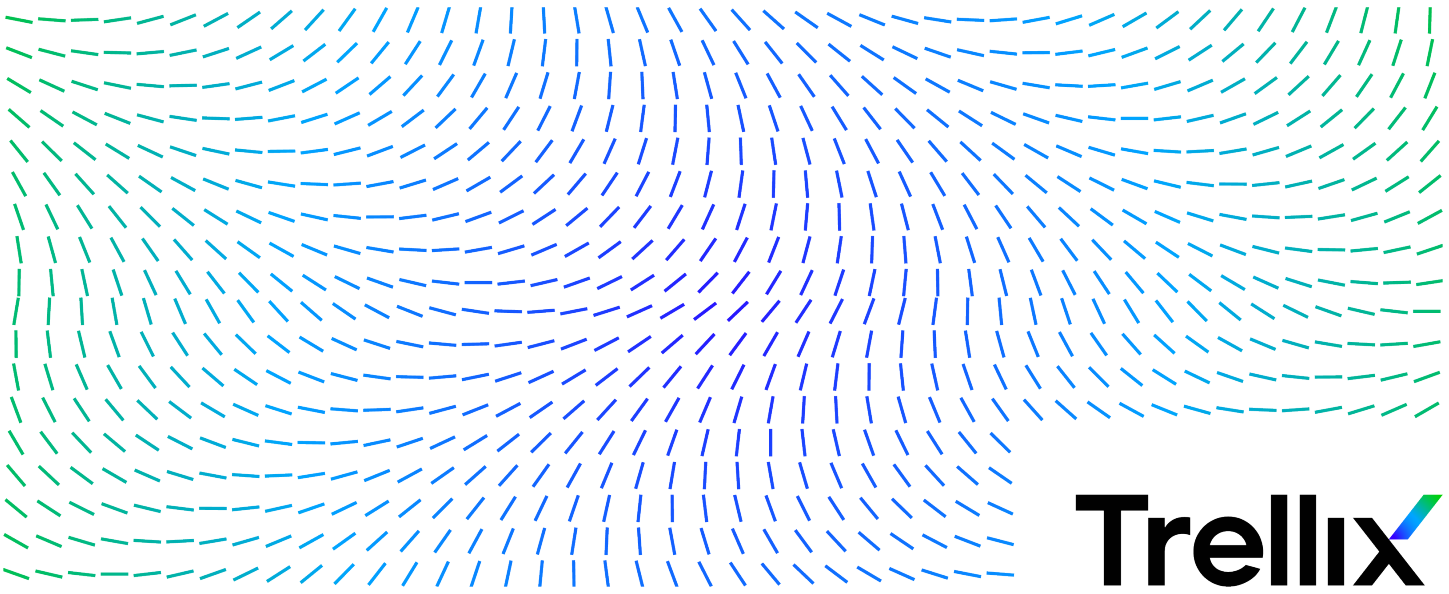
McAfee Application and Change Control 6.4.x - Linux Product Guide



Contents

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 to allow updates to protected files. 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.

Protection against threats

Application Control extends coverage to executable files, libraries, drivers, Java applications, 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.

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.

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 and directories. 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 changes in real time, eliminating need for multiple scans on endpoints to identify change violations.

Content change tracking

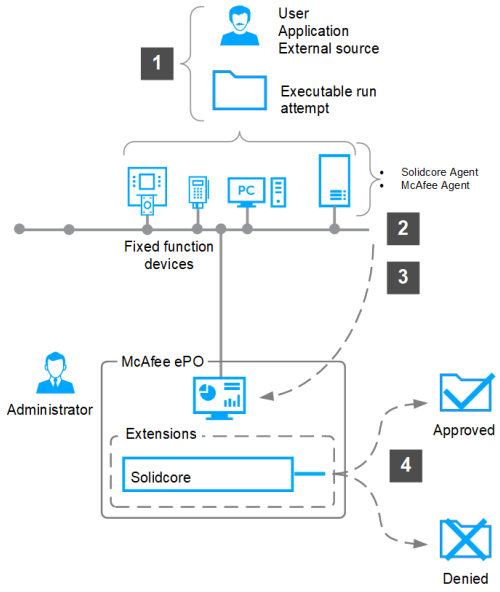
Change Control tracks content and attribute changes for files and includes special alerting mechanisms to instantly notify you of critical changes.

