|-i|-r registrykeyname`
- `sadmin write-protect-reg -f|-l`

Command short forms

You can use the commands short forms which are interchangeable.

Command	Short form
`sadmin write-protect`	`sadmin wp`

Command	Short form
`sadmin read-protect`	`sadmin rp`
`sadmin solidify`	`sadmin so`
`sadmin unsolidify`	`sadmin unso`
`sadmin list-solidified`	`sadmin ls`
`sadmin list-unsolidified`	`sadmin lu`
`sadmin begin-update`	`sadmin bu`
`sadmin end-update`	`sadmin eu`
`sadmin monitor`	`sadmin mon`

Argument details

This table lists the commands with the supported arguments and their description. In the **Argument** column, the supported arguments for the commands are listed in alphabetical order.

Argument details

Command	Argument	Description
`attr`	`-a`	Always authorizes by file name. This is a deprecated technique. For more information, contact McAfee Support.
	`-b`	Configures bypass, restore, list, and flush rules for a component protected using the Mangling technique. This is a deprecated technique. For more information, contact McAfee Support.
	`-c`	Configures bypass, restore, list, and flush rules for a component protected using the Critical Address Space Protection technique.

Command	Argument	Description
	`-f`	Bypasses from full crawl attribute. This is a deprecated technique. For more information, contact McAfee Support.
	`-h`	Adds a binary to MP Compat protection.
	`-i`	Configures bypass, restore, list, and flush rules for a binary using the Package Control feature.
	`-j`	Bypasses a binary from MP Compat protection.
	`-l`	Configures bypass, restore, list, and flush rules for a component using the Anti-Debugging technique. This is a deprecated technique. For more information, contact McAfee Support.
	`-m`	Configures the add, remove, list, and flush rules for blocking the process in the interactive mode.
	`-n`	Configures the bypass, restore, list, and flush rules for a component using the mp-nx technique.
	`-y`	Includes child processes for a component to be bypassed using the mp-nx technique. This argument can only be specified with the `-n` argument.
	`-o`	Indicates to specify the DLL module name for a specified process. This argument can be used with `-p`, `-v`, and `-i` arguments. On the Linux platform, use this argument to specify the parent program for the `-p` attribute.
	`-p`	Bypasses from process context file operations attribute.
	`-u`	Always unauthorizes by file name. This is a deprecated technique. For more information, contact McAfee Support.
	`-v`	Bypasses from Forced DLL relocation attribute.
`auth`	`-a`	Authorizes a binary using the checksum value.

Command	Argument	Description
	`-b`	Bans a binary using the checksum value.
	`-c`	Specifies the checksum value.
	`-f`	Flushes all authorized or banned binaries.
	`-l`	Lists all authorized and banned binaries.
	`-r`	Removes the authorized or banned binaries.
	`-t`	Includes the associated tag name for a binary to be banned.
	`-u`	Authorizes a binary and also provides updater rights when used with the `-a` and `-c` arguments.
`begin-update (bu)`	`workflow-id`	Indicates to specify an ID while switching to the Update mode. This ID can be used for tracking purposes in a change management for ticketing system.
	`comment`	Indicates to use a descriptive text for the workflow ID.
`cert`	`-c`	Specifies the certificate content as trusted.
	`-d`	Lists all details of the issuer and subject of the certificates added to the system.
	`-u`	Provides updater rights to a certificate that is added as a trusted certificate or list the trusted certificates with updater rights.
`check`	`-r`	Fixes any inconsistencies that are encountered.
`config`	`-a`	Appends the configuration values.
`diag`	`-f`	Applies the diagnosed configuration changes for the restricted programs, such as winlogon.exe and svchost.exe.

Command	Argument	Description
`disable`	NA	NA
`enable`	NA	NA
`end-update (eu)`	NA	NA
`event`	`-a`	Adds sinks to the specified event.
	`-r`	Removes sinks from the specified event.
`features`	`-d`	Lists all features (including the hidden features). For more information, contact McAfee Support.
`help`	NA	NA
`help-advanced`	NA	NA
`license`	NA	NA
`list-solidified (ls)`	`-l`	Lists details of the whitelisted files.
`list-unsolidified (lu)`	NA	NA
`lockdown`	NA	NA
`monitor (mon)`	`-a`	Includes the specified pattern to match file names for content change tracking. The pattern can contain the `'*'` character, as the first or last character. For example, `*.txt` and `hello.*`. This argument is useful on McAfee ePO-managed configuration. The content change tracking for files can be viewed only at McAfee ePO.

Command	Argument	Description
	`-b`	Excludes the specified pattern to match file names for content change tracking. The pattern can contain the `'*'` character, as the first or last character. For example, `*.txt` and `hello.*`. This argument is useful on McAfee ePO-managed configuration. The content change tracking for files can be viewed only at McAfee ePO.
	`-c`	Includes the directory non-recursively for content change tracking. This argument is useful on McAfee ePO-managed configuration. The content change tracking for files can be viewed only at McAfee ePO.
	`-d`	Includes the file for content change tracking. This argument can be specified with the `-i` argument or alone. The `-d` argument is useful on McAfee ePO-managed configuration. The content change tracking for files can be viewed only at McAfee ePO.
	`-e`	Excludes the specified component for monitoring changes.
	`-f`	Flushes all monitoring or content change tracking rules.
	`-i`	Includes the specified component for monitoring changes.
	`-n`	(Optional) Specifies the file encoding. The supported encoding types are Auto-Detect, UTF-8, UTF-16, and ASCII, If the `-n` option is not used, the encoding used is Auto-Detect. The `-n` argument can only be specified with `-d` argument.
	`-r`	Removes all monitoring rules.
`passwd`	`-d`	Removes the password for using Application Control.
`read-protect (rp)`	`-e`	Excludes specific components from a read-protected directory, or volume.
	`-f`	Flushes all components from read protection.
	`-i`	Includes files, directories, or volumes for read protection.

Command	Argument	Description
	`-l`	Lists the read-protected components.
	`-r`	Removes read protection applied to files, directories, or volumes.
`recover`	`-f`	Forcefully closes the McAfee ePO command and recover the local CLI.
`ruleengine`	`allow`	A rule type for adding or removing the allow rules on any attribute of a process.
	`block`	A rule type for adding or removing the block rules on any attribute of a process.
	`monitor`	A rule type for adding or removing the monitor rules on any attribute of a process.
	`command_line`	This attribute type specifies the command-line argument to execute a process. A rule type can be applied to either allow, block, or monitor a process when executed using command_line.
	`user`	This attribute type specifies the user who tries to execute a process. A rule can be applied to either allow, block, or monitor the process started by a user.
	`parent_process_name`	This attribute type specifies a particular process which a parent process tries to execute. A rule can be applied to either allow, block, or monitor its execution when a parent process tries to execute it.
	`path`	This attribute type denotes the path where the process resides whose execution is undetermined. A rule can be applied to allow, block, or monitor the process execution from that path.
	`regex`	A regular expression of one or more characters that defines the search pattern. It describes a grammar that can be constructed based on ECMA script. See this article for more details.
	`string`	Specifies a string of characters.

Command	Argument	Description
`skiplist`	`-c`	Skips path components from the monitoring feature. This command is applicable to Application Control only in Update mode where changes are tracked. User mode paths and paths with volume name do not work with this command. Text added with this command is treated as complete component. For example, text can start with a slash (/) and end with a slash (\), dot (.), or null character. No events are generated for files that contain the specified text. Also, the whitelist is not updated for such paths.
	`-d`	Skips path components from write protection to remove write protection applied to all files in that path. User mode paths and paths with volume name do not work with this command. Text added with this command is treated as complete component. For example, text can start with a forward slash (/) and end with a backward slash (\), dot (.), or null character.
	`-f`	Skips path components from file operations and the script-auth feature. User mode paths and paths with volume name do not work with this command. Text added with this command is treated as substring in a path. No events are raised and the whitelist is not updated for the skipped path components. Also, script execution control does not work for paths added with this command.
	`-i`	Skips path components from file operations using the ignore path list. This works similar to the `sadmin add -f` command. User mode paths and paths with volume name do not work with this command. When the path components are specified on Windows 64-bit platforms, even the deny-exec feature is skipped.
	`-r`	Skips registry path components from write protection for registry to remove write protection applied on the registry paths.

Command	Argument	Description
		Text added with this command is treated as complete component. For example, text can start with a forward slash (/) and end with a backward slash (\), dot (.), or null character.
	`-s`	Removes files present under the specified path component and subdirectories from the whitelist. Network path names cannot be specified with this command. Volume relative rules can also be specified using *\<vol_rel_name>.
	`-v`	Bypasses volumes from attaching to Application Control. File system, such as NTFS or FAT, can also be specified with this argument. When you specify a volume name with this argument, Application Control is not attached to that volume. Script-auth and deny-exec features are also not effective on the specified volume. Components in that volume are allowed to execute on the system. You can specify a path component using user mode volume names, such as C: and D:. Also, device names, such as \device\harddiskvolume1, and file systems, such as NTFS and FAT, can also be specified.
`solidify (so)`	`-q`	Suppresses all output except for errors.
	`-v`	Displays all processed components.
`status`	NA	NA
`trusted`	`-e`	Excludes one or more specified paths to the directories or volumes from a list of trusted directories or volumes.
	`-f`	Removes all directories and volumes from the trusted rule.
	`-i`	Adds one or more specified paths to the directories or volumes as trusted directories or volumes.
	`-l`	Lists all trusted directories and volumes.
	`-r`	Removes the specified directories or volumes from the trusted rule.

