ivanti

Endpoint Security

powered by HEAT Software

Application Control Best Practice Guide

Dec 2020

Contents

Introduction

Ivanti Application Control allows you to quickly identify all applications running in your environment and prevent the installation and execution of any unwanted, untrusted, or malicious applications—without relying on the latest antivirus definitions and vulnerability patches.

How Does Application Control Work?

Application Control prevents malware and zero-day attacks with limited disruption to your organization's productivity. This enables you to establish and maintain a secure environment while also minimizing your administrative workload.

The following are the key principles that drive Application Control:

Application Whitelisting

Manage the applications in your environment by creating and enforcing an endpoint whitelist, which is a list of the executables that are allowed to run on a specified endpoint. You create the initial whitelist using Easy Auditor, which scans the endpoint to compile the list of executables.

Central Application Authorization

After the endpoint scan completes, the list of executables appears in the Application Library so that you can organize them into Applications and Application Groups. You can then authorize the files for additional users or groups, or add the files to a Denied Applications Policy to prevent certain users or groups from executing them.

Change Management Policies

Use policies to manage changes in your applications such as update releases and user requests for new applications.

- Supplement the endpoint whitelist with a Supplemental Easy Lockdown/Auditor policy.
- Update the whitelist automatically with a Trusted Updater to minimize your workload. Updaters install new applications and patch existing applications. They can also update the endpoint whitelist if you have allowed them to make endpoint changes.
- Use Trusted Change policies to allow specific files to execute.
- Implement Local Authorization policies to allow end users to authorize applications themselves. You can still choose to add those files to the whitelist or to the Denied Applications group, overriding the end user's decision.

Endpoint Oversight

You can monitor endpoint activity with Application Event Log Queries and update policies as needed to authorize or deny executables.

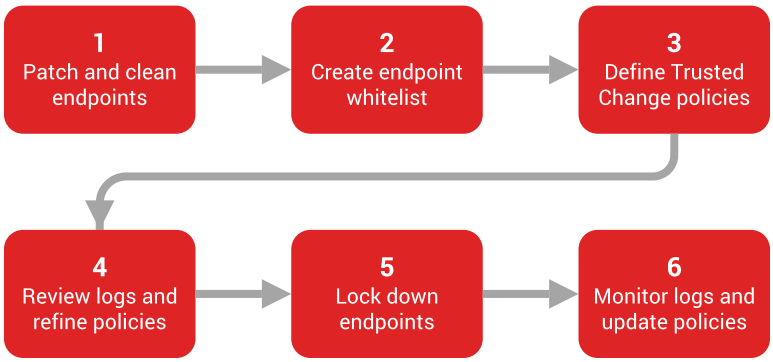
Advanced Memory Protection

Application Control includes advanced Memory Protection to defend against memory-based attacks in unpatched systems. Memory-based attacks never touch the host hard drive, so they are undetectable by file-based security systems like antivirus and application whitelisting. The Advanced Memory Protection feature provides extra defense against these prevalent attacks.

Best Practices Workflow

This document provides a best practices workflow for implementing Application Control in your environment. Use this document in conjunction with the Application Control User Guide. While Application Control is designed to minimize your administrative workload, it's important to implement these controls on your endpoints to avoid issues later.

Implement Application Control in your environment in six phases:



1. Patch endpoints and remove any malware prior to introducing Application Control.
2. Use Easy Auditor to create an endpoint whitelist.
3. Define Trusted Change policies to implement in your environment.
4. Review Application Event logs daily and refine your Trusted Change policies in preparation for locking down your endpoints.
5. Lock down your endpoints in phases.
6. Continue to monitor logs regularly to determine when to update your policies.

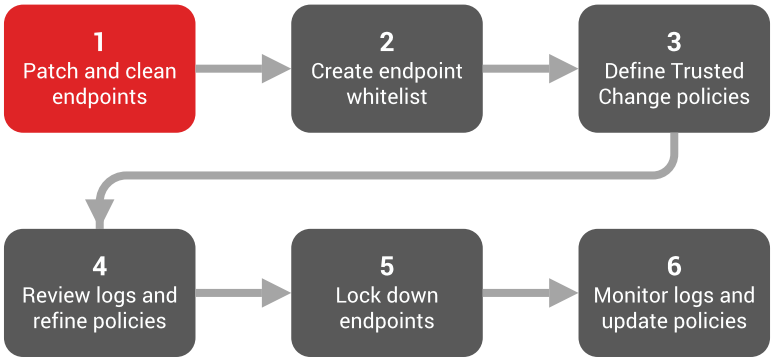
Don't lock down your endpoints before defining policies, as this increases the likelihood of problems later. Define policies first as described in this guide, and then lock down endpoints.

Communicate with Users

Notify your users that you plan to roll out Application Control and provide an overview of what they can expect. Continue communicating with users during each phase. See Appendix 2 for sample end user communications.

Phase 1: Patch and Clean Endpoints

Prior to introducing Application Control to your environment, patch any vulnerabilities on your endpoints with the latest security patches. Then scan endpoints to remove any malware that may be present. This cleanup prevents the system from adding malware to the whitelist you'll create later, so that your endpoints don't get re-infected.



In this phase you will:

- Identify and patch any known security vulnerabilities on your endpoints
- Perform a thorough antivirus scan on your endpoints to remove any dormant malware (malware buried within archives)
- Schedule the antivirus scan to run outside of your organization's operating hours to avoid disrupting productivity
- Communicate with your users so that they understand why you are patching and scanning endpoints. See Appendix 2 for sample end user communications.

Apply Security Patches

Unpatched vulnerabilities leave your environment open to malware attacks. Keeping your endpoints updated with the latest patches is crucial to keeping your network secure. Scan the endpoints in your environment to identify known vulnerabilities, then apply the necessary patches to those endpoints. Apply patches outside of your organization's operating hours where possible.

To patch your endpoints with Patch and Remediation, refer to the Ivanti Patch and Remediation User Guide and the Ivanti Patch and Remediation Best Practices Guide.

Run an Antivirus Scan

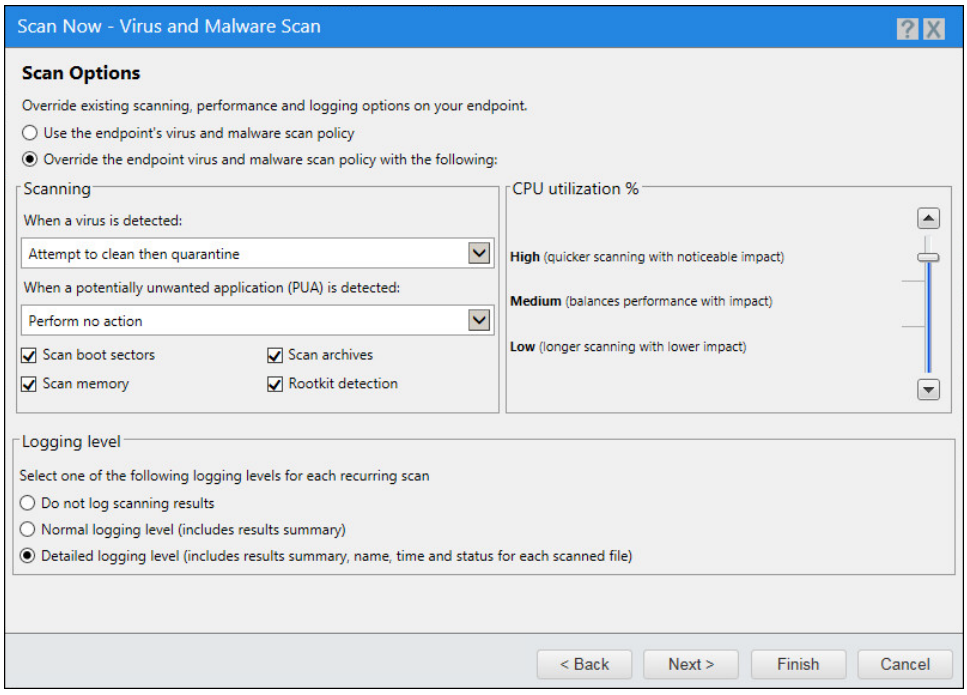
Scan your endpoints with either Ivanti AntiVirus or a third-party antivirus program. In either case, perform a thorough scan to ensure that you identify and remove any dormant malware.

Because a thorough antivirus scan could take a long time to complete, we recommend that you schedule the scan outside of your organization's operating hours. If you must run the scan during working hours, notify users so that they're aware of the process.

To Scan Endpoints with Ivanti AntiVirus

From the Endpoint Security Console, use the Scan Now - Virus and Malware Scan Wizard to perform a thorough or full system scan. See The Virus and Malware Scan Wizard in the Ivanti AntiVirus User Guide for detailed steps.

Select all the scanning options, including **Scan archives**, as shown.



You've patched known vulnerabilities and removed malware. Your endpoints are now in a "known good" state and you're ready to create your endpoint whitelist.

Communicate with Users

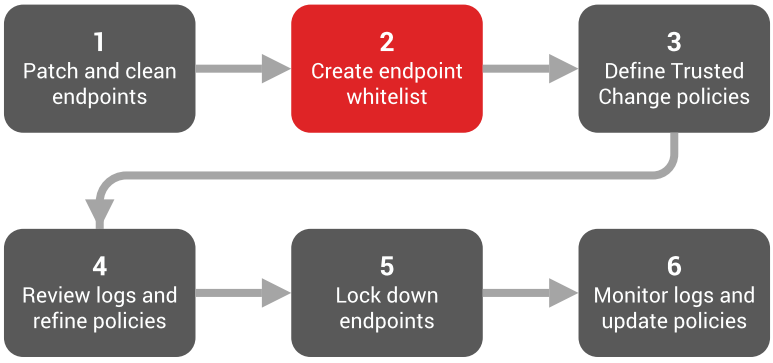
You've already communicated with your end users about the introduction of Application Control. Phase 1 likely involves some level of end-user disruption, so continue communicating in Phase 1 so that users understand why their endpoints are being patched and cleaned. Explain the impact this may have on productivity.

See Appendix 2 for sample end user communications.

Phase 2: Create an Endpoint Whitelist

This phase introduces you to Application Control. You'll see what applications are executing in your environment and decide which ones to authorize. You'll also scan your endpoints to create the endpoint whitelist that's used in later phases. This process puts the endpoints into an audit mode so that you can monitor activity on the endpoints.

This phase also introduces Memory Protection. Even though endpoints will be in audit mode, you can block specified applications and memory-based attacks.



In this phase you will:

- Scan a small number of endpoints using Easy Auditor to create an endpoint whitelist and discover what applications exist in your environment
- Review these applications in the Application Library and create Denied Applications Policies for any unwanted software
- Customize the blocked notification dialog to inform users why applications are being blocked and what to do if they need to use the blocked applications
- Enable Memory Protection to prevent memory injection attacks
- Communicate with users so that they understand that Application Control is being implemented, their endpoints will be scanned, and that certain applications are now prohibited and will be blocked. See Appendix 2 for sample end user communications.

What is Application Whitelisting?

Application Control prevents the execution of malicious code and unwanted software by using a security approach called application whitelisting. This approach allows only authorized applications to run on your endpoints.

A whitelist is a list of executable files that are authorized to run on an endpoint.

What is Easy Auditor?

Easy Auditor is a policy that creates a whitelist of authorized applications already on an endpoint, without blocking any applications that are installed later. It scans endpoints and adds the executables it finds to each endpoint's whitelist. This lets you to build a picture of application usage on the network without affecting users' ability to run the applications they need.

Plan Ahead

Scanning your endpoints to build the endpoint whitelist requires a fair amount of CPU and disk resources and may take several hours to complete. Run this scan outside of operating hours, if possible, to avoid disrupting productivity.

Make sure your endpoints are configured so that they do not go into sleep or hibernation modes, as these force the scan to start over.