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 is not whitelisted, Application Control blocks its execution.

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 execute. All files in the whitelist are protected and can't be changed or deleted.

1. A user or application tries to execute a file where Application Control and McAfee® Agent are installed.
2. Solidcore Agent and McAfee Agent are installed on the managed endpoints. When a user or application tries to execute a file, McAfee Agent registers the attempt and sends the event to McAfee ePO.
3. Solidcore Agent checks if the executable is added to the inventory as whitelisted.
4. If the executable is whitelisted, the file is allowed to run.



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.

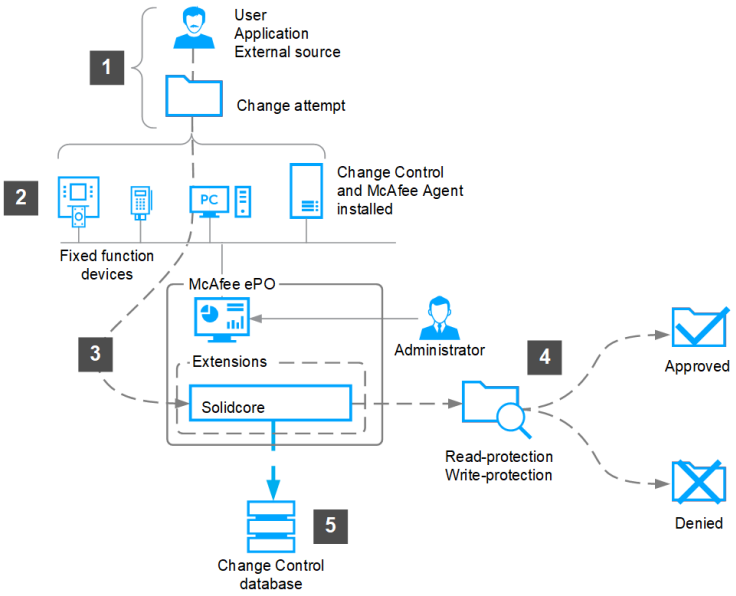
It tracks changes to files in real time and it identifies who made changes to which files.

1. A system user tries to change a file 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:

- <volume>/.solidcore/scinv

Using the software

Software modes

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

Enabled mode

This mode indicates that the software is running and protection is enabled.

In Enabled mode, Application Control allows only trusted or authorized (based on rules) applications and installers to run on servers and endpoints. Change Control prevents unauthorized changes to critical system files, directories, and configurations.

Observe mode

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

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.

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.

Disabled* mode

Although a complete disabling of the software without a system reboot is technically not possible, a partial disable or a no-tracking state can be achieved without a reboot by using a special mode called *Global Passthru* or *Disabled** mode. Because everything is passed through, Application Control monitors nothing and the system behaves as if it is in Disabled mode with the following exceptions:

- Kernel modules remain loaded.
- Minimal tracking continues.

Switching between modes

- From Observe mode, you can switch to Enabled or Disabled mode.
- From Enabled mode, you can switch to Disabled(*), Update, and Observe mode.
- From Update mode, you can switch to Enabled or Disabled mode.
- From Disabled mode, you can switch to Enabled, Update, or Observe mode.

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. Deselect **Reboot endpoint**, then click **Save**.
   When using Solidcore client version 6.1.0 or later, restarting the system is not needed to enable the software.
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. `service scsrvc restart`
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. `service scsrvc restart`
4. Verify that the software is in Enabled mode:
   `sadmin status`

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.

Authorize binaries

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

Syntax	Description
`sadmin auth add -a <checksumvalue>`	Specify the SHA-1 or SHA-256 value of the binary to be authorized. For example: `sadmin auth add -a 803291bcc5aa45a0221b4016f62d63a26d3ee4af`

Syntax	Description
`sadmin auth add -au [-t tagname] <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 add -au -t linux_updater 803291bcc5aa45a0221b4016f62d63a26d3ee4af`

Note

Use `sadmin auth list` to list authorized binaries.