Command	Argument	Description
	`-u`	Provides updater rights to all binaries and scripts in the trusted directories or volumes.
`unsolidify (unso)`	`-v`	Displays all processed components.
`updaters`	`-d`	Excludes the child processes of a binary file to be added as an updater from inheriting the updater rights.
	`-l`	Includes the library name for an execution file to be added as an updater (for Windows).
	`-n`	Disables event logging for a file to be added as an updater.
	`-p`	Adds a file as an updater only when it is started by specified parent process.
	`-t`	Performs these operations: • Includes the tags for a file to be added as an updater. • Adds a user with a tag name as an updater.
	`-u`	Adds a user as an updater (for Windows).
`version`	NA	NA
`write-protect (wp)`	`-e`	Excludes specific components from a write-protected directory or volume.
	`-f`	Flushes all components from write protection.
	`-i`	Write-protects files, directories, or volumes.
	`-l`	Lists the write-protected components.
	`-r`	Removes write protection applied to files, directories, or volumes.
`write-protect-reg (wpr)`	`-e`	Excludes one or more registry keys from write protection.

Command	Argument	Description
	`-f`	Flushes all registry keys from write protection. Flushing the registry keys from write protection removes all write protection rules applied to the registry keys.
	`-i`	Write-protects registry keys.
	`-l`	Lists all write-protected registry keys.
	`-r`	Removes write protection from one or more registry keys.

Troubleshooting

Troubleshooting and logs

Use logs to troubleshoot and resolve issues of McAfee Application and Change Control.

Log file locations

Log files and its location details are shared below:

- **Installation logs** — Solidcore_Installer.log, solidcore_setup.log, mac_mpt.log, and mac_mpt.etl
- **Windows OSes** — %SYSTEMROOT (for example, C:\Windows \)
- **Linux OSes** — Failed install - /tmp/
- **Successful install**:
    - Product logs- Solidcore.log and S3diag.log
    - Vista and above: C:\programdata\mcafee\common framework\
    - Other Windows operating system: C:\documents and settings\all users\application data\mcafee\common framework\
    - Non-Windows: /var/log/mcafee/solidcore

Log file size and count

To increase the log file size (in MB), run this command:

```
sadmin config set LogfileSize=XXXX
```

To increase the number of rotated log files, run this command:

```
sadmin config set LogfileNum=X
```

Common log level changes

At times, increasing log levels in the McAfee Application and Change Control product is needed to troubleshoot an issue. When the module logging levels are increased, reset the logging back to the default levels. For example, if a module and level is set to ENABLE, run the same command with DISABLE to undo the increase in logging.

Available log 'TYPES' — ERROR, WARNING, SYSTEM, INFO, DETAIL, FNENTRY, and FNEXIT

Default levels for all modules — ERROR, WARNING, and SYSTEM

For information about Minimum Data Collection to troubleshoot McAfee Application and Change Control, see KB90755.

Some common log levels and related troubleshooting areas are given below:

Log level	Troubleshooting area
sadmin loglevel enable swin info detail	MACC driver framework
sadmin loglevel enable mahdlr all	McAfee Agent interactions with the MACC product
sadmin loglevel enable sau info detail	Sau (script as updater) module
sadmin loglevel enable usm info	TIE or McAfee® Data Exchange Layer (DXL) responsiveness
sadmin loglevel enable inv info	Inventory module
sadmin loglevel enable pst info	Memory protection module
sadmin loglevel enable ruleengine info	MACC execution control module
sadmin loglevel enable cctl info detail	Binary execution based on McAfee GTI reputation of its certificate
sadmin loglevel enable rbl info detail	Reputation workflows (McAfee GTI and TIE)
sadmin loglevel enable tie info detail	McAfee TIE server
sadmin loglevel enable cert info	Certificate module
sadmin loglevel enable evt info	Events
sadmin loglevel enable fmon info	File monitoring

Troubleshooting Inventory issues

There are several methods to troubleshoot inventory issues in your environment.

For details about Minimum Data Collection to troubleshoot McAfee Application and Change Control, see KB90755.

Perform the steps in this section if you are experiencing issues with Inventory not present:

- Make sure McAfee ePO server services are running.
- Make sure that the client is solidified.

- Verify Inventory Fetch Time (Last and Next).
- If Inventory time is greater than 7 days, rerun the Pull task.
- If Inventory time is less than 7 days, run the Inventory time reset task. To reset Last time inventory sync on client, run the following commands:
    -

```
sadmin config set InvDiffLastAccessTime=default
```

    -

```
sadmin config set PullInvLastAccessTime=default
```

Note

7-day interval is the default value.

Verify whether you have modified the **Pull Complete Inventory Interval** value in the Application Control Options policy. Adjust the timing accordingly. Rerun the Inventory Pull task if it fails.

- Pull inventory manually by running the command `sadmin -rax > FILENAME.xml`.
- Add filename.xml into the ePO event parser directory.
- Verify eventparser.log for errors.
- If rerunning the Inventory pull task, collect the following:
    - FILENAME.XML
    - MER and Gatherinfo from affected client
    - MER with McAfee ePO Server and Orion debug logging

For details about Application Control command to reset throttling of events, policy discovery requests (observations), and inventory updates, see KB84348.

To reset the inventory-diff threshold on the endpoint, run the command `sadmin reset-inv-diff-throttle`. Inventory diff generation resumes on the endpoint after executing this command.

For details about Application Control Pull Inventory client task overview, see KB84247.

For details about Application Control corrupt inventory fallback process, see KB88222.

How to clear inventory time stamp

On McAfee ePO:

- Create SC: Run the following commands
    -

```
config set InvDiffLastAccessTime=default
```

-

```
config set PullInvLastAccessTime=default
```

- Send the task to the client.

On Client:

- Open Command Prompt with administrator's rights.
- Recover the local CLI by executing sadmin recover. A password is needed to unlock the local CLI.
- Run the following commands:
  -

```
sadmin config set InvDiffLastAccessTime=default
```

  -

```
sadmin config set PullInvLastAccessTime=default
```

Best practices for using the software

Best practices for managing applications

Application Control can work with a reputation managing source such as TIE server or McAfee Global Threat Intelligence file reputation service to fetch reputation information of files and certificates.

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

- Manage the unclassified application in your environment to reduce the number of unknown applications. This list typically includes all unknown applications, and can be considered as greylist for your enterprise. The goal is to minimize risk and achieve 95% classification by removing or reclassifying unknown files and applications. Review and process greylist routinely to keep it to a minimum size.
    - Run GetClean on endpoints with a high number of unknown files. The GetClean utility submits files for analysis to McAfee Labs where they are verified 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 Trusted.
- Enable the automatic response **Bad Binary has been detected 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 Binary has been detected 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 Cloud 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 applications. This makes management of desktop systems easier by verifying the corporate applications. Here are high-level steps to follow:
    - Validate and review all applications on a system.
    - Run GetClean on the system to classify all unknown applications on the system.
    - Set the base image on the approved system by using the **Mark Trusted** option.

Adding all binaries from the trusted system to your policy using Attr (auth by name) or Auth (auth by checksum) is not needed. This could cause performance issues on your clients. Solidification of a system with GTI/TIE reputation allows everything known with good reputation to run on your system.

Application Control rules (Windows)

Application Control options have many configurations for each customer that can be customized according to their needs.

The policy for Application Control rules is a multi-socket policy. For information about multi-slot policies, see *McAfee ePO Product Guide*. 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.

Follow these best practices when creating rules:

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 flexible 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.

Updater method	Restriction level	Reason
Certificates	Medium	Allow your signed applications to update a system. 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.
Executable Files	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). **Note:** This method is typically used for execution control and not for making changes to a system.
Installers	High	Allow a non-whitelisted standalone executable 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.

Tips and tricks for client deployments

You can use these tips and tricks for deploying the software successfully.

McAfee Application and Change Control Memory Protection must be disabled through Endpoint Security or McAfee Host Intrusion Prevention. For more information, see KB81465.

Sometimes, applications conflict with how Application Control injects into system process to monitor dlls, memory, and other components. You can change how Application Control injects dll from Nt.dll to kernel32.dll. For more information, see KB91255.

Note

If a ban by name, SHA-1, or SHA-256 rule exists for an executable file, its execution is banned regardless of the file's reputation.

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.

Tips and tricks for server performance

You can enable or disable some options on the server settings for performance enhancements.

For example, if you are not using Global Threat Intelligence or TIE in your environment then you can disable these features for increased performance.

Catalog cert extraction

Microsoft Windows binaries can be catalog signed or have an embedded signature. MACC uses custom code to extract embedded certificates. The certificates can be extracted in kernel space or user-space. Extraction of embedded certificates is the only type of signing supported with MACC until the 7.0.x release.

MACC 7.0.x supports reputation-based execution, this allows, or blocks a file by the reputation of its certificate. Because several files in Microsoft Windows are catalog signed, this feature requires extraction of catalog signatures. MACC uses the APIs provided by Microsoft to extract the catalog certificates for binaries. It extracts the certificate initially and stores them in its inventory and does not connect with the APIs every time a request is made. This saves time and improves system performance. It extracts catalog certificates only when software upgrades, changes in files, or to merge inventories.

If all reputation is disabled, there is no need to extract the catalog certificates during these events.

Run the command to disable the catalog certificate extraction:

```
Sadmin config set CatalogCertExtractionDisabled=1
```

Note

Reboot is not needed.