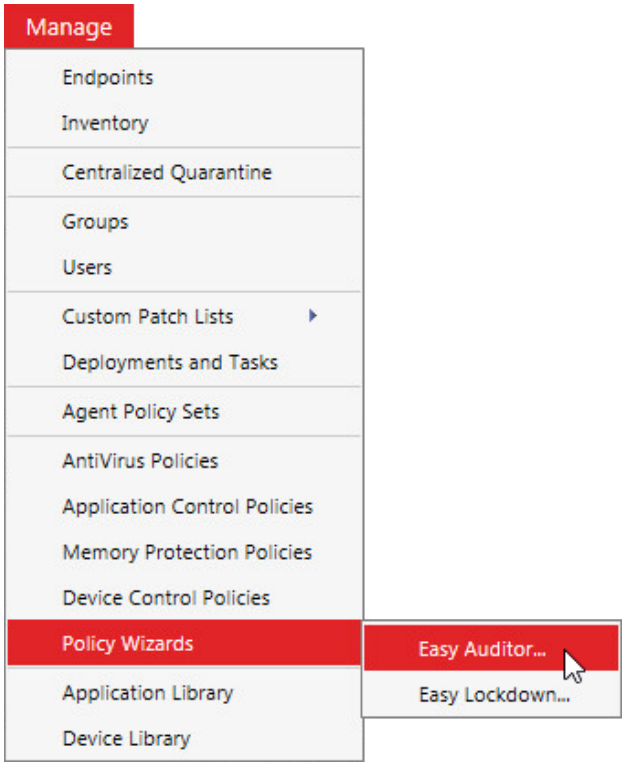
Select Sample Endpoints

In this phase, start by scanning 10 or fewer endpoints so that you can review the initial logs without being overwhelmed by data. Select endpoints that give you the widest representation of variability within your organization. These endpoints will populate the Application Library with a diverse range of applications. Include endpoints from departments such as:

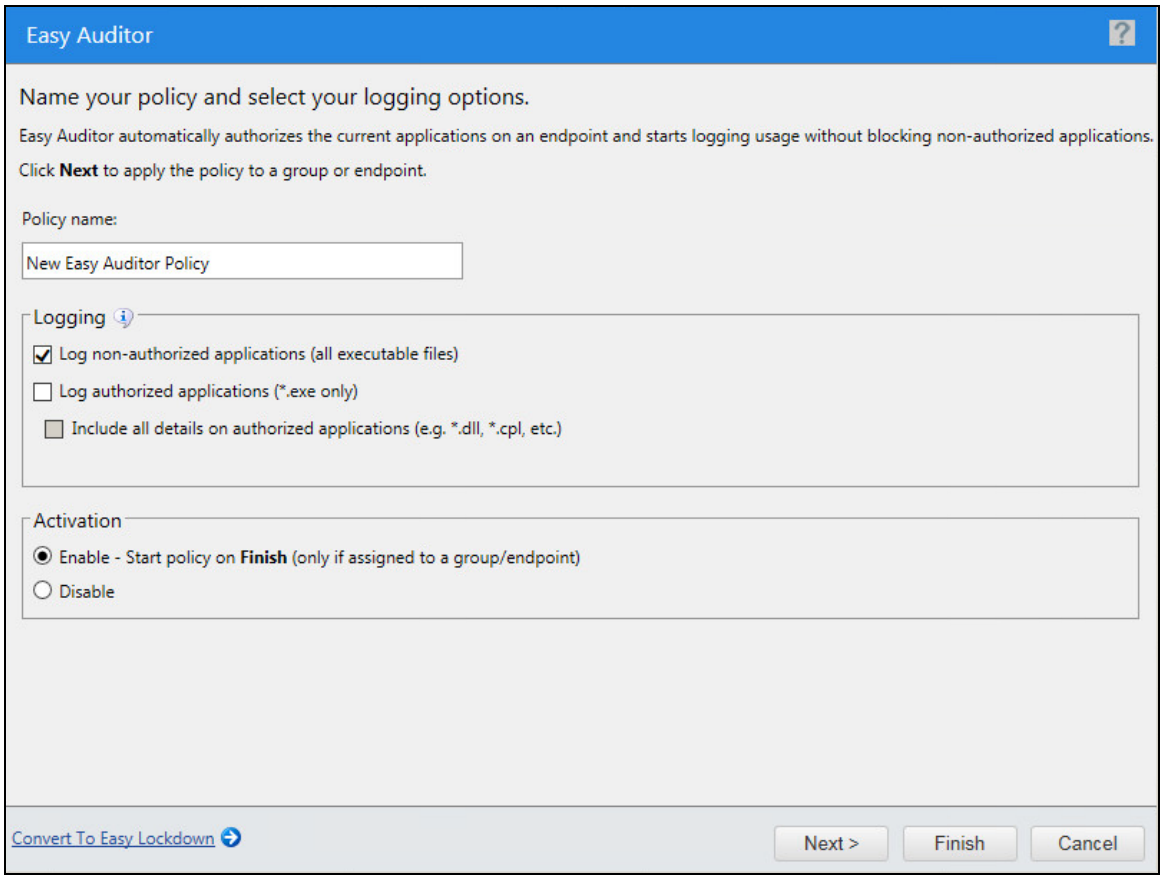
- Human Resources
- IT
- Sales
- Engineering

To Scan Endpoints with Easy Auditor

1. From the Endpoint Security Console, select **Manage** > **Policy Wizards** > **Easy Auditor**.

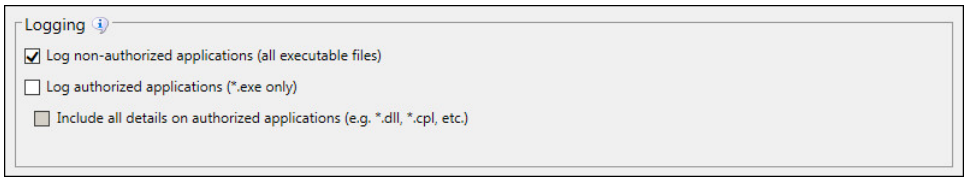


The Easy Auditor Wizard opens.



2. Proceed through the wizard. See Creating an Easy Auditor Policy in the Application Control User Guide for additional explanation and detailed steps.

Avoid positive logging, which is logging the execution of authorized applications. Logging authorized applications can result in very large log file sizes and consumes excess space on your Endpoint Security Server. Instead, log only non-authorized applications. You can, however, log authorized applications when troubleshooting an endpoint.



You've scanned your endpoints for applications and created an endpoint whitelist. Each endpoint now goes into a non-blocking audit mode and logs when applications are executed, based on the logging settings you selected. These logs are sent to your Endpoint Security Server so that you can analyze them.

View Files in Application Library

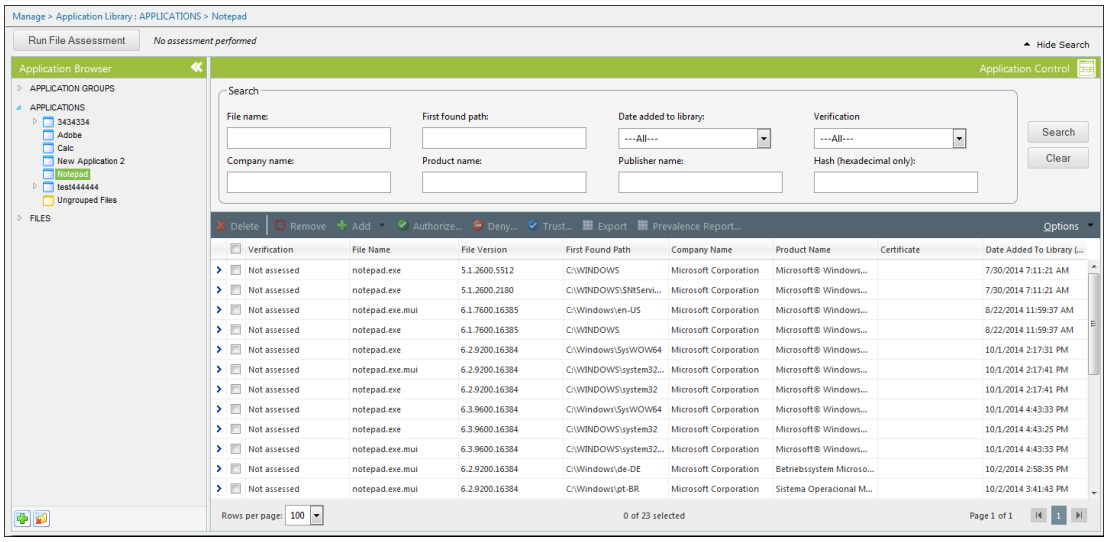
After running Easy Auditor, all of the file details from the scanned endpoints are populated in the Application Library on your Endpoint Security Server. These new files are located in the Ungrouped Files folder in the Application Library. You can organize these files into Applications and Application Groups so that you can authorize or deny them centrally.

To View the Application Library

1. From the Endpoint Security Console, select **Manage > Application Library**.

2. Select a view from the **Application Browser**.

   The list displays the files or applications associated with the selected view.



For detailed steps on organizing your Application Library, See Organizing Application Library by Application and Organizing Application Library by Application Group in the Application Control User Guide.

What are Denied Applications Policies?

A Denied Applications Policy blacklists any files, Applications, or Application Groups that you add to it. These applications won't execute in your environment. Apply the policy to all users or just to specific groups of users.

Denied Applications policies are useful not only for blocking suspicious files, but also for blocking unwanted software that interrupts productivity or increases network bandwidth consumption, including:

- Hacking tools
- Music streaming software
- Insecure instant messaging applications
- VoIP applications
- Games
- File sharing applications

You can install this unwanted software on a test endpoint, scan it, and organize it in the Application Library. Alternatively, if these applications are already in use in your environment, you can create a log query that includes these applications and deny them from there.

At this point, you should focus only on creating policies for denied applications; don't start creating policies for authorized applications yet. You'll focus on authorizing applications after locking down endpoints, which we discuss later in this document.

When to Apply a Denied Applications Policy

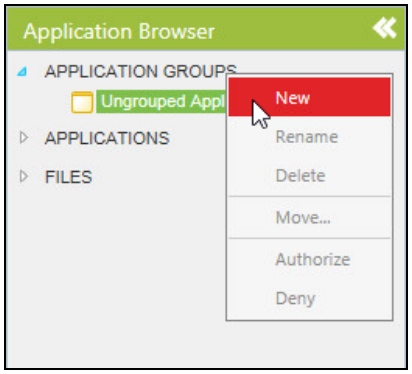
You can apply a Denied Applications policy at any time. However, if you choose to apply the policy prior to putting endpoints into Easy Auditor or Easy Lockdown, you can deny applications for *any* endpoint that has the Application Control module installed, regardless of user. This is because Application Control evaluates the Denied Applications policy before all other policies (including the endpoint whitelist), so a Denied Applications policy prevents anything from executing that could otherwise be authorized to execute via the whitelist or a Trusted Change policy. See "Appendix 1: Decision Flow at the Endpoint" on page 89 for details.

To Deny Applications for All Users

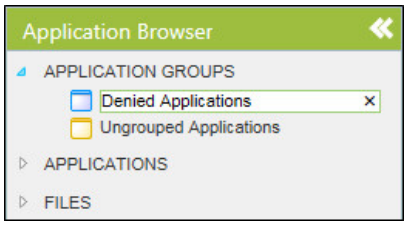
You can quickly deny applications for all users from within the Application Library.

1. From the Endpoint Security Console, select **Manage > Application Library**.

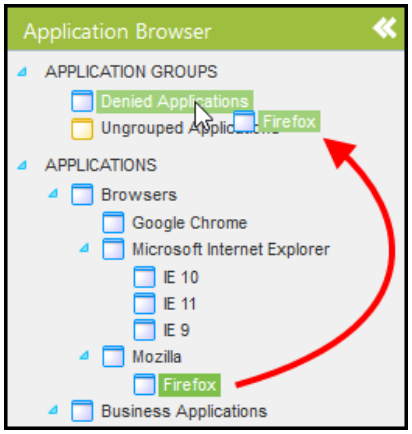
2. In the Application Browser panel on the left, right-click **APPLICATION GROUPS** and select **New**.



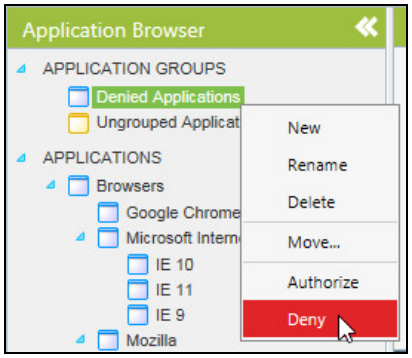
3. Name the group "Denied Applications" or something similar.



4. Identify the Applications that you want to deny for all users. Drag and drop the Applications into the **Denied Applications** group you created.



5. Right-click the **Denied Applications** group and select **Deny** to launch the Denied Applications wizard.



6. Complete the wizard to create the Denied Applications policy. Assign it to all users.

After you assign this group to all users, you can simply continue adding applications to this group and they are subsequently denied for all users.

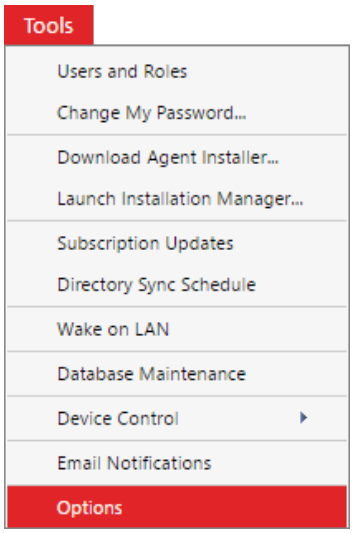
Why Customize the Blocked Notification Dialog?

You should inform users of any blocked applications and provide a process for users to request authorization for them. Some of your users may have a legitimate business need for accessing a blocked application.

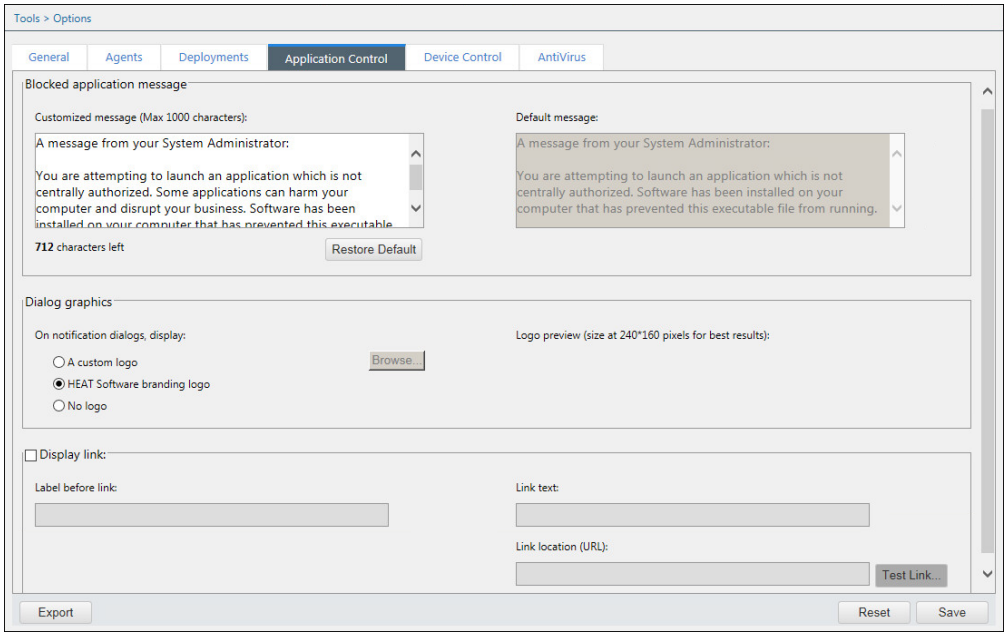
Customize the Blocked Notification dialog to explain to users why an executable was blocked and how to escalate a request to unblock it for business needs.