Ban binaries

You can restrict binaries from executing on a protected system.

Syntax	Description
`sadmin auth add -b <checksumvalue>`	Specify the SHA-1 or SHA-256 value of the file to be banned. For example: `sadmin auth add -b 803291bcc5aa45a0221b4016f62d63a26d3ee4af`

Note

Use `sadmin auth list` to list banned binaries.

Remove checksum rules

You can remove authorized or banned binaries from your system.

Syntax	Description
`sadmin auth remove <checksumvalue>`	Specify the SHA-1 or SHA-256 value of the file to be removed. For example: `sadmin auth remove 803291bcc5aa45a0221b4016f62d63a26d3ee4af`

Syntax	Description
`sadmin auth flush`	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 trusted_executable`
- `sadmin attr add -u untrusted_executable`

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 /mnt/smb_share_mountpoint
   sadmin trusted -i /etc/security
   ```
2. View the list of trusted directories:

   ```
   sadmin trusted -l
   ```
3. Exclude specific directories:

   ```
   sadmin trusted -e <pathname1...pathnameN>
   sadmin trusted -e /etc/security
   ```
4. Remove trusted directories:

   ```
   sadmin trusted -r <pathname1...pathnameN>
   sadmin trusted -r /etc/security
   ```

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.

- `sadmin trusted -i /mnt/smb_share_mountpoint`
- `sadmin trusted -i /etc/security`

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 ***** wildcard character. Using /abc/*/def is allowed while /abc/*.sh, /abc/*.*, or /abc/doc.* aren't 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.

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 Rules (Unix)** 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 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: Application Control**	**Application Control Rules (Unix)**	Multi-slot	Default rules to design the trust model on the Linux/ UNIX platform. This policy also includes default filters to exclude events that are not relevant for your setup.	Yes

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.

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.
- 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 ***** wildcard character. Using `/abc/*/def` is allowed while `/abc/*.sh`, `/abc/*.*`, or `/abc/doc.*` are not supported.

Using monitoring rules

What can you monitor?

You can monitor files, directories, and programs.

Element	Tracked operations
File	• File creation • File change (file content and attributes, such as permissions, owner, or group) • File deletion • File rename
Process	• Process start • Process stop

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.

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 or fully qualified path. 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/*.sh, /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.

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**.
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.
   b. Edit the settings to specify the filter.
   c. Click **+** or **Add Rule** to specify additional `OR` conditions or `AND` conditions.
6. 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, 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. **Note:** Changing the maximum file size affects the McAfee ePO database sizing requirements and might have an impact on performance.

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.

Write protection rules prevent users from creating and changing existing files, 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 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.

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. 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 ***** wildcard character. Using /abc/*/def is allowed while /abc/*.sh, /abc/*.*, or /abc/doc.* aren't supported.

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. 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. Enter the location of the file.
   c. Enter a unique identification label for the executable file.
   d. 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 **Parent** to allow the file to run as an updater only if it is started by the specified parent.
   e. 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.
   f. 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.
   g. 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 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.

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*.

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. Enter the location of the file.
    If you add the updater by name, the updater is not authorized automatically. The file must be added to the whitelist.
    c. Specify an identification updater label for the program.
    d. 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 **Parent** to allow the file to run as an updater only if it is started by the specified parent.
    e. 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.

f. 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.

g. 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.

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

Argument	Description
-d	Excludes the child process of the file from inheriting updater permissions. `sadmin updaters add -d <filename>`
-n	Disables event logging for a file to be added as an updater. `sadmin updaters add -n <filename>`
-t	Includes the tags for a file to be added as an updater. `sadmin updaters add -t <RULE-ID> <filename>`
-p	Adds a file as an updater, only when its parent execution file is running. `sadmin updaters add -p <parentname> <filename>`

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>
```

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.

The software controls execution of scripts with `#!` when run using the `./<script name>` syntax. By default, scripts with #! are not allowed to execute.