Avoid volume name extraction

During solidification, volume names are extracted for every file. This is an expensive process. The idea here is to maintain a small cache of volume names.

If two files (for example, A:\a\b\c\d\f1.txt and A:\a\b\c\d\f2.txt) have the same volume name, it can be used to avoid volume name extraction. You must see a significant reduction in solidification time and enable task time with this one.

Run the command to reduce solidification time:

```
Sadmin config set AvoidVolumeNameExtractionWherePossible=1
```

Note

Reboot is not needed.

Embedded cert extraction

This is similar to Catalog cert extraction. The only difference is that it is for Embedded certificates. Caveats are the same, if reputation is enabled, this must not be disabled.

Note

Auth-by-cert and cert-as-updater rules don't depend on certificate extraction in the user-space, and those still work with this configuration.

Run the command to disable the embedded certificate extraction:

```
Sadmin config set EmbeddedCertExtractionDisabled=1
```

Note

Reboot is not needed.

IsInvbackup

This feature is enabled by default and creates a backup copy of the local whitelist. This backup copy is created during the boot sequence, which increases system boot time and cause performance issue. If the whitelist is corrupted, MACC can recover it from a backup copy rather than resolidify the system.

Run the command to create a backup copy of the local whitelist:

```
Sadmin config set IsInvbackupEnabled=0
```

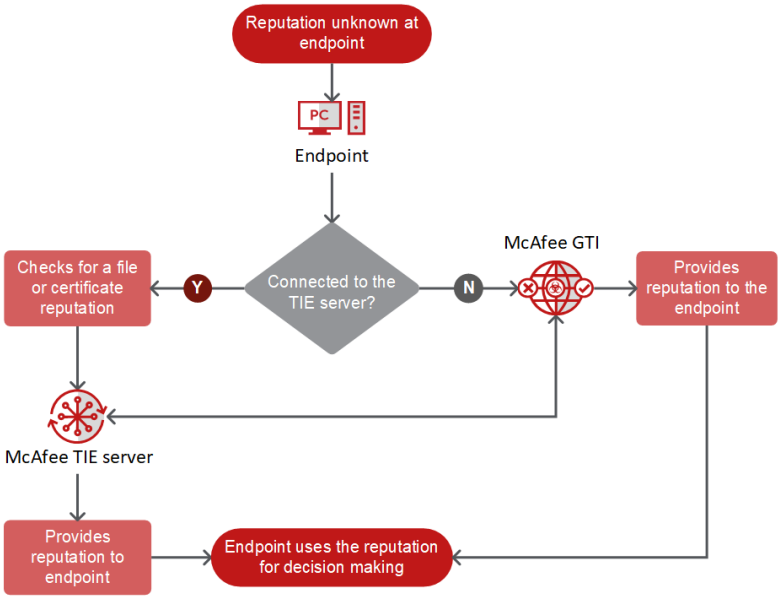
Note

Reboot is not needed.

Reputation-based tracking

If you are using reputation-based tracking, and your clients can't connect directly to the McAfee GTI server then you could have performance issues on your system. For information about how to resolve the issue, see KB86638.

If you use a proxy for clients to connect to the internet, you either need to use TIE for reputation or allow your clients to directly connect to McAfee GTI servers. For more information about McAfee GTI or TIE configuration, see McAfee product documentation of McAfee GTI and TIE.



After you install MACC, you should exclude its processes and folders from being scanned by Endpoint Security or VirusScan Enterprise scanning engine. Scanning MACC processes and folders consumes time and impacts system performance. Make sure you have exclusions in your antivirus software. For more information, see KB88915.

Create an on-access scanner low-risk process exclusion (**Disable scanning when writing to or reading from disk**) for the McAfee Application and Change Control process **Scsrvc.exe**.

Note

The default location for MACC process is **C:\Program Files\McAfee\Solidcore**. Create an exclusion for the MACC folder **<drive>\Solidcore**.

If you use a third-party antivirus or Endpoint Protection software, use the same exclusions in the third-party program.

Example: Windows defender

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths]

- "C:\\Solidcore"=dword:00000000
- "C:\\Program Files\\McAfee\\Solidcore"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes]

- "scsrvc.exe"=dword:00000000
- "swin.sys"=dword:00000000

Policy Discovery request best practices

Follow these suggestions for better management of rules when reviewing Policy Discovery requests.

- Limit the use of "Allow File Globally" action. This adds the rule to the **Global Rule** rule group, which is embedded in the **McAfee Default** Application Control policy. High use of this action can lead to policy bloat and policy enforcement issues, and increased difficulty in managing the Application Control policies. Rules that allow activity within Application Control must be categorized based on vendor/application name, rather than dumped into a single Rule Group bucket for efficient management of rules.
- When creating Rule Groups, a standard naming convention must be used to help organize policies within McAfee ePO. Rule Groups include policies and application vendors such as ACCT_ADOBE or BASELINE_Microsoft.
- Use **Create Custom Policy** to create rules based on Policy Discovery requests. Organize the rules created for separate categories such as company/vendor name, application name, application purpose, and, function rather than putting all rules into a single group. This can help manage the rules.
- Some Policy Discovery requests can't be added through this process, due to the activity being generated from a Generic Launcher Process. An error "Updater rule can’t be made for Generic launcher process" might be displayed when doing so. Manual creation of rules for Generic Launcher Process is not recommended.
- When trying to trust your gold image there is no need to trust the inventory of one system and allow it by adding all binaries to a rule group (auth by checksum, or auth by name). Solidification allows everything on these systems to run already unless specified not to based on your policy (ban rules or reputation). Doing so could cause performance issues due to large policies trying to apply to the system.
- We do not have any constraints on how many objects can be assigned to a rule group or a policy. But, we do not recommend large number of objects in the Auth or ATTR groups. MACC is multi-slotted in **Policy Catalog**. If you have many large rule groups with many objects, McAfee Application and Change Control considers this as 1 group and link the objects. We apply each object to the system 1 by 1 which could take a couple of seconds to apply. If you have large policies, we recommend that you leave the policy enforcement at default settings (60 mins) to allow your policy to complete. It applies only delta changes instead of trying to reapply the whole policy at every enforcement. We have seen this cause a constant cpu constraint of 25% and never released due to policy enforcement never completing.
- Policies are applied to an endpoint using one command at a time. Policies with rules numbering in thousands can cause significant performance issues, especially if duplicate updaters or rules are present.
- If a non-generic process is identified as a parent process for several binaries, you can add the parent process as an updater eliminating the need for the child processes to be added as a binary.
- Using certificates can significantly cut down on the administration overhead and policy size.
- If possible, an in-house certificate authority must be used to sign home grown applications.

Frequently asked questions

Here are answers to frequently asked questions.

What features are enabled with which license?

Licence	Features enabled
Application Control	• Active-x • App-control • App-control-dsr • App-control-installer-detect • Checksum • Deny-exec • Deny-exec-dlls • Deny-exec-drivers • Deny-exec-exes • Deny-exec-ads • Deny-Read (disabled) • Discover-updaters • Enduser-notification • Execution-control • Integrity • Mon (disabled) • MP • MP-Casp • Mp-nx • Mp-vasr • Mp-vasr-forced-relocation • Network tracking • OB-logging • pkg-ctrl • Pkg-ctrl-bypass • Pkg-ctrl-uninstall • TIE-reputation • GTI-reputation • Script-auth • SAU • Self-approval • Throttle-OB

Licence	Features enabled
	• Throttle-INV
Change Control	• Deny-Read • Integrity (disabled) • Mon • Mon-ads • Mon-file • Mon-fattr • Mon-file-diff • Mon-proc-exec • Mon-reg • Mon-uat • Network tracking • Throttle-evt
Application Control and Change Control	• Deny-Write • Popups • Signing • Signing-fic • Throttle

What are these features?

Feature	Description
app-control	Helps you to define applications that are allowed to run on your system (white list applications) and applications that are blocked from running on your system (blacklist applications).
app-control-dsr	Provides additional information about a file such as file type, size, and version.
app-control-installer-detect	Checks whether an application being launched is an installer or not in context of App-control feature. If the application is an installer, it works as an Updater if configured so.
checksum	Calculates and matches the checksum of the file to be executed with the checksum stored in the inventory.

Feature	Description
deny-exec	Prevents execution of any unauthorized EXE files, DLL files, and drivers.
deny-exec-dlls	Prevents execution of any unauthorized DLL files.
deny-exec-drivers	Prevents execution of any unauthorized drivers (for example .sys files).
deny-exec-exes	Prevents execution of any unauthorized EXE files.
deny-exec-ads	Prevents execution of Advanced Data Streams.
deny-read	Read-protects critical components. When this feature is applied on the components, the components can't be read. Read protection is listed as deny-read feature in the features list. Read protection works only when Application Control is running in the Enabled mode.
deny-write	Write-protects the specified components. When this feature is applied on the components, the components are rendered as read-only thereby protecting your valuable data. This feature is supported only when Application Control is operating in the Enabled mode.
discover-updaters	Retrieves a list of potential updaters that can be included in the system.
integrity	Protects the files and registry keys of Application Control from unauthorized tampering. It allows the product code to run even when the components of Application Control are not in the inventory. This makes sure that all components of the product are whitelisted. Accidental or malicious removal of the components from the whitelist is prevented to make sure the product remains usable. This feature is supported on the Windows and Linux platforms. When the product is in Update mode, this feature is disabled to facilitate product upgrades.
mon	Allows you to designate a set of files, processes to be monitored for changes.
mon-file	Monitors file.
mon-fattr	Monitors file attributes.
mon-file-diff	Monitors file differentials.
mon-proc-exec	Monitors process execution.