To Customize the Blocked Notification Dialog

1. From the Endpoint Security console, select **Tools > Options**.



2. Click the **Application Control** tab. On this tab you can do the following:
    - Add a customized message (up to 1,000 characters) to inform the user why an executable has been blocked and what steps they should take if they need to access the application.
    - Add your own company logo so that the user is aware that this is a message from your organization.
    - Add a URL to your help desk ticketing system or to a repository of approved software.



Blank Page

Blank Page

Enable Advanced Memory Protection

Application Control's Advanced Memory Protection feature protects against memory-based attacks, including buffer overflows and reflective memory injection (RMI). While RMI is generally associated with malware, some legitimate software vendors use RMI. For example, counterfeit deterrence system (CDS) software uses RMI with printers and scanners to prevent users from accessing or printing images of currency.

What is a Memory Protection Policy?

A Memory Protection policy detects and manages RMIs. The policy can operate in two modes:

- Enforcement mode shuts down the affected process once the RMI is detected.
- Audit mode logs the RMI without shutting down the process.

Use Audit Mode First

Apply a Memory Protection policy in audit mode to your initial group of endpoints. Review the logs over a few days to determine if any legitimate RMI is in use on your endpoints. Audit mode generates log events regardless if the RMI is malicious or legitimate.

If you see RMI detections immediately after applying the policy, determine whether the RMI is malicious or legitimate.

- If detection occurs only on a single endpoint or with a single file, the RMI is more likely to be malicious.
- If detection occurs on many endpoints and is easily reproducible, it is more likely that a process in your environment uses RMI legitimately.

For more information, see Knowledge Base Article #23389, Identifying Exceptions for Memory Injection Policies.

Manage Legitimate RMI Processes

If you encounter a legitimate RMI process, contact Support to confirm which application uses the RMI. Support can help you determine whether you can safely add the process as an exception to your Memory Protection policy.

When Ivanti identifies legitimate RMI processes, we add signatures for them to the Memory Protection module so that exceptions are no longer required. However, until signatures are available, you'll need to add legitimate processes as exceptions.

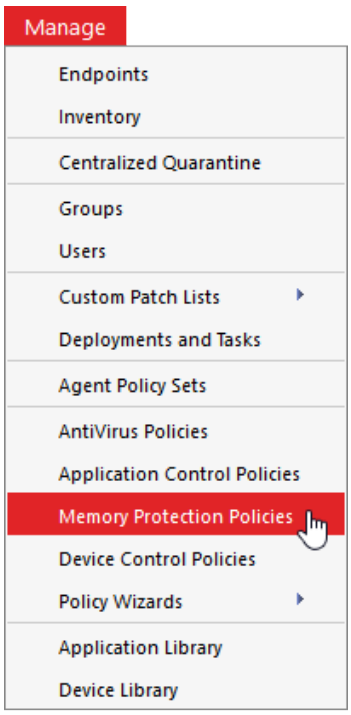
Extend Policy to Other Endpoints

Once you've added exceptions to your Memory Protection policy and the logs are showing no additional RMI events, extend the policy to additional endpoints in your environment. As with the initial endpoints, keep these additional endpoints in audit mode and review the logs for RMI events over a few days. When the logs show no additional RMI events, enforce the Memory Protection policy for all endpoints in your environment.

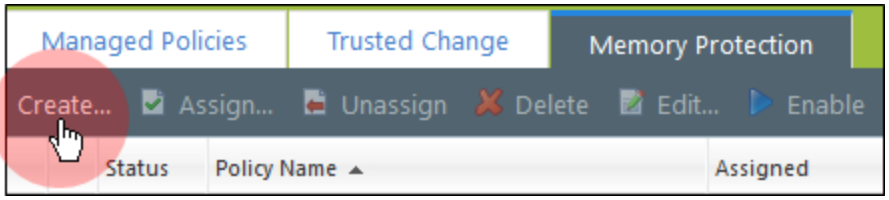
To Create a Memory Protection Policy

Use the Memory Injection Policy wizard to create a Memory Injection policy.

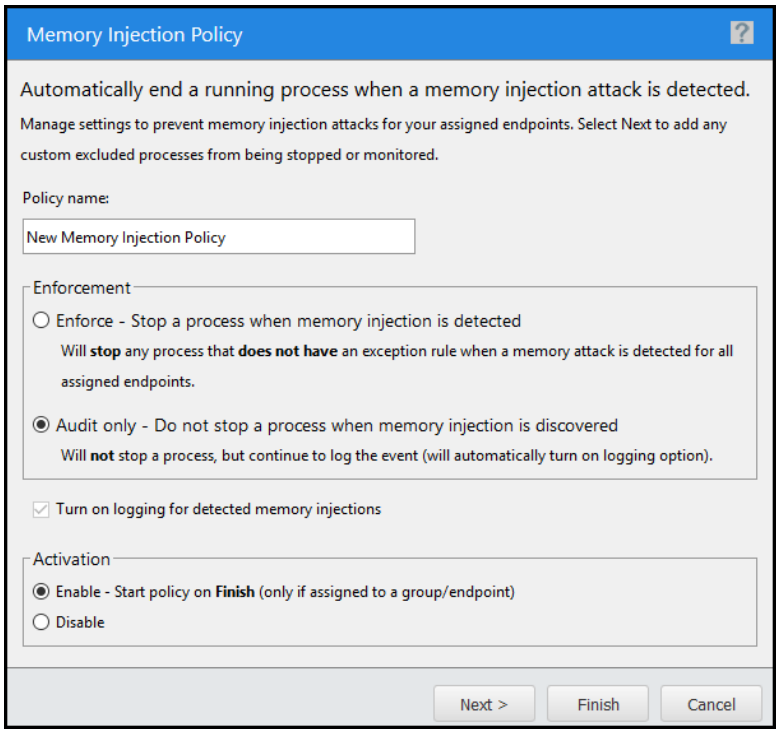
1. From the Endpoint Security console, select **Manage > Memory Protection Policies**.



2. On the **Memory Protection** tab, click **Create**.



The Memory Injection Policy wizard opens.



3. Complete the wizard. For detailed steps, see Creating a Memory Injection Policy in the Application Control User Guide.

Communicate with Users

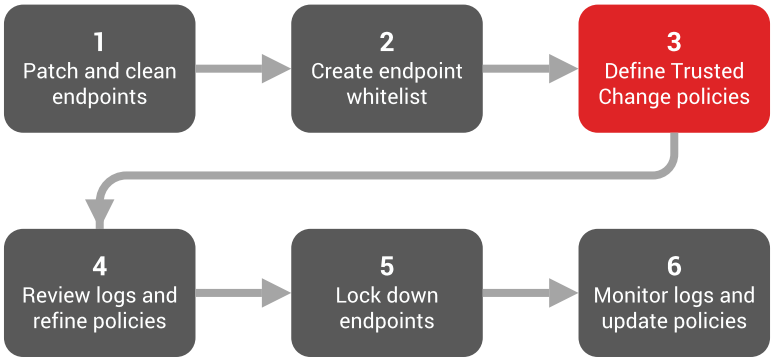
Continue communicating with users during Phase 2 to minimize the number of support calls you'll receive. Explain the following points:

- Users' endpoints will be scanned to build a list of the applications in use. Explain when the scans will occur and what users should expect during the scan.
- Blocked applications are no longer permitted. Users will receive a blocked dialog if they attempt to use the applications, and attempted usage of these applications will be logged. If users need access to these applications for business purposes, they should request access through the process you've set up. Provide users with a repository of approved software for download, if appropriate.
- Advanced Memory Protection is in use to block memory-based attacks. This might result in application processes being stopped automatically if memory injection is detected. For users, this could mean that applications or actions within those applications that worked previously may no longer work. Explain what users should do in this situation.

See Appendix 2 for sample end user communications.

Phase 3: Define Trusted Change Policies

Create policies that support Trusted Change on your endpoints. These policies automate whitelist maintenance and reduce the burden of managing software changes in your environment. Investing time into creating sufficient policies is key to successfully implementing Application Control.



In this phase you will:

- Review the applications in your environment and develop strategies for how to support change in the applications
- Refrain from placing endpoints into lockdown until after you have defined policies
- Define Trusted Change policies including Trusted Updater, Trusted Publisher, and Trusted Path policies
- Communicate with users so that you understand which applications they use and how to update them. See Appendix 2 for sample end user communications.

Develop a Change Management Strategy

You should develop a strategy for managing changes and updates to the applications in your environment, including determining which applications you will allow users to update themselves and which applications you will update centrally.

You can approach change management in two ways:

- Use the Easy Auditor logs, which tell you when changes have occurred on your endpoints. Then you can determine how to manage the change with policies.
- Identify applications that you know are going to change and put policies in place proactively.

In this phase we assume that you have already run the Easy Auditor scan, but you can also define policies prior to using Easy Auditor. Once the initial endpoints are scanned and you have created policies for them, you should apply these policies to additional endpoints *before* you scan them with Easy Auditor. Applying policies reduces the number of Easy Auditor log events that you need to review, since the **Easy Auditor: Applications Blocked When Enforcement is Enabled** log query only creates logs for executed files that are not on the whitelist or are not covered by a Trusted Change policy.

Don't Put Endpoints into Lockdown Just Yet

It's important that you create Trusted Change policies for your endpoints before putting your endpoints into lockdown. After creating your policies, spend *at least* one month monitoring the Application Event logs for any additional changes not already accounted for in the existing policies. This monitoring period should include at least one Patch Tuesday and, ideally, a major event like quarter-end. You need this time to validate that policies are working correctly because some applications may only make updates once per month or less frequently.

Bottom line: Resist putting endpoints into lockdown until you have policies in place to support changes in the endpoints' applications. Otherwise, when the applications update they will be blocked from executing, since the updated files are not on the endpoint whitelist.

Types of Trusted Change Policies

You can use the following Trusted Change policies to manage change in the applications in your environment. The following sections explain each policy in detail.

- **Trusted Updater**

  Trusted Updater allows you to install and automatically authorize software patches or new applications without additional overhead.

- **Trusted Publisher**

  Trusted Publisher automatically authorizes software installers, updates, and new applications to execute when they have been signed by trusted certificates.

- **Trusted Path**

  Trusted Path authorizes applications to run based on their location instead of adding them to a whitelist.

Trusted Updater

Trusted Updater allows you to install and automatically authorize software patches or new applications without additional overhead. By assigning trust to particular executables, any files added to the endpoint by those executables are automatically added to the whitelist for that endpoint. You should use Trusted Updater where possible to manage change in your applications.

Trusted Updater is the only trust mechanism that updates the endpoint whitelist directly. You should not use other trust mechanisms to install or update applications, as it can result in stability issues if the installations or updates change the driver files used in the boot sequence.

Where to Use Trusted Updater Policies

We recommend that you set up Trusted Updater policies for the following software categories:

- Software distribution tools or patch and remediation tools, including:
  - Windows Update
  - Ivanti Ivanti Patch and Remediation
  - Novell Zenworks
  - HP Radia
  - Microsoft System Center Configuration Manager (SCCM)
  - Altiris
  - Tivoli
  - Shavlik
- Third-party antivirus solutions, including:
  - Sophos
  - McAfee
  - Symantec
  - Kaspersky
  - Trend Micro
- Self-updating applications such as:
  - Adobe
  - Apple iTunes
  - Java
  - Mozilla Firefox

The following sections provide best practices for defining Trusted Updater policies for each of the above software categories.

Windows Update

Windows update is enabled on endpoints by default. However, to prevent instability issues on endpoints, Application Control blocks Windows Update from executing unless you add Windows Update as a Trusted Updater. If you're using Windows Update to update endpoints, create a Windows Update Trusted Updater policy before you put endpoints into lockdown.

For your convenience, we have created a Windows Update policy kit that contains a list of all the hashes of the updater files for Windows Update. Given the number of different updater files and versions, this kit greatly simplifies the task of creating a Windows Update Trusted Updater policy yourself. To import this policy kit to your Endpoint Security Server, please contact Support.

Software Distribution Tools or Patch and Remediation Tools

Ivanti Ivanti Patch and Remediation is a Trusted Updater by default, so no configuration on your part is required. If you are using other software distribution or patch and remediation tools, you should add the application executable to the Trusted Updater policy. You should also add any updater files for the application to the policy.

Third-party Antivirus Solutions

Antivirus solutions are updated every day with new signature files and occasionally with new engine files. To accommodate these changes, you need to create a Trusted Updater policy. However, you must add only the antivirus updater and *not* the antivirus scan engine to the policy. If you add the the scan engine to the Trusted Updater policy, every file that the scan engine accesses (i.e., every file that the user accesses) will inherit the trust settings. This has the same effect as turning off Application Control on the endpoint altogether.

Bottom line: Trust the antivirus updater only, not the scan engine.

Web Browsers

You should *not* add entire browser files (e.g., `iexplore.exe`, `firefox.exe`, etc.) to the Trusted Updater policy, as this has the same effect as trusting the entire Internet! Instead, you should add the browser *updater* to the Trusted Updater policy to support browser updates. You could add Firefox's updater `updater.exe`, for example.