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]...`
2. View interpreter and file extension associations
   `sadmin scripts list`
   Sample output appears like this:

```
.sh      "ksh" "sh" "tcsh" "bash" "csh"
.jar     "java"
.class   "java"
.py      "python"
.pl      "perl"
```

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 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.

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**.

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

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
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
7	20706	END_UPDATE	**Closed Update Mode**	Info	Information	SC
8	20707	COMMAND_EXECUTED	**Command Executed**	Info	Information	SC
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
56	20755	OWNER_MODIFIED	**File Ownership Changed**	Info	Information	CC
57	20756	OWNER_MODIFIED _UPDATE	**File Ownership Changed**	Info	Information	CC
62	20761	INVENTORY_CORRUPT	**Inventory Corrupted**	Critical	Critical	AC
63	20762	BOOTING_DISABLED _SAFEMODE	**Booted in Disabled mode**	Warning	Warning	SC

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
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
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

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
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
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

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
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
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**	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
			Stream Created			
107	20806	STREAM_DELETED	**Alternate Data Stream Deleted**	Info	Information	CC
108	20807	STREAM_MODIFIED	**Alternate Data Stream Modified**	Info	Information	CC
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	**Attribute Modified in**	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
		_MODIFIED_UPDATE	**Data Stream**			
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
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

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
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
125	20824	BOOTING_OBSERVE	**Booted in Observe Mode**	Info	Information	AC
131	20830	THROTTLING_STARTED	**Data Throttled**	Major	Warning	SC
132	20831	THROTTLING_CACHE _FULL	**Data Dropped**	Major	Error	SC

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)	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
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

Event ID (on endpoints)	Threat event ID (on McAfee ePO)	Event name	Event display string	Solidcore client severity	McAfee ePO severity	Event type
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
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

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**
- **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

To check events in Standalone - Linux system, view the **solidcore.log**.
cat /var/log/mcafee/solidcore/solidcore.log

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	Trellix 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	Trellix Solidifier prevented an attempt to change file <string> by process/script <string> (sha1: <string> , md5: <string>,

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
				sha256: <string>) (Process Id: <string>, User: <string>).
21	20720	EXECUTION_DENIED	Major	Trellix 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	Trellix 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	Trellix Solidifier prevented process <string>, run by <string>, from making unauthorized access to API <string> (return address <string>). The process was terminated
49	20748	REG_VALUE_WRITE_DENIED	Major	Trellix 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	Trellix Solidifier prevented an attempt to change Registry key '<string>' by process <string> (Process Id: <string>, User: <string>)

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
51	20750	REG_KEY_CREATED_UPDATE	Info	Trellix Solidifier detected creation of registry key '<string>' by program <string> (User: <string>, Workflow Id: <string>).
52	20751	REG_KEY_DELETED_UPDATE	Info	Trellix Solidifier detected deletion of registry key '<string>' by program <string> (User: <string>, Workflow Id: <string>).
54	20753	REG_VALUE_DELETED_UPDATE	Info	Trellix Solidifier detected deletion of registry value '<string>' under key '<string>' by program <string> (User: <string>, Workflow Id: <string>).
57	20756	OWNER_MODIFIED_UPDATE	Info	Trellix Solidifier detected modification to OWNER of '<string>' by program <string> (User: <string>, Workflow Id: <string>).
61	20760	PROCESS_HIJACKED	Major	Trellix Solidifier detected an attempt to exploit process <string> (sha1: <string>, md5: <string>, sha256: <string>) from address <string>.
62	20761	INVENTORY_CORRUPT	Critical	Trellix Solidifier detected that its internal inventory for the volume <string> is corrupt.
75	20774	FILE_CREATED_UPDATE	Info	Trellix Solidifier detected creation of '<string>' by program <string> (User: <string>, Original User: <string>, Workflow Id: <string>).
76	20775	FILE_DELETED_UPDATE	Info	Trellix Solidifier detected deletion of '<string>' by program <string> (User:

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
				<string>, Original User: <string>, Workflow Id: <string>).
77	20776	FILE_MODIFIED_UPDATE	Info	Trellix Solidifier detected modification of '<string>' by program <string> (User: <string>, Original User: <string>, Workflow Id: <string>)
79	20778	FILE_RENAMED_UPDATE	Info	Trellix 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>).
89	20788	READ_DENIED	Major	Trellix Solidifier prevented an attempt to read file '<string>' by process <string> (Process Id: <string>, User: <string>).
96	20795	PKG_MODIFICATION _PREVENTED	Critical	Trellix Solidifier prevented package modification by '<string>'(sha1: <string>, md5: <string>, sha256: <string>) by user: '<string>'.
97	20796	PKG_MODIFICATION_ALLOWED _UPDATE	Info	Trellix Solidifier allowed package modification by <string>'(sha1: <string>, md5: <string>, sha256: <string>) by user: '<string>'. (Workflow Id: <string>).

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
98	20797	PKG_MODIFICATION _PREVENTED_2	Critical	Trellix Solidifier prevented package modification by '<string>' by user: '<string>'.
99	20798	NX_VIOLATION_DETECTED	Critical	Trellix 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	Trellix Solidifier detected modification to registry value '<string>' of type '<string>' under key '<string>' by program '<string>' (User: <string>, Workflow Id: <string>), with data: <string>
103	20802	FILE_READ_UPDATE	Info	Trellix Solidifier detected read for '<string>' by program <string> (User: <string>, Original User: <string>, Workflow Id: <string>)
124	20823	INITIAL_SCAN_TASK_COMPLETED	Info	Trellix Solidifier Initial Scan task is complete and Application Control is enforced on the system now.
126	20825	ACTX_ALLOW_INSTALL	Info	Trellix Solidifier allowed installation of ActiveX <string> Workflow Id: <string> by user <string>
127	20826	ACTX_INSTALL_PREVENTED	Major	Trellix Solidifier prevented installation of ActiveX <string> Workflow Id: <string> by user <string>

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
129	20828	VASR_VIOLATION_DETECTED	Critical	Trellix 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.
136	20835	OBSERVED_FILE_EXECUTION	Info	Trellix 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	Trellix 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>'.

Event ID (on systems)	Threat event ID (on McAfee ePO)	Event name	Severity	Description
138	20837	INVENTORY_RECOVERED	Critical	Trellix Solidifier has detected that the inventory for volume <string> is corrupt. The backup dated <string> is loaded.
139	20838	INVENTORY_RECOVER_FAILED	Critical	Trellix 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	Trellix 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

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.

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**.

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 tried 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 tried 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. • 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.
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 based on 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 the Application Control licenses. The pie chart categorizes the information by 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.

Query	Description
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.
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.

Query	Description
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.
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.
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.

Write protection and read protection

What is write protection?

Write protection is a feature that protects the files, directories, and volumes 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 volume, write protection is applied to all files and subdirectories in that directory or volume. 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 volumes to prevent unauthorized programs or users from changing them.

Task

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 ***** wildcard character. Using/abc/*/def is allowed while /abc/*.sh, /abc/*.*, or /abc/doc.* is not supported.

For example:

-

```
# sadmin write-protect -i /etc/security/limits.conf
```

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 /mount-point`	Specify the mount point name on the Linux platform. For example: `sadmin write-protect -i /nfs`

Exclude components from write protection

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

Task

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 /etc/security/limits.conf`

View write-protected components

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

Task

Run this command at the command prompt.

`sadmin write-protect -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 /etc/security/limits.conf`

2. Flush write protection from all components.

   `sadmin write-protect -f`

What is read protection?

Read protection is a feature that protects the files, directories, and volumes 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 ***** wildcard character. Using/abc/*/def is allowed while /abc/*.sh, /abc/*.*, or /abc/doc.* is not supported.

For example:

- `# sadmin read-protect -i /etc/password`

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 volume.

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 /etc/password`

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 /etc/password`

2. Flush read protection applied to all components.

   `sadmin read-protect -f`

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.

When running in Observe mode, Application Control emulates Enabled mode but only logs observations.

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.

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 uninstallation activities for managed endpoints.

In Observe mode, a file is allowed to execute unless it is banned by a specific rule. 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.