Feature	Description
mon-reg	Monitors registry changes.
mon-uat	Monitors user-account.
mp	Protects the running processes on a system from malicious/hijacking attempt. This feature is supported only on the Windows platform. Unauthorized code injected into a running process is trapped, halted, and logged. In this manner, attempts to gain control of a system through buffer overflow and similar exploits are rendered ineffective and logged.
mp-casp	Renders useless code that is running from the non-code area. Code running from the non-code area is an abnormal event that usually happens due to a buffer overflow being exploited. This technique is available on the 32-bit Windows platforms.
mp-nx	The NX feature uses Windows' Data Execution Prevention (DEP) feature to protect processes against exploits that try to execute code from writable memory area (stack/heap).
mp-vasr-forced-relocation	Forces relocation of those dynamic-link libraries that have opted out of Windows native ASLR feature. Some malware relies on these DLLs to get loaded at the same and known address. By relocating such DLLs, these attacks are prevented.
network-tracking	Tracks files over network directories and blocks the execution of scripts on network directories. By default, this feature is enabled. Also, write-protecting or read-protecting the components on a network directory are effective when this feature is disabled.
ob-logging	Controls if observations are reported.
pkg-ctrl	Manages the installation and removal of all MSI-based installers on a protected Windows endpoint.
pkg-ctrl-bypass	Controls bypassing from the package control feature. When this feature is enabled, pkg-ctrl feature is bypassed and every software installation and removal is allowed.
pkg-ctrl-allow-uninstall	Controls the removal of software packages. When this feature is enabled, all software removal is allowed.
popups	Allows the user to get the solidifier events in a pop-up with logs and event viewer.
TIE-reputation	Reputation checking with McAfee Threat Intelligence Exchange.

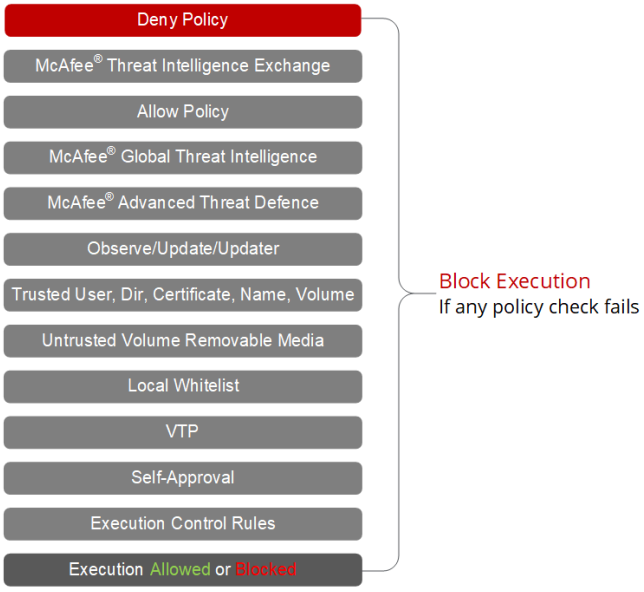
Feature	Description
McAfee GTI-reputation	Reputation checking with McAfee Global Threat Intelligence.
script-auth	Prevents the execution of supported script files, which are not present in the whitelist. Only the whitelisted script files are allowed to execute on an endpoint. For example, supported script files such as .BAT, .CMD, .VBS (for Windows) and containing #! (hash bang) for supported local file systems (for Linux) are added to the whitelist to be allowed to execute on an endpoint.
self-approval	Application Control prevents any new or unknown applications from running on protected endpoints. When the self-approval feature is enabled and users try to run an unknown or new application on a protected endpoint, they are prompted to approve or deny the application execution.
script as updater	Provides updater rights to supported script files such as .BAT, .CMD, .VBS (for Windows).
signing	Allows user to control execution of a binary based on trusted publisher certificates.
signing-fic	Controls execution of binary based on both checksum and trusted publisher certificates.
throttle	Controls Throttling policy. If this is not set, neither the events are sent to throttle cache, nor any pull from throttle cache or any type of throttle tracking happens. The installer enables this feature by default in version 6.2.0. This is a common feature for all types of throttling (events/invdiff/observations). Enabling or disabling this feature applies to all 3 types of throttling.
throttle-evt	Controls throttling of events.
throttle-ob	Controls throttling of observations.

Where do I get MACC training videos?

For MACC training videos, see McAfee Support YouTube channel.

What is the execution decision flow of Application Control?

For more information about execution decision flow of Application Control, see KB85695.



Which one takes precedence in monitoring (file, user, or folder)?

The order of precedence is considered as listed:

1. User name-based filter
2. Process name-based filter
3. File extension-based filter
4. File name-based filter
5. Folder/directory-based filters

   For example, on Windows, if folder C:\Folder1\Folder2 is included but folder C:\Folder1 is excluded, any change operations performed on a file in folder C:\Folder1\Folder2 will record events because C:\Folder1\Folder2 (longest pathname) has higher precedence over C:\Folder1. Hence, all other folders present under C:\Folder1 are not monitored.

Why do I get an error when I try to save changes in McAfee ePO to my policy?

McAfee ePO currently does not limit but alerts the user if large number of policies are selected to be applied. An error is displayed when saving the policy if larger than the set limit.

By default, McAfee ePO in the server.xml tomcat is limited to take http post req of maxi size 2 MB.

If you need to increase this size, perform the following steps:

- Press Windows+R, type **services.msc**, and click **OK**.
- Right-click the **McAfee ePO x.x.x Application Server** service and select **Stop**.

Note

Replace McAfee ePO **x.x.x** with the actual McAfee ePO server version running in your environment.

- Press Windows+R, type **explorer**, and click **OK**.
- Navigate to: **c:\Program Files\McAfee\ePolicy Orchestrator\Server\conf**.
- Right-click **server.xml**, click **Edit**, and add the appropriate attribute to the connector 8443 section as follows:
  - For McAfee ePO 5.9.0 and later: **maxPostSize="10485760 MB" (For a 10 MB file)**.
  - **Original**:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector id="orion.server.https" port="8443" maxHttpHeaderSize="8192" maxThreads="150"
                minSpareThreads="25"
                maxSpareThreads="75"
                enableLookups="false"
                disableUploadTimeout="true"
                acceptCount="100"
                maxPostSize="10485760"
                scheme="https"
                secure="true"
                clientAuth="want"
                sslProtocol="TLS"
                keystoreFile="keystore/server.keystore"
                keystorePass="snowcap"
                truststoreFile="keystore/certAuthCa.truststore"
                truststorePass="snowcap"
                URIEncoding="UTF-8"
                server="Undefined"
```

  - **maxPostSize="10485760 MB" is added to the connector**:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<Connector id="orion.server.https" port="8443" maxHttpHeaderSize="8192" maxThreads="150"
                minSpareThreads="25"
                maxSpareThreads="75"
                enableLookups="false"
                disableUploadTimeout="true"
                acceptCount="100"
                maxPostSize="10485760"
                scheme="https"
                secure="true"
                clientAuth="want"
                sslProtocol="TLS"
                keystoreFile="keystore/server.keystore"
                keystorePass="snowcap"
                truststoreFile="keystore/certAuthCa.truststore"
                truststorePass="snowcap"
                URIEncoding="UTF-8"
                server="Undefined"
```

- Save the **server.xml** file with these edits.
- Press Windows+R, type **services.msc**, and click OK.
- Right-click the following service and click **Start**: McAfee ePO x.x.x Application Server.

Note

Replace **x.x.x** with the actual McAfee ePO server version running in your environment.

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.

How to handle Memory Leak from scsrvc.exe (User-mode)

Before you start collecting traces, you need to define how long it takes for the Application Control process to consume all available RAM from the Operating System, so you can divide the time and use it to capture 4 traces. Also, enable the advanced debugging for scsrvc.exe in Gflags tool (Global Flags Editor).

Gflags tool is included in Debugging Tools for Microsoft Windows. For more information, see Download Debugging Tools for Windows.

Once the debugging kit is installed, the tool (gflags.exe) is saved in: C:\Program Files (x86)\Windows Kits\10\Debuggers\x64 for Systems running 64 bits Windows or C:\Program Files (x86)\Windows Kits\10\Debuggers\x86 running 32-bits version of Windows.

In addition, you need poolmon.exe which is also part of the debugging tools, and procdump.exe which can be downloaded from Microsoft Sysinternals tool website. For details, click here.

Note

If the debugging package is installed while the product is in Update mode, all tools are solidified. But, if you are copying the tool from another system or downloading while the product is in Enabled Mode, solidify the tools or change the product to Update Mode. Otherwise the execution is denied.

Instructions to start the advance trace for scsrvc.exe:

- Open Command Prompt as an administrator and navigate to the path where the tool is saved.
- Run the following command:

```
<tool path>\gflags.exe /i SCSRVC.exe +ust
```

- Verify the Gflags is enabled for scsrv.exe by opening the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SCSRVC.exe\GlobalFlag = 0x00001000.
- Make sure MACC is in the operation mode where the memory leak is exhibited.
- Reboot the system for advance logging to start recording.