Self-Updating Applications

Software applications are updated over time to address bugs, security issues and to add new features. Each application typically has one or more updater files it uses to perform updates. These updater files will execute because you'll have already added them to the whitelist during the Easy Auditor scan. However, the new files that the updater adds to the endpoint will not execute as they are not on the whitelist. For each of these updaters, decide whether to:

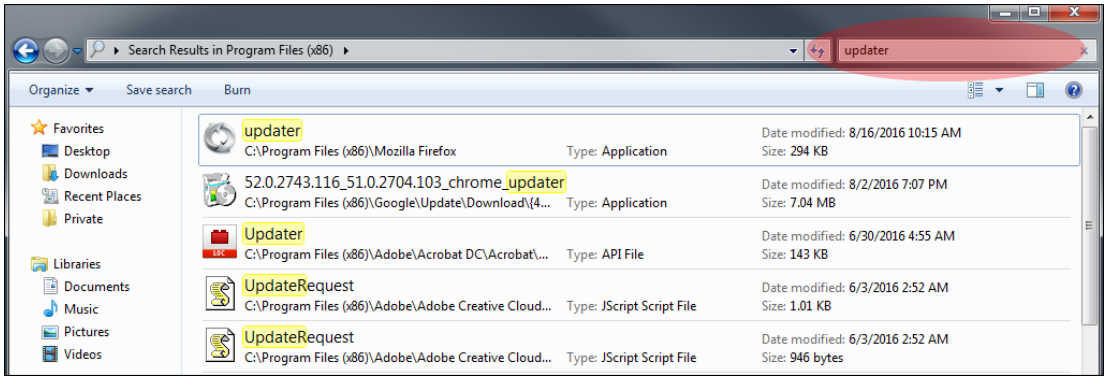
- Explicitly deny the updater in the environment
- Add the updater as a Trusted Updater

Identify Updater Files

A common challenge when creating a Trusted Updater policy for applications is identifying and locating the updater files. Use one or more of the following methods to help you identify updater files:

- Search for "update" or "updater" in C:\Program Files.

  Applications that update themselves have specific executables that perform the updates. The executable often has the word "update" in its name or in the name of the folder containing the executable.



- Refer to the vendor's documentation.

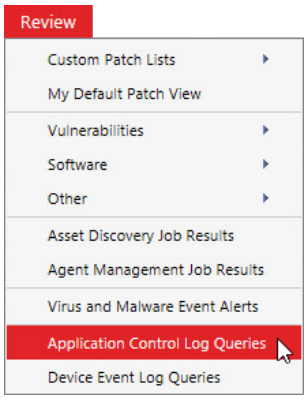
  Application vendors often provide information on the update mechanisms for their applications.

- Use the logs.

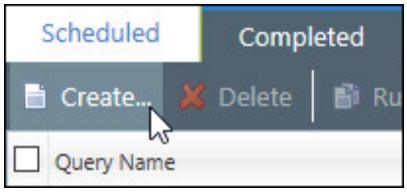
  Create a daily Application Event log query for **Easy Auditor: Applications Blocked When Enforcement is Enabled**. This query highlights any executables that would have been blocked if the endpoint had been in lockdown. The parent processes for these executables may be updaters. However, the parent process in the logs is the immediate preceding process and may not always be the actual updater process.

To Create the Applications Blocked When Enforcement is Enabled Query

1. From the Endpoint Security Console, select **Review** > **Application Control Log Queries**.



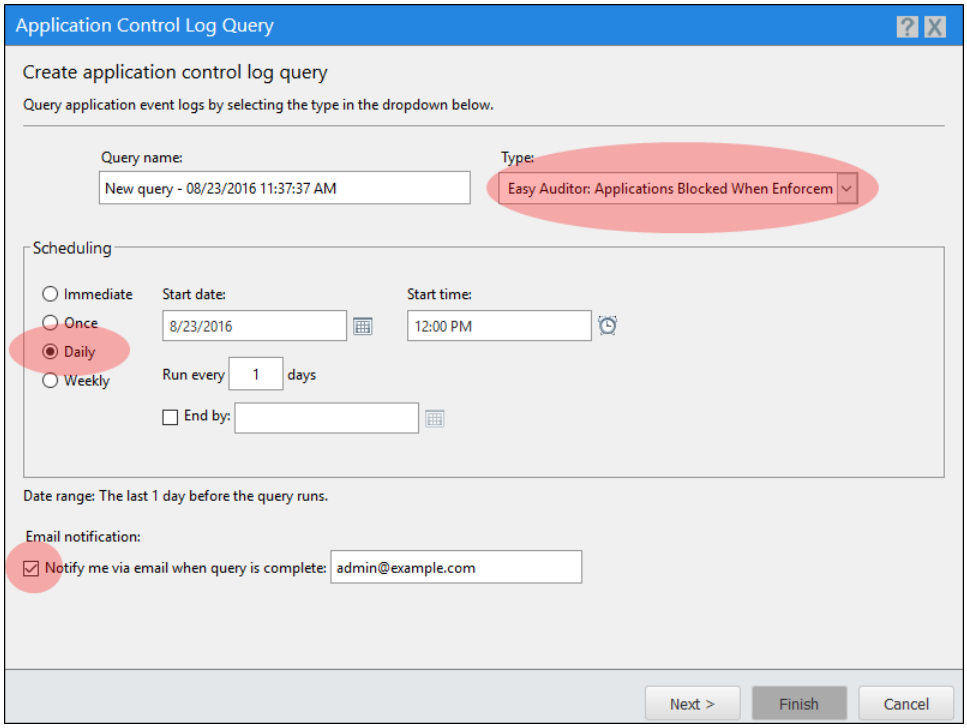
2. On the Application Control Log Queries page, click **Create**.



The Application Control Log Query wizard opens.

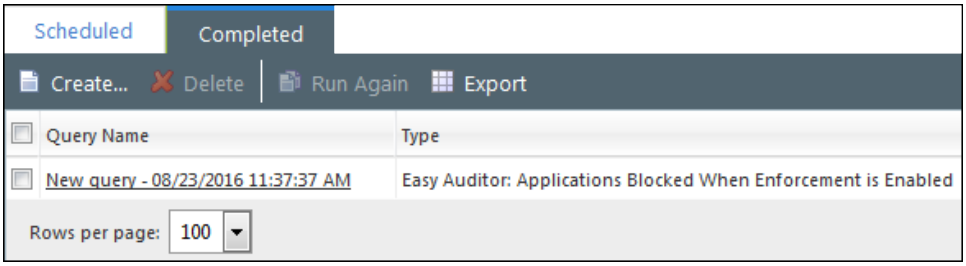
3. Complete the following in the wizard:
    a. Type a name for the new query in the **Query Name** field.
    b. Under **Type**, select **Easy Auditor: Applications Blocked When Enforcement is Enabled**.
    c. Under **Scheduling**, select **Daily**. Define a **Start date** and **Start time**.
    d. Select whether to have an email sent to you when the query is complete.

    We recommend you receive email notifications. These act as a daily reminder to review the logs and update the policies as needed. Make sure that you have already defined your email server within Endpoint Security. See Configuring Alert Settings in the Endpoint Security User Guide.



4. Click **Next** and add endpoints or groups of endpoints to the query.

5. Click **Finish** to create the query. After the query runs, view its summary and results on the **Completed** tab.



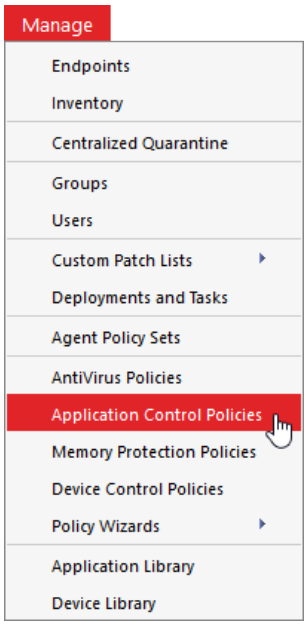
Having trouble determining the updater for an application? Contact Support for help.

Create a Trusted Updater Policy

You've identified the updater files across your endpoints. Now use the Trusted Updater wizard to create a new Trusted Updater policy and add the updater files to it.

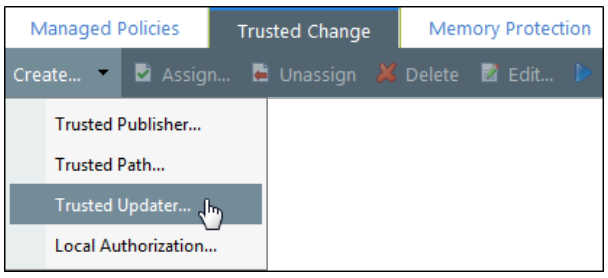
For the Trusted Policy to be effective, add all updater versions to the policy.

1. From the Endpoint Security Console, select **Manage > Application Control Policies**.

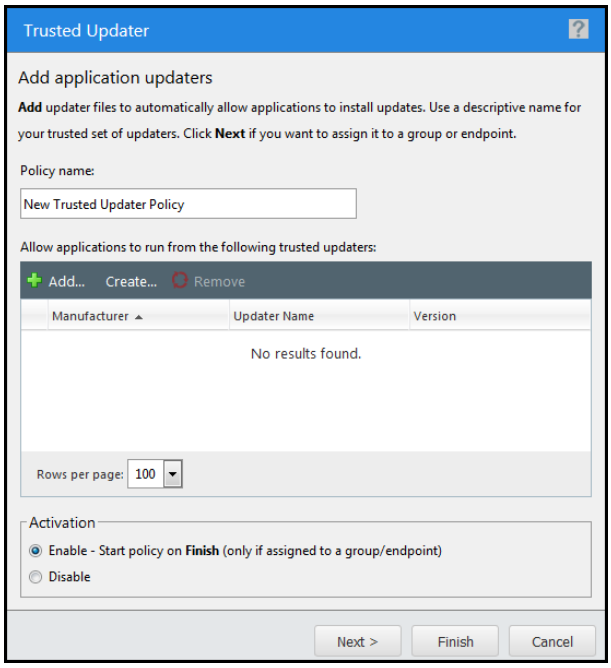


2. Click the **Trusted Change** tab.

3. Select **Create > Trusted Updater** to open the Trusted Updater wizard.



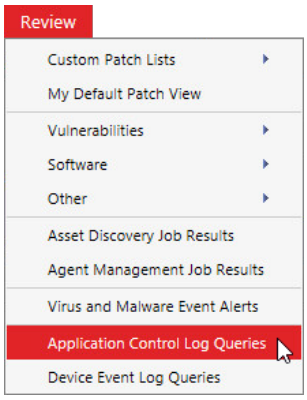
4. Complete the wizard. See Creating a Trusted Updater Policy in the Application Control User Guide for detailed steps.



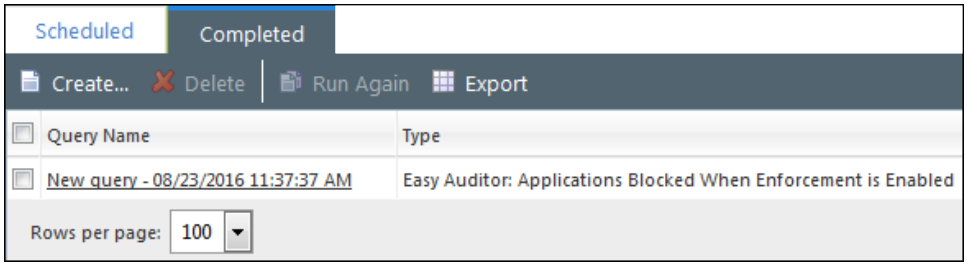
Add a Trusted Updater Directly from Logs

In addition to using the Trusted Updater wizard, you can add Trusted Updaters directly from the log queries. If an application updater file appears in the **Easy Auditor: Applications Blocked When Enforcement is Enabled** log query, you can either add the updater to an existing Trusted Updater policy or create a new policy.

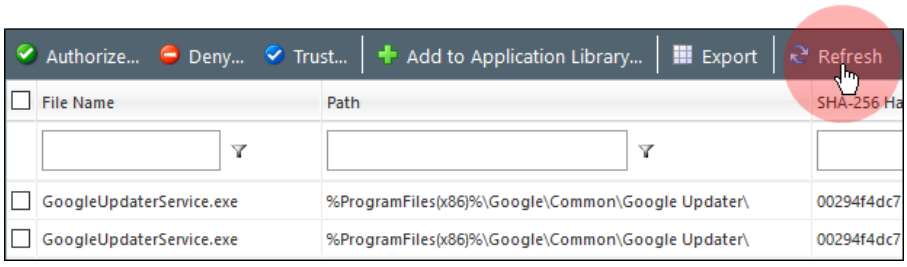
1. From the Endpoint Security Console, select **Review > Application Control Log Queries**.



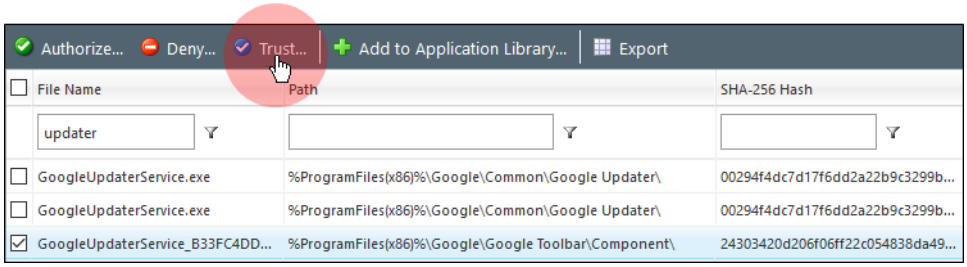
2. On the **Completed** tab, open the **Easy Auditor: Applications Blocked When Enforcement is Enabled** query that you previously created.