   Note

   Observe mode can only be activated after the endpoint has been solidified once.

   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.

Place endpoints in Observe mode

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

Select at least one endpoint for each type you have in your environment.

Task

1. On the McAfee ePO console, select **Menu** → **Systems** → **System Tree**.
2. Select a group or an endpoint:
    - 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: Observe Mode**, then click **Create New Task** to open the **Client Task Catalog** page.
    a. Specify the task name and add any descriptive information.
    b. (Optional) Specify a *workflow ID* tag to label the events generated during Observe mode.
    c. Click **Save**, specify scheduling details, then click **Next**.
    d. On the **Schedule** page, specify scheduling details, then click **Next**.
5. Review the task details, then click **Save**.
6. (Optional) Wake up the agent to send your client task to the endpoint immediately.

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.
- **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.

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, and user comments, if any.
   c. Review the individual requests that make up the collated request in the **Enterprise Level Activity** pane.
   d. 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 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.

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**, or **Allow Trusted Path**, 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.

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.

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.

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.

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.

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.

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**.

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.

```
Trellix Solidifier:           Disabled
Trellix Solidifier on reboot: Disabled

ePO Managed:    No
Local CLI access: Recovered

[fstype]           [status]        [driver status]      [volume]
* ext4     Solidified       Attached        /
```

Status detail	Description
Trellix Solidifier	Specifies the operational mode of Application Control.
Trellix 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

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, `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`
	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	Enabled	Windows

Feature	Description	Default status	Supported Operating System
	installations. Simultaneous installation of ActiveX controls using multiple tabs of Internet Explorer is not supported.		
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
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.	Enabled	Windows and Linux

Feature	Description	Default status	Supported Operating System
	• 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.		
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
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

Feature	Description	Default status	Supported Operating System
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>`

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 directories

- 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.

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. 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.

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	Path	Description
solidcore.log	/var/log/mcafee/solidcore/	After the product is deployed on a system, a log file named solidcore.log is created in the solidcore directory. 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.

Log file	Path	Description
		Note: Configuring log files is applicable only to the solidcore.log file. You can't change the configuration of any other log file.
Solidcore_Installer.log and solidcoreS3_install_<rel>-<build>.log	• /tmp/solidcoreS3_install.log • /var/log/mcafee/solidcore/solidcoreS3_install.log	Application Control installation logs are stored in this file. If installation fails, the file is stored at: /tmp/solidcoreS3_install_<rel>-<build>.log. If installation is successful, the file is stored at: /var/log/mcafee/solidcore/solidcoreS3_install_<rel>-<build>.log

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.

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|-p|-u file...`
- `sadmin attr add -o parent=PARENT_FILE -p FILE`
- `sadmin attr remove [-a|-p|-u]`
- `sadmin attr list [-a|-p|-u] [file...]`
- `sadmin attr flush [-a|-p|-u ]`

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 add { -a | -u [ -t rule-id ] | -au [-t rule-id ] | -b } <checksum>`
- `sadmin auth flush`
- `sadmin auth list`
- `sadmin auth remove <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]]`

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`

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]`

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 remove [-p parent-binaryname] binaryname`
- `sadmin updaters remove [-l libraryname] binaryname`
- `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`

Command short forms

You can use the commands short forms which are interchangeable.

Command	Short form
`sadmin write-protect`	`sadmin wp`
`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.
	`-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.

Command	Argument	Description
`auth`	`-a`	Authorizes a binary using the checksum value.
	`-b`	Bans a binary using the checksum value.
	`-t`	Includes a rule-id associated to the updater-related actions.
	`-u`	Authorizes a binary and also provides updater rights when used with the `-a` argument.
`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.
`check`	`-r`	Fixes any inconsistencies that are encountered.
`config`	`-a`	Appends the configuration values.
`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

Command	Argument	Description
`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.
	`-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.

Command	Argument	Description
	`-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.
	`-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.
`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.

Command	Argument	Description
	`-r`	Removes the specified directories or volumes from the trusted rule.
`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.
	`-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.
`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.

COPYRIGHT

Trellix