Scenario for data collection: If scsrvc.exe takes 48 hours to reach 4-GB RAM (all available RAM), you can reduce the trace time, because the 0-GB trace does not have enough info and 4-GB RAM trace might be hard to capture as the system might be in a crash state. So, in case, you remove 8 hours, in total we have 40 workable hours to capture 4 traces.

Every 10 hours, you must capture: poolmon and process dump (procdump) at the same time, using these commands:

- Open Command Prompt as an Administrator, and run:
  - <tool path>\poolmon.exe -b -p -r -n <filename>.log
  - <tool path>\procdump.exe -ma scsrvc.exe

- Repeat this process 4 times.
- Once you finish collecting poolmon and process dumps, disable gflags by executing: <tool path>\gflags.exe -i SCSRVC.exe.
- Then reboot the system and collect a MER.

How to handle memory Leak from Solidcore Tags (Kernel Mode)

In kernel mode, Solidcore tags name start with: Q*.

This issue is exhibited when these tags don't release allocated memory, which leads to system crash and the only way to recover is by rebooting it.

Before collecting any trace, you need to configure your system to generate full memory dump, and this is due to the nature of the issue, no User-mode processes exhibit high consumption generally.

Following instructions to force a system crash by pressing a combination of keys. For instructions, click here.

When configuring the dump options in Control Panel > System and Security > System. Click Advanced system settings. Under Startup and Recovery, click Settings. Select Complete Memory Dump in Write Debugging Information.

Like the user-mode scenario, you can define a time frame to capture 4 poolmon, and a full memory dump (forced through keyboard) when the system crashes or is unresponsive.

How to manually Purge data from McAfee ePO?

Application Control and Change Control collects and store information from all endpoints. This information can be categorized as: events, inventory, and Policy Discovery. McAfee Recommends that after all data is reviewed by the Solidcore Administrator, it needs to be purged to avoid data redundancy and performance degradation on the database caused by the product extension.

Before you purge any data related to Application Control and Change Control, you need to know-how much space this data would occupy and grow on your database. For that, McAfee has created a database sizing guide which helps you to identify the amount of data the product stores. For details about McAfee ePO database sizing recommendations to manage Application Control 6.2 and later, see KB83754.

From McAfee ePO, all purging tasks can be created and scheduled from Server Tasks:

- On the McAfee ePO console, select **Menu** → **Automation** → **Server task**.
- Click **New Task** to open the **Server Task Builder** wizard.
- Type the task name, then click **Next**.
- Select **Solidcore: Purge** from the **Actions** drop-down list.
- Configure **choose feature** option - Select the reporting feature for which to purge records.

Note

You can expand the **choose feature** option to find Client Task Log, Alerts, Inventory, Content Change Tracking Repository, Image Deviation, and Policy Discovery.

- Click **Next** to open the **Schedule** page.

- Specify schedule details, then click **Next** to open the **Summary** page.
- Review and verify the details, then click **Save**.

The following schedule frequencies need to be adapted in compliance with your company auditing and data restore policies:

- What we recommend — Purge Events older than 90 days.

Note

Purging the records from Solidcore Events table also purge related records from McAfee ePO Events Table.

- Purge Client Task Log older than 30 days.
- Purge alerts older than 90 days.
- Inventories are frequently updated and there is no need to remove them, if you need to remove the inventory from 1 particular system, you can use: Purge By Query. For more information, see KB81994.
- Content Change Tracking Repository is purged by query only.
- Purge Policy Discovery older than 90 days.

How to delete data directly on McAfee ePO database

- Go to the server that holds the McAfee ePO database.
- Select **All Programs** → **Microsoft SQL Server <version>** → **SQL Server Management Studio**.
- Select the Authentication type (Windows or SQL Server), and click **Connect to log** on to the SQL Server instance hosting the McAfee ePO database.
- Right-click database name for your McAfee ePO server and select New Query.
-

Note

If you are using McAfee ePO 5.10, do not select the events database. The script does not work properly unless it is run against the primary database.

Events — Solidcore client normally generates two events, and one is forwarded to EPOEvents table and the other one to SCOR_EVENTS table. Hence events need to be clean from both tables:

- DELETE from SCOR_EVENTS WHERE '2020-05-19T23:59:00.000' > SCOR_EVENTS.DETECTEDUTC
- DELETE from EPOEvents WHERE '2020-05-19T23:59:00.000' > EPOEvents.DetectedUTC AND EPOEvents.Analyzer='SOLIDCORE_META'

For example, today is 24 May 2020, and I want to remove events 90 days old, then both queries should be:

- DELETE from SCOR_EVENTS WHERE '2020-02-24T23:59:00.000' > SCOR_EVENTS.DETECTEDUTC
- DELETE from EPOEvents WHERE '2020-02-24T23:59:00.000' > EPOEvents.DetectedUTC AND EPOEvents.Analyzer='SOLIDCORE_META'

Alerts:

- DELETE from SCOR_ALERTS WHERE '2020-05-19T23:59:00.000' > SCOR_ALERTS.ALERT_TIMESTAMP

For example, today is 24 May 2020, and I want to remove events 90 days old, then the query should be:

- DELETE from SCOR_ALERTS WHERE '2020-02-24T23:59:00.000' > SCOR_ALERTS.ALERT_TIMESTAMP

Content tracking:

- DELETE from SCOR_FD_FILE_REPOS WHERE '2020-05-19T23:59:00.000' > SCOR_FD_FILE_REPOS.DETECTED_UTC
- DELETE from SCOR_FD_FILE_INFO WHERE '2020-05-19T23:59:00.000' > SCOR_FD_FILE_INFO.LAST_MODIFIED_TIME

For example, today is 24 May 2020, and I want to remove events 90 days old, then the query should be:

- DELETE from SCOR_FD_FILE_REPOS WHERE '2020-02-24T23:59:00.000' > SCOR_FD_FILE_REPOS.DETECTED_UTC
- DELETE from SCOR_FD_FILE_INFO WHERE '2020-02-24T23:59:00.000' > SCOR_FD_FILE_INFO.LAST_MODIFIED_TIME

Policy Discovery — The Policy Discovery information is stored in 4 different tables on the database:

- SCOR_VW_SA_GROUPED_REQUEST
- SCOR_VW_SA_REQUEST
- SCOR_SA_RULES
- SCOR_VW_SCOR_SA_REQUEST

To delete the data — DELETE from SCOR_VW_SCOR_SA_REQUEST where '2020-05-25T09:35:10.367' > SCOR_VW_SCOR_SA_REQUEST.DETECTED_UTC.

Solidification FAQs

What files do we solidify?

- PE 32 > EXE, DLL, SYS > all executable files
- Scripts > BAT, CMD, 16-bit EXE, VBS
- PE 64 > 64-bit executables

How to view scripts that can be solidified?

Run the following command to view scripts:

```
Sadmin Scripts list
```

How to determine if something is Solidified (on the whitelist)?

Run the following command to **list solidified** items:

```
Sadmin ls
```

- If it echoes the path and name, it is solidified.
- If not, not solidified.

Run the following command to **list unsolidified** items:

```
Sadmin lu
```

- If it echoes the path and name, it is unsolidified.
- If not, it is solidified.

Run the following command to **get advanced details about a file**:

```
Sadmin ls - lax
```

What hashes are collected in inventory?

Hashes collected for Solidcore version 7.x or earlier:

- SHA-1
- MD5

Hashes collected for Solidcore version 8.x or later:

- SHA-1
- MD5
- SHA-256

What is collected in Solidcore inventory file?

Inventory file contains details such as hash, reputation, and location.

Where can you view your client inventory?

On the McAfee ePO console, select **Menu** → **Application Control** → **Inventory**.

What is the function and specific use cases for each skiplist?

You can add skip rules using the `sadmin skiplist add` command and specify the needed arguments to skip path components from several features such as monitoring, write protection, file operations and script-auth, whitelist, and Application Control.

Monitoring

- Skiplist -c

Skiplist -c is used predominately in the Update mode to disable monitoring on files. This can be used to quiet events from showing up in MACC events. Think of a more powerful filter built into operate while in the Update mode.

Use case	This skiplist is used mainly on inventory files to suppress events in Update mode.

Applying this feature to an endpoint	You can't apply this skiplist through a policy. You must run from a sadmin command or locally from an endpoint. `Sadmin skiplist add -c <path/file>`
Risk	The risk associated with this process is medium. If a file is no longer monitored, it can't be executed without additional permission configured.

Write protection

- Skiplist -d

Skiplist -d is used to deny write passthrough attribute. This skiplist removes write protection from a file allowing it to be changed by any source.

Use case	This skiplist can be used when you modify a file with a generic updater. You can remove write protection from a file and block a generic process from updating your file. This allows the file to remain solidified but create hash mismatches. Net framework and directories where libraries are frequently upgraded and require execution.
Applying this feature to an endpoint	This skiplist can be applied through a policy in McAfee ePO or a sadmin run command. To apply it as a policy, go to the specified rule group, click filters, and select exclude path from write-protect rules. You must specify a path for the file. `Sadmin skiplist add -d <path/file>`
Risk	The risk associated with this process is high. There is a chance a malicious file could be placed in a path.

- Skiplist -r

Skiplist -r creates a registry path passthrough attribute. This process allows an application to modify the registry.

Use case	When registry write deny events are triggered by an application, a skiplist -r might be needed to allow the change.

Applying this feature to an endpoint	This skiplist can't be applied through a policy. You must run from a sadmin command or locally from an endpoint. `Sadmin skiplist add -r <registry>`
Risk	The risk associated with this process is high. It should only be used for processes that are known and trusted. It can be exploited if the policy is defined broadly.