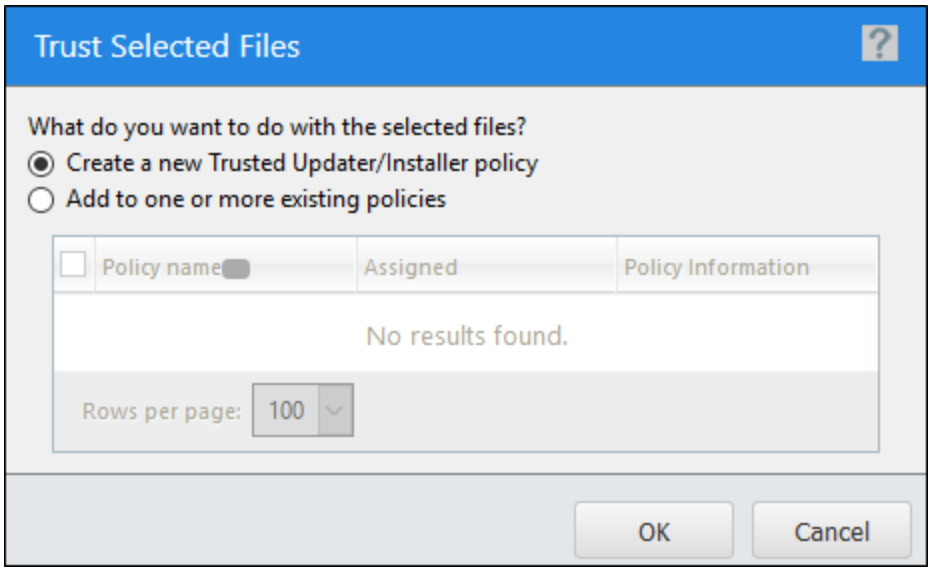
3. [Optional] There may have been activity on your endpoints since you initially created the query. To refresh the query and capture any new log entries, click **Refresh**.



4. Select the updater file you want to add as a Trusted Updater and click **Trust**.



The Trust Selected Files dialog appears.



5. Select whether to create a new Trusted Updater policy or add the file to an existing policy.

Understand and Manage Updater Behavior

Common Updater Behavior

Applications receive updates differently; there is no standard update mechanism across all applications. The most common update method uses updater files, which you should add to the Trusted Updater policy. However, over time vendors may change the method they use to update applications. If this happens, the updated version of the application may be blocked. Resolve this by:

- Identifying the new updater and adding it to the Trusted Updater policy
- Authorizing the new version of the application for any affected users

Unsecured Updaters

Some updating mechanisms are inherently insecure from an application control perspective. For example, sometimes the application itself, such as a web browser, detects that a new version of the application is available and downloads the installer automatically. In this scenario:

- There are no specific updater files to add to the Trusted Updater Policy. Adding the primary application executable instead would be very insecure (recall from earlier in this section that you should not trust browser executables).
- The installer uninstalls the old version of the application and installs the new version.
- The new version is not on the endpoint whitelist and therefore does not execute.

How do you manage this scenario? Add the new version of the installer to the Trusted Updater policy. Then you can reinstall the new application version on any affected endpoints.

Installers as Trusted Updaters

When an installer is a Trusted Updater, any file installed on the endpoint by that installer is automatically whitelisted. If you plan to refer users to a repository of approved software, scan the repostory location and add all of its application installers to a Trusted Updater Policy. Users can then download the installers and install the approved software on their endpoints as needed.

Best Practice Recommendations

- Take time to understand updater behavior while endpoints are in Easy Auditor.
- If you can't create a Trusted Updater policy for an application, consider an alternate trust mechanism such as Trusted Publisher.
- Alternatively, disable automatic updates for the application and use a test endpoint in automatic update mode to obtain the new updater or installer. Then add the new updater or installer to the Trusted Updater policy and roll out the updated version.

Trusted Publisher

Trusted Publisher automatically authorizes software installers, updates, and new applications to execute when they have been signed by trusted certificates. The software executes when the user executes it, with no action needed from you.

When a Trusted Publisher policy is assigned, any application may run as long as the initial executable is signed with a certificate in the policy. The policy doesn't update the endpoint whitelist.

- Since Trusted Publisher doesn't update the endpoint whitelist, only use it to install applications that don't modify core system files or Dynamic Link Libraries (DLLs) that are shared with other applications. If the installation causes system files or DLLs to update, the applications sharing those files may no longer execute. This problem could occur, for example, if the whitelisted files get replaced by unsigned DLLs.
- Trusted Updater should be your default policy for installing and updating applications. Only use Trusted Publisher when you can't use a Trusted Updater policy for a specific application.

When to Use Trusted Publisher

We recommend using Trusted Publisher to authorize the following software:

- Cloud-distributed applications that do not reside on the disk until they are executed, such as WebEx and GoToMeeting. These are signed ActiveX controls that are downloaded into a browser
- Browser plugins, which generally do not have updater tools
- In-house signed custom applications

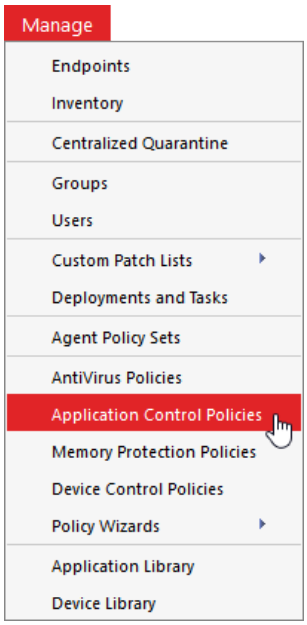
The file that is authorized to execute is allowed to load all dependent processes; they don't need to be signed. Only the initial executable must be signed.

Be Aware of Multiple Certificates

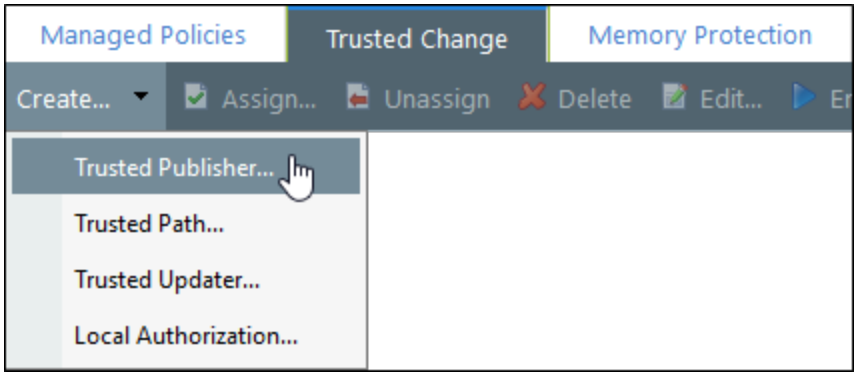
Most software vendors have multiple certificates, but not all certificates for the same vendor are authorized. Only the specific certificates in the Trusted Publisher policy are authorized. If an executable that you expect to be authorized is blocked, check to see if the certificate matches the certificate in the policy. If the certificates are different, add the missing certificate to the policy.

To Create A Trusted Publisher Policy

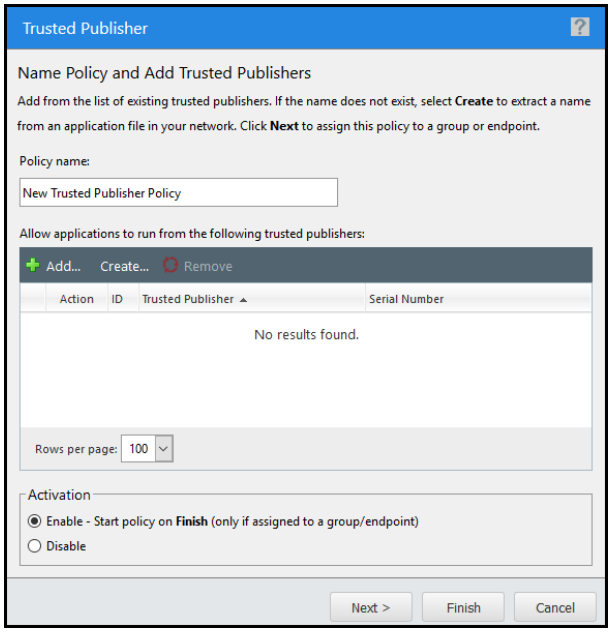
1. From the Endpoint Security Console, select **Manage > Application Control Policies**.



2. Click the **Trusted Change** tab.
3. Select **Create > Trusted Publisher** to open the Trusted Publisher wizard.



4. Progress through the wizard. See Creating a Trusted Publisher Policy in the Application Control User Guide for detailed steps.



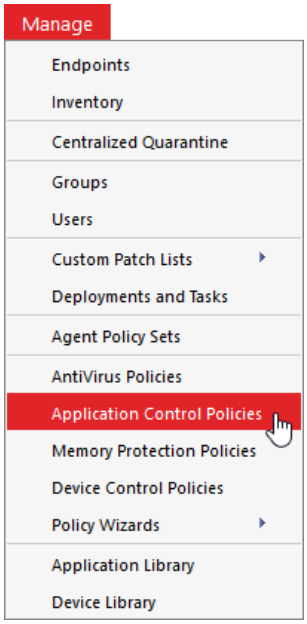
Trusted Path

Trusted Path authorizes applications to run based on their location instead of adding them to a whitelist. Trusted Path allows an application to execute if it is stored in one of the paths specified in the policy. We recommend you consider using Trusted Path for:

- Unsigned executables that change frequently, where every installation of the application is unique
- Shared Network Paths, such as build output locations for in-house software development

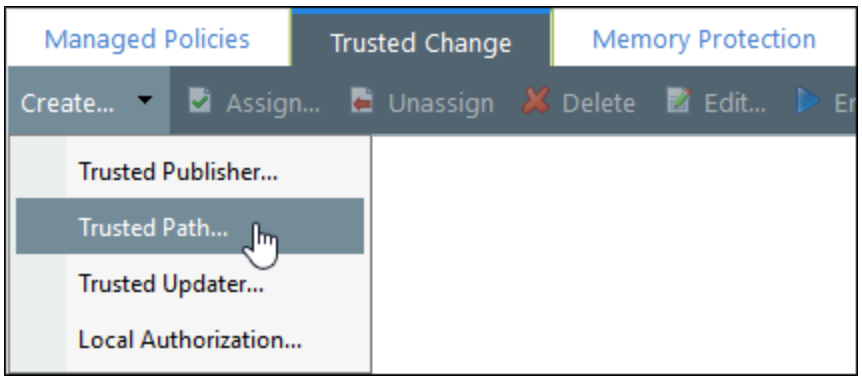
To Create a Trusted Path Policy

1. From the Endpoint Security Console, select **Manage > Application Control Policies**.

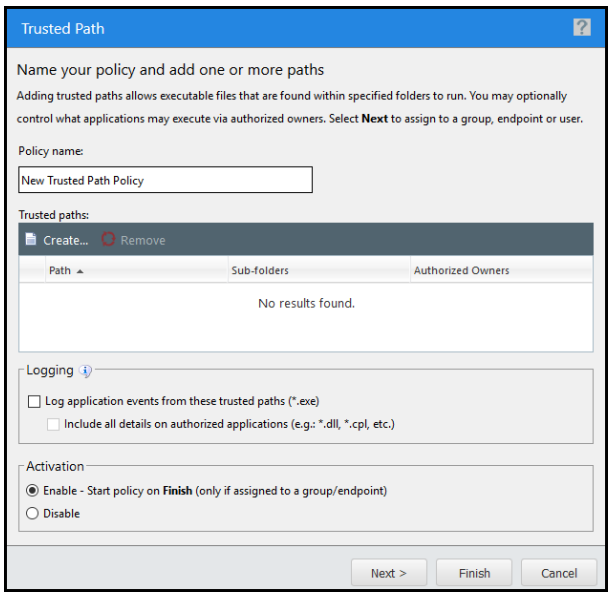


2. Click the **Trusted Change** tab.

3. Select **Create > Trusted Path** to open the Trusted Path wizard.



4. Progress through the wizard. See Creating a Trusted Updater Policy in the Application Control User Guide for detailed steps.