File operations and script-auth

- Skiplist -f (think file)

Skiplist -f is used to create file operations passthrough. This rule allows you to create, modify, and delete files regardless of solidification. It will not allow you to overwrite links and rename files.

Use case	This skiplist is used when files are noisy and updated frequently if a filter does not work.
Applying this feature to an endpoint	This skiplist can be applied through a policy in McAfee ePO or a sadmin run command. To apply it as a policy, go to the specified rule group, click filters, and select exclude path from file operations rules. You must specify a path for the file. `Sadmin skiplist add -f <path/file>`
Risk	The risk associated with this process is high. It should be used when a filter is not working.

- Skiplist -i (think folder)

Skiplist -i or ignore passthrough attribute, ignores path, and works similar to a skiplist -f.

Use case	When on a 64-bit platform, this skiplist can be used with 32-bit and earlier processes. A reboot is needed for this rule to work. Another use case is jar files that are modified frequently that do not run without an interpreter.
Applying this feature to an endpoint	This skiplist can be applied through a policy in McAfee ePO or a sadmin run command. To apply it as a policy, go to the specified rule group, click filters, and select Ignore path for file operations rules. You must specify a path for the file.

	`Sadmin skiplist add -i <path/file>`
Risk	The risk associated with this process is medium as files can now be modified freely.

Whitelist

- Skiplist -s

Skiplist -s is a process used to bypass the solidification status of a file. This process also unsolidifies files.

Use case	This skiplist should be used when files or paths do not need solidification. The solidified files and paths are not allowed to execute.
Applying this feature to an endpoint	This skiplist can be applied through a policy in McAfee ePO or a sadmin run command. To apply it as a policy, go to the specified rule group, click filters, and select exclude local path and all its files and subdirectories from the whitelist. You must specify a path for the file. `Sadmin skiplist add -s <path/file>`
Risk	The risk associated with this process is low. Once files are unsolidified, they can't be executed. The only risk is if you unsolidify a legitimate application, it is denied execution.

Application Control

- Skiplist -v

Skiplist -v is used to exclude a volume or drive from being whitelisted.

Use case	This skiplist is used when a server has multiple drives that do not require solidification.
Applying this feature to an endpoint	This skiplist can be applied through a policy in McAfee ePO or a sadmin run command. To apply it as a policy, go to the specified rule group, click filters, and select exclude volume from Application Control protection. You must specify a volume/drive. `Sadmin skiplist add -v <volume:>`
Risk	The risk associated with this process is low.

What is an Alternate Data Stream (ADS)? Does Change Control monitor changes to ADS?

On the Microsoft NTFS file system, a file consists of multiple data streams. One stream holds the file contents and another contains security information. You can create alternate data streams (ADS) for a file to associate information or other files with the existing file. In effect, alternate data streams allow you to embed information or files in existing files. The ADSs associated with a file do not affect its contents or attributes and are not visible in Windows Explorer. So, for practical purposes, the ADSs associated with a file are hidden. Malicious users can misuse the ADS feature to associate malicious files with other files without the malicious files being detected.

Change Control monitors changes to any ADS associated with files on Windows platforms. For a monitored file, ADS-related changes, including stream creation, modification, update, deletion, and attribute changes are reported as events. If you are also using Application Control, the base file name is retrieved and permissions for the base file are checked when an ADS is invoked. The ADS is allowed or denied execution based on the permissions of the base file and current mode of Application Control. Also, any executable programs (associated as an ADS with an existing file) are prevented from running. To disable ADS monitoring, execute the **SC: Run Commands** client task to run the `sadmin features disable mon-ads` command on the endpoint.

Why am I not receiving the events for user account activity for an endpoint?

User account activity is not tracked by default for endpoints. To track operations for user accounts, you must enable this feature specifically on endpoints where Change Control is deployed and enabled. To enable this feature, execute the **SC: Run Commands** client task to run the sadmin features enable mon-uat command on the endpoint.

In addition, you must make sure that the Audit Policy is configured on the Windows operating system to allow generation of user activity events.

To successfully track user account activity for an endpoint, verify the Audit Policy configuration for the endpoint.

1. Navigate to **Control Panel** → **Administrative Tools**.
2. Double-click **Local Security Policy**.
3. Select **Local Policies** → **Audit Policy**.
4. Double-click the **Audit account logon events** policy.
5. Select **Success** and **Failure**, then click **OK**.
6. Repeat steps 4 and 5 for the **Audit account management** and **Audit logon events** policies.

What are the implications of recovering the local CLI access for an endpoint?

To troubleshoot or debug issues, you might need to recover the local CLI access for an endpoint. Recovering the local CLI for an endpoint prevents the enforcement of policies from McAfee ePO to the endpoint. This implies that when the CLI is recovered for an endpoint, no existing or new policies (created on the McAfee ePO server) are applied to that endpoint.

What is the significance of the label specified in a policy while configuring updater processes, installers, and users?

The specified labels help you correlate the generated events with the actions performed by the trusted resources. For example, when an event is generated for an action performed by a trusted user, the **Workflow ID** attribute for the event includes the label specified for the trusted user.

How do I unsolidify a file, directory, or volume?

To unsolidify a file, directory, or volume, run the **SC: Run Commands** client task with the `sadmin unso <resource name>` command.

Note

As a best practice, do not unsolidify a system drive or volume.

I recently fetched inventory for an endpoint but can't review GTI ratings for the inventory items. What can I do?

If GTI ratings are unavailable for inventory items after you fetched inventory, review the logs generated by the **Fetch File Details from McAfee GTI Server** and **Fetch Certificate Reputation from McAfee GTI Server** server tasks on the **Server Task Log** page. Log entries are added atypically for the **Fetch File Details from McAfee GTI Server** server task to the **Server Task Log** page.

- If the task succeeds and the previous run was unsuccessful, a log entry is added.
- If the task fails, a new log entry indicating failure is added. But, if communication with the server fails continuously, one entry is added for a day. The time stamp indicates the failure time and the log message provides the reason for failure.

So, on the **Server Task Log** page, you might see fewer entries indicating task success and multiple entries indicating failure for this task.

Do Change Control and Application Control work in Network Address Translation (NAT) environments?

If the McAfee ePO server can communicate with the McAfee Agent in a NAT environment, Change Control and Application Control work.

How can I trust applications developed for use in my organization?

Sign the applications with a self-generated certificate, then trust the certificate.

1. Perform one of these actions.
   - Locate your certificate if you have an existing certificate.
   - Generate an X.509 certificate pair using a tool, such as makecert.exe (see this for details).
2. Export the certificate in PEM (Base-64 encoded X.509 - .CER) format.
3. Upload the certificate and add it to an Application Control policy as a trusted certificate.
4. Apply the policy to the endpoints.
5. Use the certificate to sign and verify in-house applications. This can be done using a tool, such as SignTool.exe.

   Note

   When working with scripts, convert the script into a self-extracting executable file, then sign the file.

6. Define the internal certificate as a trusted certificate.

Can I script sadmin commands?

Yes, you can script sadmin commands. While recovering the CLI, you are prompted to enter to password. To achieve this in a script, suffix the `sadmin recover` command with `-z <password>`.

How can I resolve discrepancies and inconsistencies in the Solidcore rule groups after upgrading the Solidcore extension? When I access the Rule Groups page, an Internal Server Error is displayed.

Run the **Rule Group Sanity Check** server task from the McAfee ePO console to fix the inconsistencies in the rule groups. This server task reports and corrects (if possible) discrepancies and inconsistencies in the Solidcore rule groups and policies.

1. Select **Menu** → **Automation** → **Server Tasks**.
2. Click **New Task**.

   The **Server Task Builder** wizard opens.

3. Type the task name and click **Next**.
4. Select **Solidcore: Rule Group Sanity Check** from the **Actions** drop-down list.
5. Click **Next**.
6. Specify the schedule for the task.
7. Click **Next**.

   The **Summary** page appears.

8. Review the task summary and click **Save**.
9. Review the logs generated by the server task (on the Server Task Log page) to view the warnings, if any.

How do I manage the predefined rules available with Change Control and Application Control?

Revisit the predefined rules available with Change Control and Application Control when you install or upgrade the Solidcore extension. Because the software installed on the endpoints in your enterprise might change (is added or removed), you must revise the rules periodically. Based on the software installed on the endpoints in your setup, revise the rules and remove unwanted or irrelevant rules.

How can I enable or disable selected features on endpoints from the McAfee ePO console?

Use the Application Control Options (Windows) policy to enable or disable selected features on endpoints from the McAfee ePO console.

1. Select **Menu** → **Policy** → **Policy Catalog**.
2. Select the **Solidcore 8.0.0: Application Control** product.
3. Select the **Application Control Options (Windows)** category.
4. Click the **My Default** policy.
5. Switch to the **Features** tab.
6. Select **Enforce feature control from ePO**.
   For more information about these features.

   - ActiveX, see *ActiveX controls*.
   - Memory Protection, see *Memory-protection techniques*.

- Package Control, see *Package Control*.

7. Select the features to enable or disable.
8. Save the policy and apply to the relevant endpoints.

How can I implement change reconciliation and ticket-based enforcement in my setup?