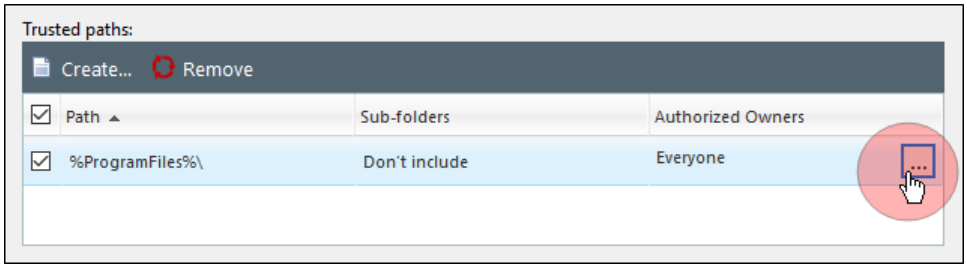


Set Ownership Restrictions

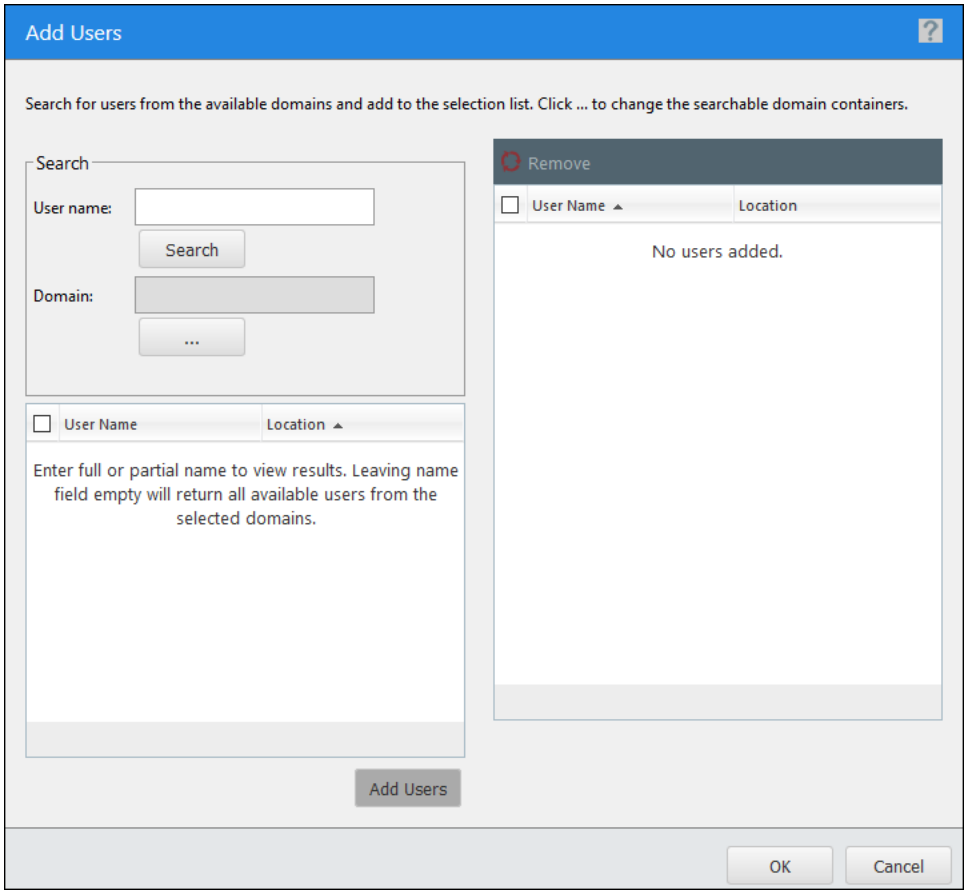
While allowing applications to execute based on their location may not seem like a particularly secure solution, you can set ownership restrictions by specifying an Authorized Owner. This restriction allows a file to execute in the Trusted Path only if the owner matches the Authorized Owner that you specified in the Trusted Path policy.

You can add one or more Authorized Owners while you're in the Trusted Path wizard, using the Add Users dialog.

1. In the Trusted Path wizard, click on the **Authorized Owners** ellipses (...) button next to the Trusted Path you created.



The Add Users dialog opens.



2. Search for users that you want to set as Authorized Owners and add them to the selection list. See Adding an Authorized Owner to a Trusted Path in the Application Control User Guide for details.

Communicate with Users

Endpoints are still in Easy Auditor, so users may continue to use all their applications, even if you haven't yet implemented Trusted Change policies for them. Exceptions are applications that you've explicitly denied or applications that are terminated due to a memory injection detection.

Communicate with users to:

- Know which applications users need
- Understand how the applications are updated
- Decide how to manage the applications

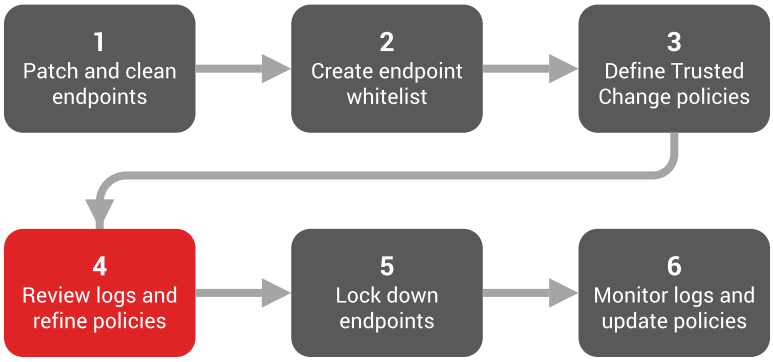
Depending on your reasons for introducing Application Control, you may decide to select specific applications or application versions to limit the number of applications you support. In this case, provide users with a list of corporate applications or application versions and explain where users can obtain them.

If users need applications or versions of applications outside of the approved list, explain how users can request approval (such as submitting a ticket to a helpdesk).

See Appendix 2 for sample end user communications.

Phase 4: Review Logs and Refine Policies

After you have completed Easy Auditor scans on your test endpoints and developed initial policies, monitor the Application Event logs daily to identify any missing policies or policies that need to be updated.



In this phase you will:

- Create scheduled Application Event log queries
- Review Easy Auditor logs daily and create or adjust Trusted Change policies to accommodate changes
- Manage re-appearing entries by authorizing files directly or re-running Easy Auditor to "reset" logs, if necessary
- Review Memory Injection Detection events logs daily and add exceptions to the Memory Protection Policy, if required
- Identify and eliminate potential Trust Leaks
- Optionally, apply Local Authorization policy to users in Easy Auditor once the logs are stabilized
- Maintain a test endpoint so that new software can be scanned and added to the Application Library
- Increase the number of endpoints in Easy Auditor and adjust your policies to accommodate the new endpoints
- Communicate with users to prepare them for lockdown and to ensure that they understand how to obtain approval for blocked applications. See Appendix 2 for sample end user communications.

The goal in this phase is to prepare endpoints for lockdown. Endpoints create log events when actions occur on the endpoint for which an Application Control policy does not yet exist. When log event entries appear in daily log queries, it means that there are policies you still need to create to manage the actions occurring on the endpoints. The endpoints are not ready for lockdown until you've created all the necessary policies.

This phase continues until the logs are stable with no unexpected entries. Recall that the stabilization period should:

- Last for at least one month
- Incorporate at least one Patch Tuesday
- Incorporate at least significant corporate event, such as quarter-end

At the end of this phase you'll be ready to move your endpoints into lockdown.

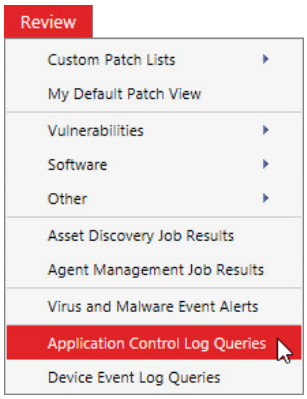
Create Scheduled Application Event Log Queries

Use the **Easy Auditor: Applications Blocked when Enforcement is Enabled** log query to identify when and how changes take place on endpoints. Log entries appear when executables are run that are not on the whitelist or are not covered by a Trusted Change policy.

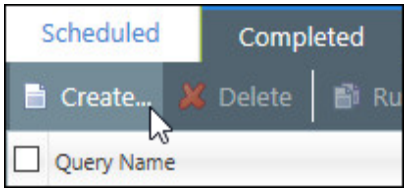
Remember: Don't put endpoints into lockdown just yet. If the endpoint is locked down, executables that are not on the whitelist or are not covered by a Trusted Change policy are blocked from executing, which creates gaps in log entries. It's important that you create or update policies before putting endpoints into lockdown.

To Create the Applications Blocked When Enforcement is Enabled Query

1. From the Endpoint Security Console, select **Review** > **Application Control Log Queries**.



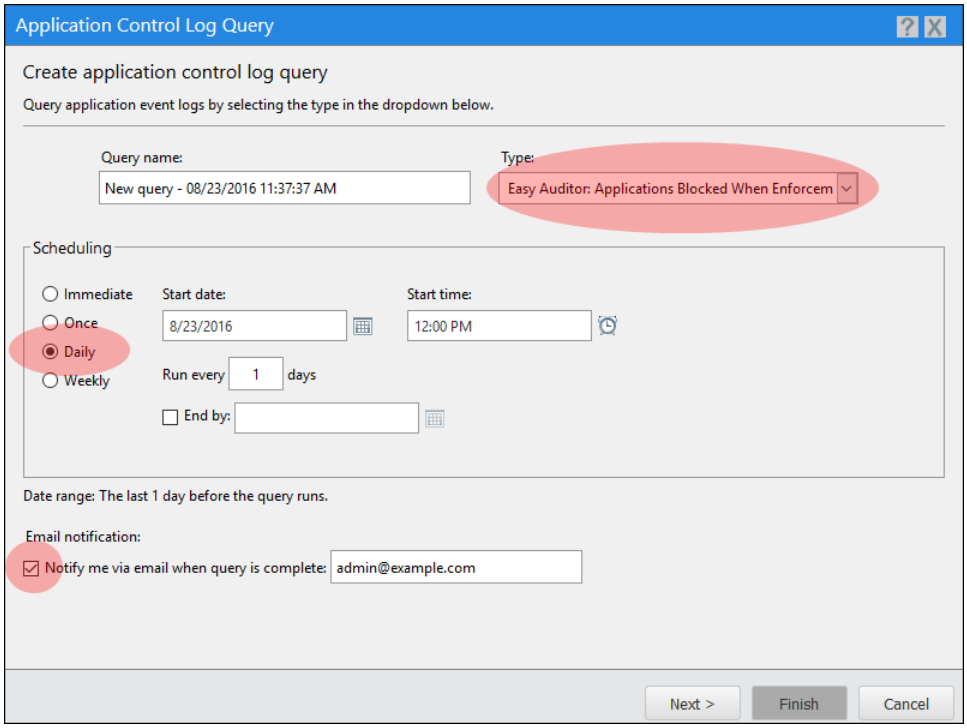
2. On the Application Control Log Queries page, click **Create**.



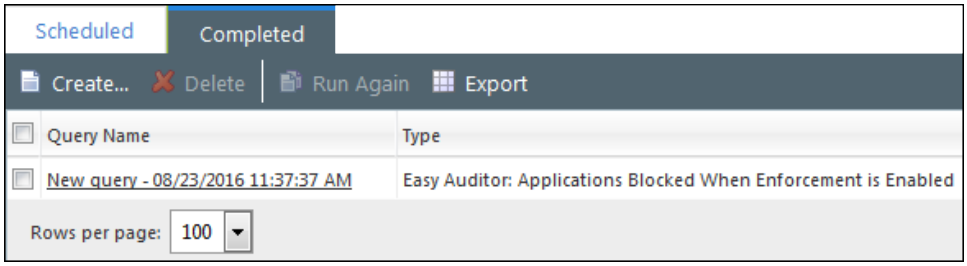
The Application Control Log Query wizard opens.

3. Complete the following in the wizard:
    a. Type a name for the new query in the **Query Name** field.
    b. Under **Type**, select **Easy Auditor: Applications Blocked When Enforcement is Enabled**.
    c. Under **Scheduling**, select **Daily**. Define a **Start date** and **Start time**.
    d. Select whether to have an email sent to you when the query is complete.

    We recommend you receive email notifications. These act as a daily reminder to review the logs and update the policies as needed. Make sure that you have already defined your email server within Endpoint Security. See Configuring Alert Settings in the Endpoint Security User Guide.



4. Click **Next** and add endpoints or groups of endpoints to the query.
5. Click **Finish** to create the query. After the query runs, view its summary and results on the **Completed** tab.



Review Easy Auditor Logs Daily

During the initial monitoring period, check the Easy Auditor: Applications Blocked When Enforcement is Enabled logs daily. Avoid skipping days as the logs rapidly build up and become a challenge to maintain.

After the initial week or two have passed and the number of new log entries starts to dwindle, begin to roll Easy Auditor out to an increased number of endpoints and/or reduce the frequency of the query to once or twice per week.

When Endpoint Security generates log query email notifications, the text "No Results Found" appears in the subject field if there are no results associated with that query. Use your email filtering rules to delete these emails automatically so that you only receive emails when the log query contains results.

Manage Entries in the Easy Auditor Logs

Recall that when log event entries appear in the Easy Auditor logs, it means that a file executed on an endpoint, but the file:

- Was not authorized by Application Control
- Would have been blocked if the endpoint were in lockdown

Since the endpoint was scanned in Easy Auditor to create the endpoint whitelist, the appearance of these log entries means that an unplanned change occurred on the endpoint. These unplanned changes can occur due to one of the following:

- The endpoint user downloaded an application from the Internet and attempted to execute it.
- A malicious file was downloaded to the endpoint and attempted to execute.
- An installed application was updated to a more recent version and there was no Trusted Change policy in place to support the update.

Because the endpoint is in audit mode, the user is allowed to execute files. Since the endpoint will be rescanned before going into lockdown, these specific files will not be blocked when the endpoint is locked down. However, unplanned changes may take place on the endpoint again once it is locked down. Depending on the type of change, it could result in productivity issues or support calls.

When unexpected log entries appear, examine them and determine what action to take to prevent a problem occurring later.

- Is the file/application one that you explicitly did not want to allow to execute and should be blocked? Add it to a Denied Applications Policy.

- Is the log event associated with an application that was already on the endpoint during Easy Auditor? If so, the application was either patched or updated to a later version. You need to understand how this change occurred and create a policy to support this type of change when it re-occurs.
    - Rather than just authorizing these files, identify the file that performed the update. Typically this file is the first entry associated with the application in the logs.
    - Trust the updater by adding it to a Trusted Updater policy or create a new Trusted Updater policy.

Create or Update Policies Directly from Logs

You can authorize, deny, or trust files directly from Application Control Log Queries. This is a convenient way to manage any unexpected log entries. See Authorizing, Denying, and Trusting Files from Logs in the Application Control User Guide for detailed steps.

Manage Re-Appearing Entries

A log entry may continue to appear even after you have created a policy to manage the scenario. This could happen because an application is updated and the new version is not on the whitelist. Here are some options to manage this:

- You can create a Trusted Updater policy for this application, which adds files to the whitelist the next time the application is updated. However, each time the current version is executed it will still result in log entries.
- If only a few log entries appear, authorize the files directly from the log query. With this method, you avoid having to scan the entire endpoint again.

  See Authorizing Files from Logs in the Application Control User Guide for detailed steps.
- If many log entries appear, unassign the Easy Auditor policy for that endpoint. The policy remains in the system as an unassigned policy. You then reassign the Easy Auditor policy to the endpoint, which allows the Easy Auditor scan to re-run and "reset" the logs by adding these new files to the endpoint whitelist.

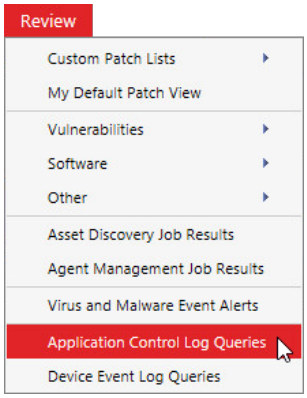
  See Unassigning an Easy Auditor Policy in the Application Control User Guide for detailed steps.

Create a Memory Injection Detection Events Log Query

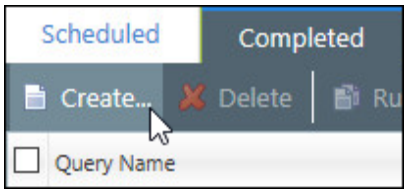
Create a daily **All Memory Injection Detection Events** log query so that you can see if reflective memory injection (RMI) events are occurring on your endpoints. Such events could indicate malicious activity or could be a result of legitimate application behavior. In either case, the log query acts as the trigger to investigate RMI activity.

To Create the Memory Injection Detection Events Log Query

1. From the Endpoint Security Console, select **Review** > **Application Control Log Queries**.



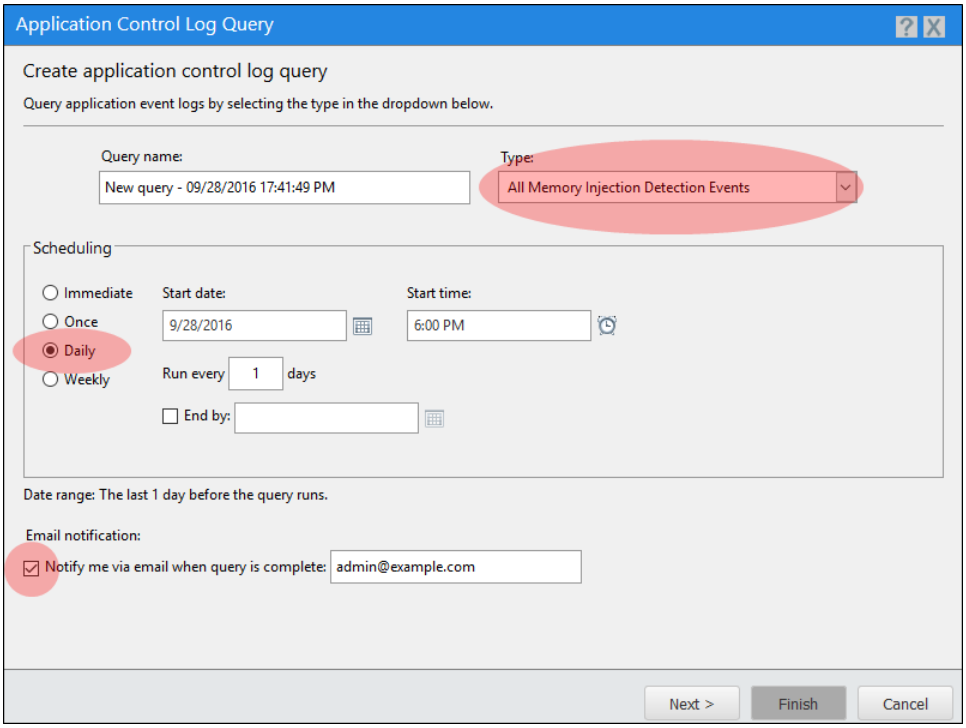
2. On the Application Control Log Queries page, click **Create**.



The Application Control Log Query wizard opens.

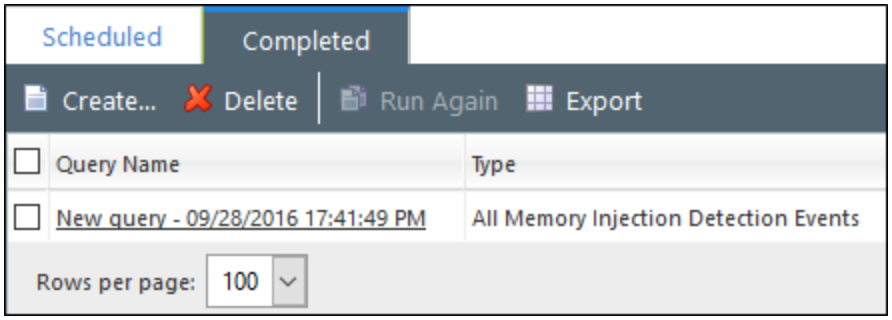
3. Complete the following in the wizard:
    a. Type a name for the new query in the **Query Name** field.
    b. Under **Type**, select **All Memory Injection Detection Events**.
    c. Under **Scheduling**, select **Daily**. Define a **Start date** and **Start time**.
    d. Select whether to have an email sent to you when the query is complete.

    We recommend you receive email notifications. These act as a daily reminder to review the logs and update the policies as needed. Make sure that you have already defined your email server within Endpoint Security. See Configuring Alert Settings in the Endpoint Security User Guide.



4. Click **Next** and add endpoints or groups of endpoints to the query.

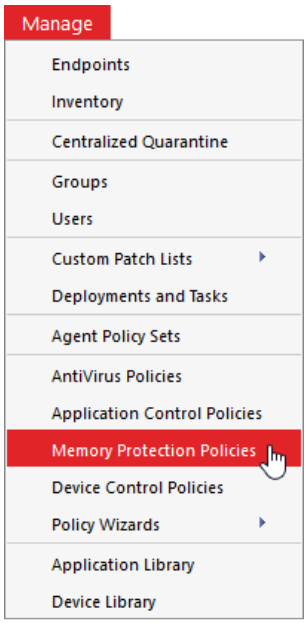
5. Click **Finish** to create the query. After the query runs, view its summary and results on the **Completed** tab.



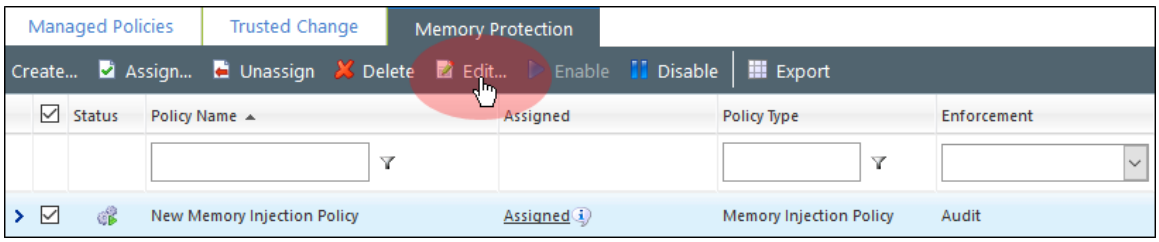
Add Exceptions for Legitimate RMI Processes

If RMI events are associated with legitimate software behavior, add exceptions to the Memory Protection policy you created in Phase 2 to prevent these applications from being terminated when enforcement is enabled.

1. From the Endpoint Security console, select **Manage > Memory Protection Policies**.



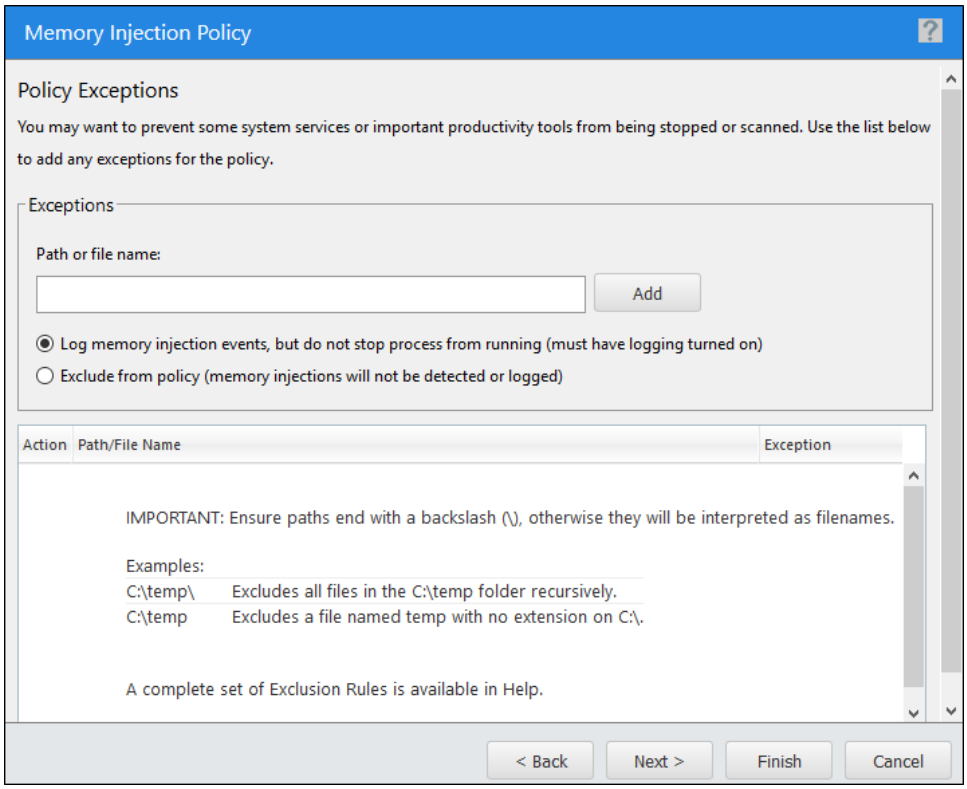
2. On the **Memory Protection** tab, select the Memory Injection policy you created and click **Edit**.



The Memory Injection Policy wizard opens.

3. Click **Next**.

The Policy Exceptions page displays.



4. Enter the path or file name.
5. Select whether to **Log memory injection events, but do not stop the process from running** or **Exclude from policy**.
6. Click **Add**.
7. Repeat steps 4 through 6 to add all required paths or files as needed.
8. Click **Finish**.

Identify Trust Leaks

A Trust Leak occurs when files are added to the whitelist unintentionally. Trust Leaks typically occur if you add a file that's not an application updater to a Trusted Updater policy. For example, if you add the antivirus engine as a Trusted Updater, files that are scanned for malware could actually get added to the whitelist.

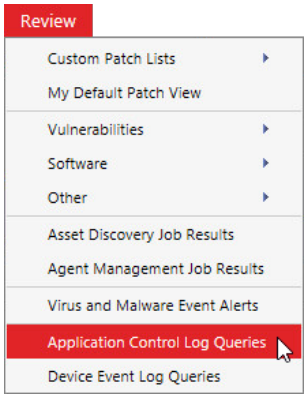
While you should take care to identify updaters correctly, you can also use the **All Applications Added by Trusted Updaters** log query to identify potential trust leaks. This query lists the applications on the whitelist that are allowed to execute because of a Trusted Updater policy. Run this query for a small number of test endpoints (about five). You may have a trust leak if you see multiple, unexpected files on your whitelist. Modify your Trusted Updater policies to eliminate this leak before applying these policies to more endpoints.

If you extend the Application Control rollout to many endpoints without first eliminating trust leaks, it could result in:

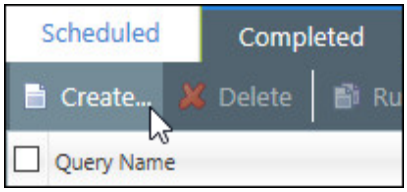
- Compromised security
- A high volume of logs that consume space and resources

To Create the All Applications Added by Trusted Updaters Query

1. From the Endpoint Security Console, select **Review** > **Application Control Log Queries**.



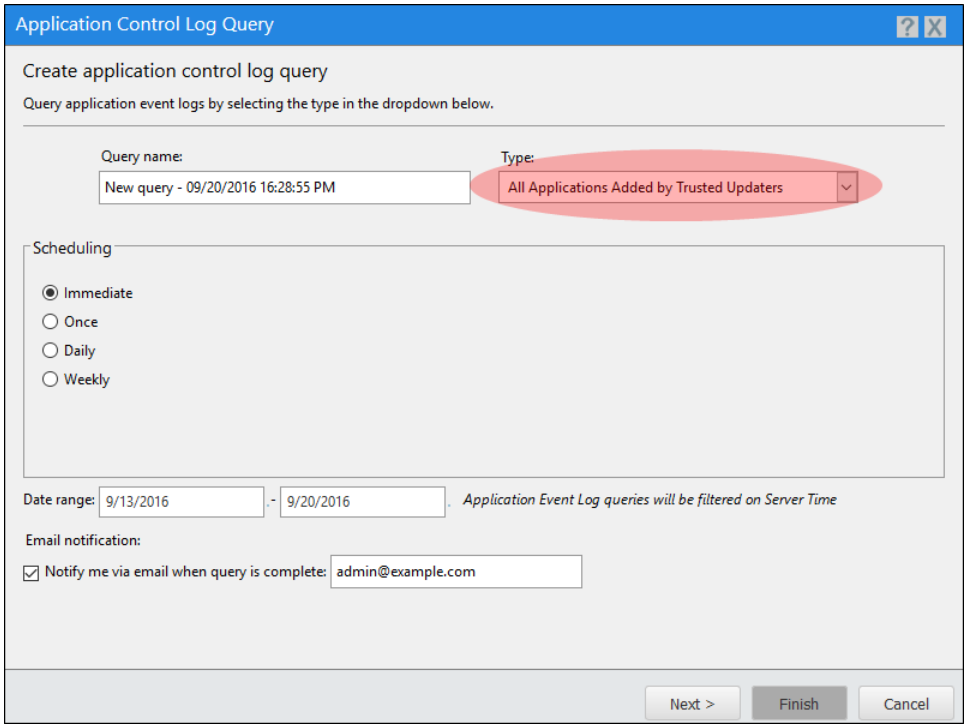
2. On the Application Control Log Queries page, click **Create**.