Change reconciliation correlates change events from monitored systems with tickets in your change management system (CMS). This correlation categorizes events as authorized or unauthorized based on whether the change was made during an update window. This information is used for change tracking and compliance reporting. Ticket-based enforcement allows you to automatically open update windows on systems protected with Application Control and Change Control by integrating with your CMS. Based on tickets created in the CMS, update windows open on the protected systems to allow modification of protected files and registry keys. Implementing ticket-based enforcement reduces system outages and improves uptime by allowing only approved changes to the systems.

Perform these steps to configure and implement change reconciliation and ticket-based enforcement.

1. Make sure that reconAutoReconcileEvents setting in the database is set to true. Contact McAfee Support for instructions.
2. Set the required permissions.
    - User must have **System Tree** access to the systems where the tasks are to be scheduled.
    - User must have permission to send agent wake-up call.
    - Create and edit tags permission is required to run tasks on multiple systems.
    - View and change task settings permission is needed in McAfee Agent if you are using McAfee ePO 5.0 or later.
3. Understand and use the web service APIs provided by Application Control and Change Control.

Web service API	Description	
`begin-update (systemNames/systemIds, workflowId, time, wakeupAgent)`	Opens an Update window to perform ticket-related changes. This service takes these parameters:	
	`systemNames/systemIds`	(Required) Comma-separated list of system names, IP addresses, or system IDs (from the McAfee ePO database). If you specify system IDs and system names, only the specified system IDs are considered.
	`workflowId`	(Required) Ticket ID from the ticketing system for the update window. The specified ticket ID is associated with the updated records.

Web service API	Description	
	`time`	(Required) Time when to open the Update window on the endpoints. Use the yyyy-mm-dd hh:mm:ss format to provide the value.
	`wakeupAgent`	(Optional) Flag to indicate whether to wake up agents after scheduling the task. The default value for this parameter is true.
	This service returns the ID associated with the client task that opens the Update window on the specified endpoints.	
`end-update (systemNames/ systemIds, workflowId, time, wakeupAgent)`	Closes the Update window after performing ticket-related changes. This service takes these parameters:	
	`systemNames/systemIds`	(Required) Comma-separated list of system names, IP addresses, or system IDs (from the McAfee ePO database). If you specify system IDs and system names, only the specified system IDs are considered.
	`workflowId`	(Required) Ticket ID from the ticketing system for the update window.
	`time`	(Required) Time when to close the Update window at the endpoints. Use the yyyy-mm-dd hh:mm:ss format to provide the value.
	`wakeupAgent`	(Optional) Flag to indicate whether to wake up agents after scheduling the task. The default value for this parameter is true.
	This service returns the ID associated with the client task that closes the Update window on the specified endpoints.	
`delete-task (taskIds)`	Deletes the client tasks created to open and close the Update window for a ticket. This service takes only one parameter.	
	`taskIds`	(Required) Comma-separated list of IDs associated with the client tasks that open and close the Update window

Web service API	Description	
		on the specified endpoints. The client tasks that are associated with the IDs are deleted.
	This service returns a list of true and false values corresponding to each specified client task ID. True indicates that the client task associated with the specified ID was successfully deleted.	

These web service APIs can be accessed through URLs. Here are a few examples to help you understand the type of calls you can make to the web service APIs.

- begin-update — `https://<epo-server>:<port>/remote/scor.updatewindow.updateWindowCommand.do?:output=json&action=begin-update&systemNames=<comma separated IP addresses or names>&time=2013-12-19%2011:05:00&workflowId=ticket1&wakeupAgent=true`
- end-update — `https://<epo-server>:<port>/remote/scor.updatewindow.updateWindowCommand.do?:output=json&action=end-update&systemNames=<comma separated IP addresses or names>&time=2013-12-19%2012:05:00&workflowId=ticket1&wakeupAgent=true`
- delete-task — `https://<epo-server>:<port>/remote/scor.updatewindow.updateWindowCommand.do?:output=json&action=delete-task&taskIds=123,234`

4. Review the sample Java connector that is shipped with the Solidcore extension. You can download and save the SampleConnector.zip file from the McAfee Downloads site. This file is available for your reference and can help you understand how to integrate with the web service APIs in your setup.

After I deploy Application Control, how can I check the status of the memory protection techniques, such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR), provided by the Windows operating system?

Review the status of the techniques for one endpoint	1. Click the endpoint on the **Systems** page to view details for the selected endpoint. 2. Click the **Products** tab. 3. Click the **Solidcore** row to view product details. 4. Review the values for the **Memory Protection (ASLR)** and **Memory Protection (DEP)** properties.
Review the status of the techniques for multiple endpoints	1. On the McAfee ePO console, select **Menu** → **Reporting** → **Queries and Reports**. 2. Select the Application Control group under **McAfee Groups**. 3. Click **New**. 4. Select **Solidcore Client Properties** for the **Result Type** and click **Next**.

	5. Select **Table** in the **Display Results As** list, select **System Name** in the **Sort By** list, and click **Next**. 6. Add the **Memory Protection (ASLR)** and **Memory Protection (DEP)** properties and click **Next**. 7. Click **Run** to view details for the endpoints in your setup.

Here are the possible values for DEP and ASLR.

Technique	Possible value	Description
DEP	Enabled (Always On)	DEP is enabled for all processes.
	Disabled (Always Off)	DEP is disabled for all processes.
	Disabled (With Opt In)	DEP is enabled only for Windows system components and services.
	Enabled (With Opt Out)	DEP is enabled for all processes. You can choose to remove processes from the DEP technique.
	Not Supported	DEP technique is not supported on the hardware.
ASLR	Enabled	ASLR is enabled for all processes.
	Disabled	ASLR is disabled for all processes.
	Enabled (Partial)	ASLR is enabled and VASR bypass rules might be present.

The software is allowing the execution of a banned file. What could be the reason?

When defined rules are applied, the software combines or aggregates the rules defined for a file. When applying the rules, it uses the following order to determine whether the file execution is allowed or blocked. The order in which the methods are listed indicates the precedence the software applies to the method.

1. Banned by SHA-1 or SHA-256
2. Executed by updater process or trusted user
3. Allowed by SHA-1 or SHA-256

4. Allowed by certificate
5. Banned by name
6. Allowed by name
7. Executed from trusted directory
8. Added to whitelist

If none of the above apply for a file, the software blocks the execution of the file.

I have defined variables on the Linux platform. Can I use these variables to define rules in Application Control or Change Control?

User-defined variables are not supported in the McAfee ePO-managed configuration.

The McAfee ePO interface is slow or unresponsive and count of observations on the Predominant Observations page is high. What is the cause and how can I resolve this problem?

Application Control includes predefined rules to filter non-relevant and unnecessary observations you receive from endpoints. The rules are included in the **Observation Filter Rules (Deprecated)** rule group (shipped with the product). By default, these rules are applied to the global root in the **System Tree** and hence are inherited by all McAfee ePO-managed endpoints.

If you remove this rule group, you might receive many observations that cause the McAfee ePO interface to be slow or unresponsive. Review your setup and make sure that this rule group is applied to the endpoints.

How can I check the solidification or whitelisting status for an endpoint?

Perform these steps to review the solidification or whitelisting status for an endpoint.

1. From the McAfee ePO console, select **Menu** | **Systems** | **System Tree**.
2. Select the group associated with the endpoint in the **System Tree** pane.

   The endpoints in the group are listed in the **Systems** tab.

3. Click **Actions** | **Choose Columns**.
4. Navigate to the **Solidcore Client Properties** list and select the **Solidification Status** property.
5. Click **Save** to return to the **Systems** tab.
6. Navigate to the row corresponding to an endpoint and review the value listed in the **Solidification Status** column.

How can I apply multiple policies to one node in the System Tree?

Perform these steps to apply multi-slot policies to a group or specific endpoints.

1. From the McAfee ePO console, select **Menu** | **Systems** | **System Tree**.
2. Perform one of these actions.
   - Group — Select a group in the **System Tree** and switch to the **Assigned Policies** tab.
   - Endpoint — Select the endpoint on the **Systems** page, then click **Actions** → **Agent** → **Modify Policy on a Single System**.

3. Click **Edit Assignments** for the multi-slot policy where you want to assign multiple policies.
4. Click **New Policy Instance**.
5. Select the policy that you want to assign from the **Assigned policy** field.
6. Click **Save**.

I am trying to fetch the software inventory for an endpoint, but the SC: Pull Inventory client task fails and I receive a message that the inventory cannot be fetched. What is the reason and how can I fetch the inventory successfully?

By default, you can fetch the inventory for an endpoint once in seven days. This value is set as the minimum interval between consecutive inventory runs. But, if needed, you can configure this value for your enterprise. See *Configure settings for fetching the inventory*.

What is the difference between custom action and taking global actions for a request?

For selected endpoints, to define custom rules to allow, ban, or allow by certificate an application or executable file, use the **Create Custom Policy** action. You can also define custom rules to allow a network path for selected endpoints. But, to allow, ban, allow by certificate an application or executable file globally (on all endpoints in your enterprise), or to allow a network path globally, take global actions.

I am using the Number of Systems where Throttling Initiated in Last 7 days monitor on the Health Monitoring dashboard. Why is no data visible when I select List events that initiated throttling for a system link?

When you select the **List events that initiated throttling for a system** link, the **Events** page lists events that resulted in the generation of the **Data Throttled** or **Data Dropped** events. The list includes all events that were generated in the 7-days period before receiving the **Data Throttled** or **Data Dropped** events.

In these two scenarios, the **Events** page does not list any data.

- Consecutive **Data Throttled** and **Data Dropped** events are received for a system.
- Events yet to be received at the McAfee ePO console. This can occur when the endpoint for which throttling initiated is parsing older data and is yet to send the newer events to the McAfee ePO server.

Also, the same scenario can occur for policy discovery requests (observations) and inventory updates.

I want to change the value of a configuration parameter for a managed endpoint. I cannot find a policy or method to complete this from the McAfee ePO console. How can I complete tasks for which no method is available on the McAfee ePO console?

From the McAfee ePO console, you can use the **SC: Run Commands** client task to run any CLI commands remotely on one or more endpoints. The commands can include tasks that can or cannot be completed using McAfee ePO, such as enable or disable the product, change the value for configuration parameters, or fetch the software inventory.

1. From the McAfee ePO console, select **Menu** | **Systems** | **System Tree**.
2. Perform one of these actions.
    - To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
    - To apply the client task to an endpoint, select the endpoint on the **Systems** page, then click **Actions** → **Agent** → **Modify Tasks on a Single System**.

3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select the **Solidcore 8.0.0** product, **SC: Run Commands** task type, then click **Create New Task** to open the **Client Task Catalog** page.
5. Specify the task name and add any information.
6. Specify the command you want to run on the endpoints.

   For example, to change the value of configuration parameters, specify the `sadmin config set <ParameterName>=<ParameterValue>` command.

7. (Optional) Specify the option to receive the result of the command by clicking **Requires Response**.

   The command output is available on the **Menu** → **Automation** → **Solidcore Client Task Log** page.

8. Click **Save**.

How can I lock down or recover the local CLI for managed endpoints?

By default, the local CLI is locked down for McAfee ePO-managed endpoints. But, you can recover the CLI for one or more endpoints, if needed.

Important

When you recover the CLI, any changes to configuration, policies, tasks pushed from the McAfee ePO server are not enforced on the endpoint. So, the CLI status must be set to **Restrict** to enforce any changes to the endpoint.

1. From the McAfee ePO console, select **Menu** | **Systems** | **System Tree**.
2. Perform one of these actions.
   - To apply the client task to a group, select a group in the **System Tree** and switch to the **Assigned Client Tasks** tab.
   - To apply the client task to an endpoint, select the endpoint on the **Systems** page, then click **Actions** → **Agent** → **Modify Tasks on a Single System**.
3. Click **Actions** → **New Client Task Assignment** to open the **Client Task Assignment Builder** page.
4. Select the **Solidcore 8.0.0** product, **SC: Change Local CLI Access** task type, then click **Create New Task** to open the **Client Task Catalog** page.
5. Change CLI status to **Restrict** or **Allow**.
6. Click **Save**.

I seem to have run into issues while applying a content update package in my setup. How can I resolve this?

If the McAfee ePO server is temporarily unavailable when a content update is being applied, you might run into issues. We recommend that you wait until the update is applied. Review the **Content update for Application Control and Change Control** entry on the **Server Task Log** page to verify if the content update was applied successfully. If the issue isn't resolved or the update status is failed, contact McAfee Support for assistance.

I am trying to access a page and it displays the Content update is in progress warning message. Why is this happening?

We can now automatically push content updates for Application Control and Change Control through the McAfee ePO console. This eliminates the need for customers to apply hotfixes for configuration changes, such as rules, policies, or McAfee GTI settings. For example, any changes to the McAfee GTI settings or certificate are automatically applied in your setup.

When a content update is being applied, you should not make any changes to existing rules and configuration. The warning message is displayed while the content update is being applied and disappears after the update is complete. For every content update that is applied, a corresponding **Content update for Application Control and Change Control** entry is added to the **Server Task Log** page. You can review the entry for details of the changes made.

How can I view the reputation for a specific file on an endpoint?

To view the reputation for a specific file on an endpoint, fetch the file reputation from a source (TIE server, McAfee GTI, or Advanced Threat Defense), as applicable. But, make sure that the reputation setting is enabled in **Application Control (Options)** policy applied to the endpoint. For more information about how to enable reputation settings, see *Configure reputation settings*.

Use the **SC: Run Commands** client task to run this command on the endpoint.

```
sadmin getreputation [ -v | -b ] -f <filename> -m <md5> -h <sha-1> -s <reputation-source>
```

You must specify MD5 and SHA-1 value for a file to fetch its reputation. But, if you also specify the file name with its MD5 and SHA-1 value, the file name is considered for fetching the reputation.

This table lists the supported arguments and their description.

Argument	Description
-v	Specify this argument to display all sources and the file reputation stored in them.
-b	Specify this argument to bypass the internal cache for stored file reputation and fetches the reputation from the specified source.
-f	Specify the file name for which you want to fetch the reputation.
-m	Specify the MD5 value of the file for which you want to fetch the reputation.
-h	Specify the SHA-1 value of the file for which you want to fetch the reputation.
-s	Include the source to fetch the file reputation from.

How can I recover the CLI for an endpoint if the CLI is disabled after multiple incorrect password attempts?

If the CLI is disabled after multiple incorrect password attempts, there are two methods to recover the CLI:

- To immediately recover the CLI, the administrator can send the **SC: Change Local CLI Access** client task from the McAfee ePO console.
- To recover the CLI from the endpoint, enter the correct CLI recover password on the CLI after the disable time period lapses.

When the CLI is recovered, the **Recovered Local CLI** event is sent to the McAfee ePO console to notify the administrator.

I am reviewing inventory items and can see the Inventory for one or more systems could not be processed. Increase memory allocated for Java Virtual Machine. message. How can I resolve this?

Starting with the 8.0.0 release, Application Control can process large volume of inventory items. If inventory cannot be fetched from an endpoint due to lack of Java Virtual Machine memory on the server, the

Inventory for one or more systems could not be processed. Increase memory allocated for Java Virtual Machine.

message is displayed on the **By Applications** and **By Systems** pages. To resolve this, complete these steps:

1. Navigate to the **By Systems** page.
2. Select the **Systems with Failed Inventory Fetch** filter.
3. Review the listed systems.
4. For each system where **Inventory Fetch Status** is set to **Failed (low JVM memory)**, hover over the status to review information about JVM memory needed.
5. Optionally, select **Actions | Choose Columns** and select **JVM Memory Required (in GB)** from **Available Columns** list and click **Save**. You can review the minimum memory required for each system.
6. Increase memory according to listed requirements for the endpoints. Before upgrading to the suggested JVM value, make sure that your system meets the needed RAM requirements. For more information, review this link.

When using Application Control and Change Control, which features and workflow support SHA-1 and SHA-256?

Starting with the 8.0.0 release, we have added support for file SHA-256 values (for the Windows platform). This table lists how existing features and workflows use SHA-1 and SHA-256 values.

Feature	Capability	SHA-1	SHA-256
Executable files	Define allow or ban rules for executable files (in policy or rule group)	Yes	Yes
Updater Processes	Define allow or ban rules for updater processes (in policy or rule group)	Yes	Yes

Feature	Capability	SHA-1	SHA-256
Installers	Define allow or ban rules for installer (in policy or rule group)	Yes	Yes
Certificates	Add rules for trusted certificates (in policy or rule group)	Yes	Yes
	View certificate details about Solidore pages	Yes	No
Policy discovery	Add rules to process requests	Yes	Yes
	Group requests for display on **Policy Discovery** page	Yes	No
Inventory	Add rules for inventory items	Yes	Yes
	Group items for display on **Inventory** pages	Yes	No
Solidcore events	Review event information and file details	Yes	Yes
Rule groups	Add rules to a rule group to associate with a policy	Yes	Yes
Reputation-based rules	Add rules to allow or ban files based on their reputation	Yes	No
Scan a Software Repository server task	Scan a repository to add installers and certificates to McAfee ePO	Yes	Yes
Send McAfee GTI feedback	Send feedback to McAfee about your current use of the McAfee GTI and Application Control features	Yes	No
Offline GTI Tool	Fetch McAfee GTI ratings for files and certificates	Yes	No
McAfee GTI reputation	Determine file reputation and classification	Yes	No
TIE server	Determine file reputation and classification	Yes	No

Except when stated, all other Application Control and Change Control workflows are based on file SHA-1 values. In other words, the linking between events (on **Solidcore Events** page), file details (on **Inventory** pages), and requests (**Policy Discovery** page) are based on the file's SHA-1 values.

I recently fetched inventory for an endpoint and need to fetch inventory for it again. How can I do this?

For Application Control, the minimum interval between consecutive inventory runs (when the inventory information is fetched from the endpoints) is set to seven days. This is the default value and implies that for an endpoint you can pull inventory once a week. But, if needed, you can configure this value for your enterprise. See *Configure settings for fetching the inventory*.

One of these happen when you fetch inventory for an endpoint:

- If inventory for the endpoint was fetched in the last seven days, inventory updates are fetched.
- If inventory for the endpoint was not fetched in the last seven days, complete inventory details are fetched.

I received the Unable to Recover Inventory event for an endpoint. What can I do?

The **Inventory Corrupted** event is generated for an endpoint if the internal inventory for the endpoint is corrupt. Application Control maintains inventory backup for the endpoint and recovers the inventory for the endpoint from the backup copy.

- If the inventory is recovered successfully from the backup copy, the **Recovered Inventory** event is generated.
- If for some reason, the inventory can't be recovered from the backup copy, the **Unable to Recover Inventory** event is generated. To rectify, execute the **SC: Run Commands** client task with the sadmin so command.

COPYRIGHT

Trellix