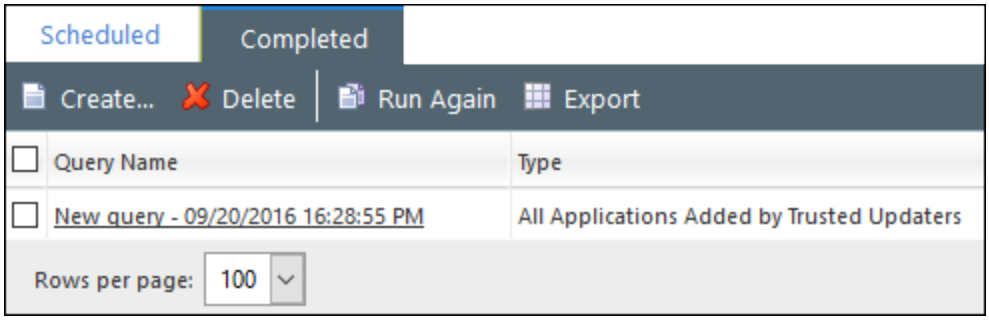
The Application Control Log Query wizard opens.

3. Complete the following in the wizard:
    a. Type a name for the new query in the **Query Name** field.
    b. Under **Type**, select **All Applications Added by Trusted Updaters**.
    c. Select a **Scheduling** option.
    d. Select whether to have an email sent to you when the query is complete.

    Make sure that you have already defined your email server within Endpoint Security. See Configuring Alert Settings in the Endpoint Security User Guide.



4. Click **Next** and add endpoints or groups of endpoints to the query.
5. Click **Finish** to create the query. After the query runs, view its summary and results on the **Completed** tab.



Apply a Local Authorization Policy, if Needed

Prior to locking down endpoints, you can apply a Local Authorization policy that asks the endpoint user to authorize any executables that are not on the whitelist or are not authorized by another Trust policy.

Why Use Local Authorization?

Using Local Authorization on your endpoints provides a number of benefits:

- **Communication**. Allowing your users to authorize executables helps users understand that this is a transition stage before a full blocking mode. Prior to this point (in Easy Auditor), users are unaware of the impact of installing and updating software themselves.

  Notify users that they are entering this new phase of Application Control so that they know what to expect: productivity will not be affected but applications are now being controlled.

- **Monitoring**. You can still monitor any executables that are locally authorized by users, and you have the option to add these executables to a Denied Applications policy if you do not want these applications to be used in your environment. Alternatively, you can add the executables to a Supplemental Easy Lockdown/Auditor policy if you do want these executables to be available to some or all users.
- **Preparation**. Using Local Authorization on endpoints in Easy Auditor assures that these endpoints are fully ready to be locked down. It's difficult to move to endpoint lockdown if you are concerned that applications will be blocked across a range of endpoints, resulting in many support requests and lost productivity. Minimize this concern by using Local Authorization to provide your users with the ability to authorize applications that would have been blocked otherwise.
- **Testing**. You can also use Local Authorization on test endpoints to identify any executables that would have been blocked if the endpoints were in lockdown.
  - When you receive a Local Authorization prompt on these endpoints, you can immediately update the policies to account for this situation rather than having to wait for the daily or weekly Application Event log query email notification.
  - Occasionally, when you review the Application Event log queries, it's difficult to determine from the blocked executable which application is actually being blocked and what policy needs to be created or updated to address it. Local Authorization helps you identify the associated application quickly and prompts you to update your policies.
- **Malware control**. Local Authorization controls malware spreading throughout your environment. As each user is asked to authorize any new executable on their endpoint, the spread of malware is limited by the number of users who authorize the new executable.

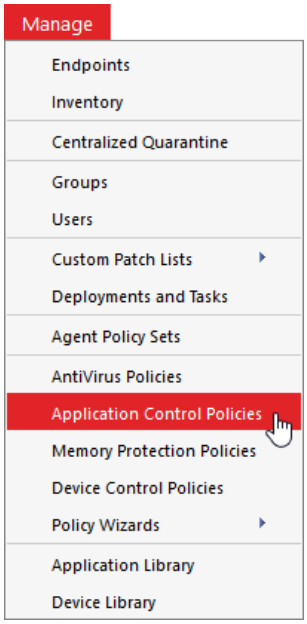
Before Using Local Authorization

Prior to applying Local Authorization in Easy Auditor, you should un-assign and reassign the Easy Auditor policy so that any system files that were modified while in Easy Auditor are now added to the whitelist. Otherwise, these files could cause problems at boot-up before the user can respond to local authorization prompts. Ensure that you've implemented the necessary policies to account for the modification of these system files in the future.

Do not apply a Local Authorization policy to an endpoint that has Windows Update enabled but doesn't have a Windows Update Trusted Updater policy. Authorizing Windows Updates locally could result in boot-up issues.

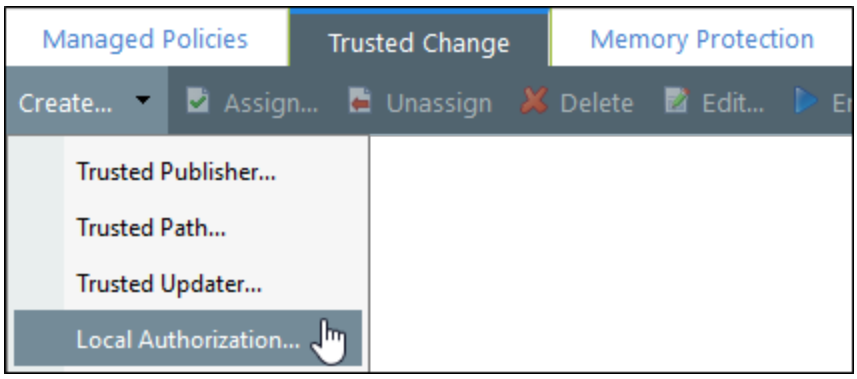
To Create a Local Authorization Policy

1. From the Endpoint Security Console, select **Manage > Application Control Policies**.

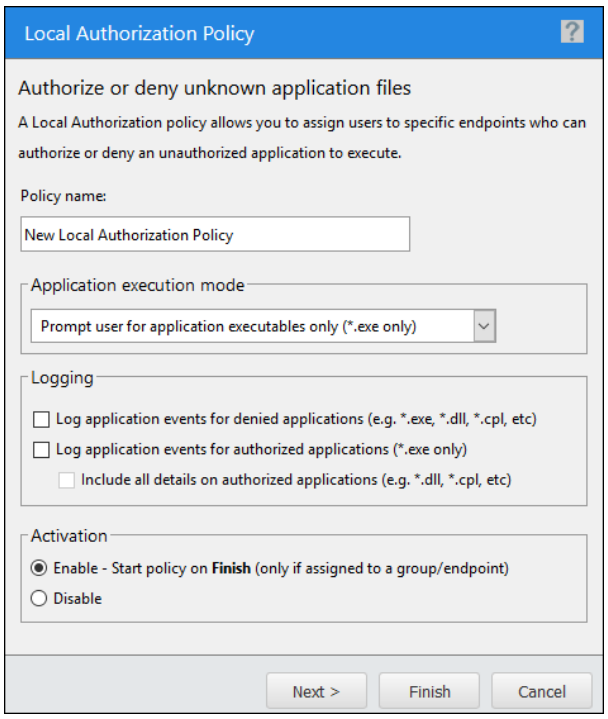


2. Click the **Trusted Change** tab.

3. Select **Create > Local Authorization** to open the Local Authorization Policy wizard.



4. Progress through the wizard. See Creating a Local Authorization Policy in the Application Control User Guide for detailed steps.



Blank Page

Best Practices with Local Authorization

The following explains how to help users make good authorization decisions, how to adjust logging, and why it's important to maintain a test endpoint when using Local Authorization.

Review Logs when Using Local Authorization

Once you've applied a Local Authorization policy to an endpoint, you'll no longer see any entries in the **Easy Auditor: Applications Blocked When Enforcement is Enabled** Application Event log query. This is because all "blocked" executables are now presented to the endpoint user for Local Authorization. Going forward, log entries appear in the **All Applications Executed by Local Authorization** query.

We recommend that you replace your daily/weekly scheduled application event log query with the Local Authorization log query so that you keep receiving email reminders to review the logs and update the policies. Endpoint users may authorize unwanted applications using Local Authorization. Review the logs for these applications and update your Denied Applications policies as needed.

Maintain a Test Endpoint

Executables must be in the Application Library to authorize or deny them. If the executables are not already in the Application Library, maintain a test endpoint that you can add these applications to. As you review the executables that endpoint users authorize or deny via Local Authorization, you may choose to authorize or deny these executables for all users. Maintaining a test endpoint helps facilitate this process.

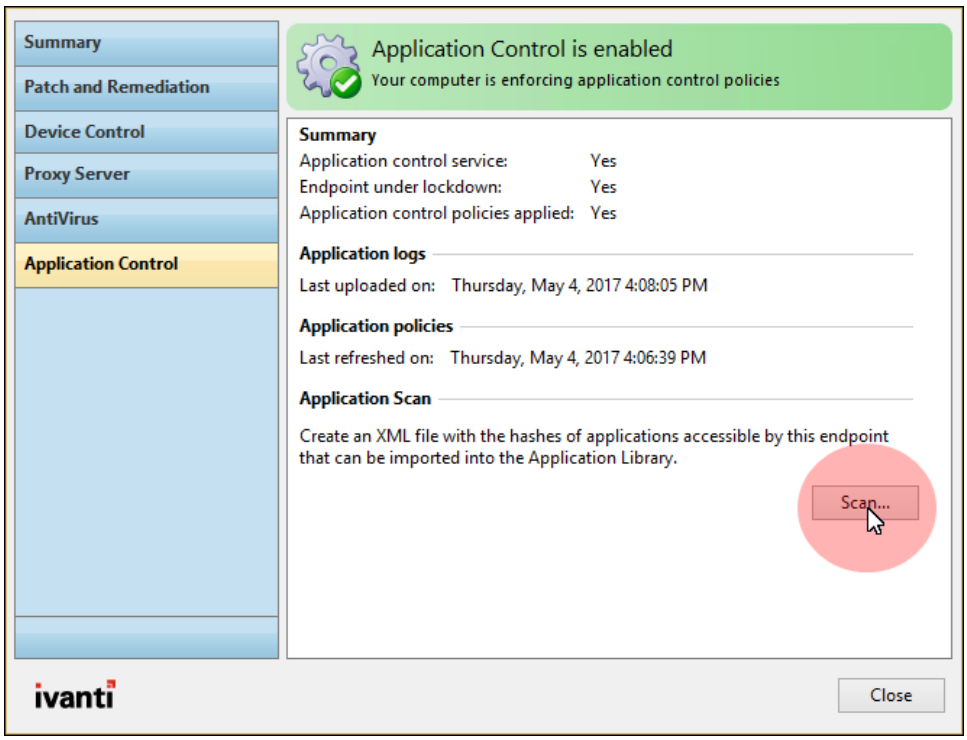
You can either:

- Scan the test endpoint with Easy Auditor to add the applications to the Application Library
- Recommended: Scan the specific installer, executable file, or folder of an application using Application Scan on a target endpoint. Import the results to the Application Library and authorize or deny the files from there.

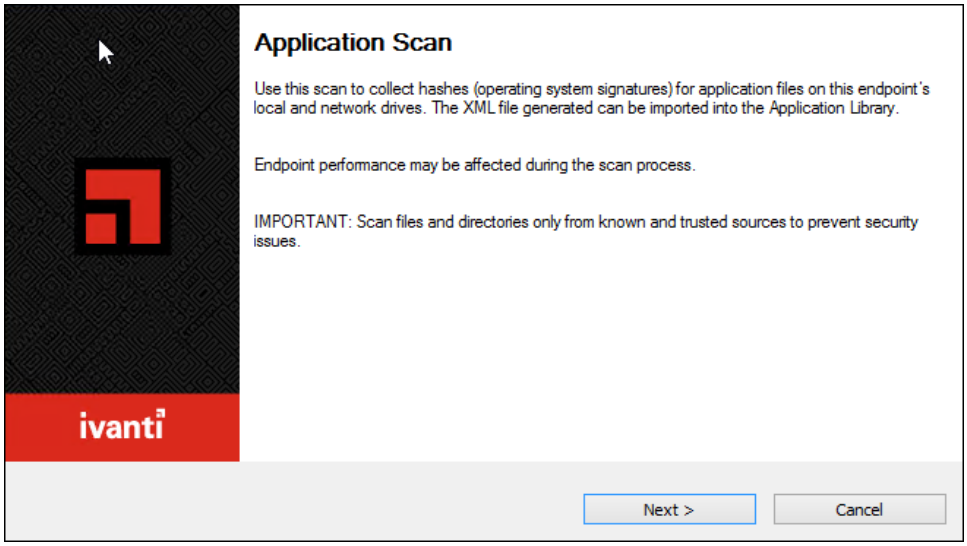
To Complete an Application Scan and Import into the Application Library

1. On the endpoint, select **Start > Control Panel**.
2. Double-click **Ivanti Endpoint Security Agent Control Panel**.
3. From the main menu, click **Application Control**.

4. In the **Application Control** section, click **Scan**.



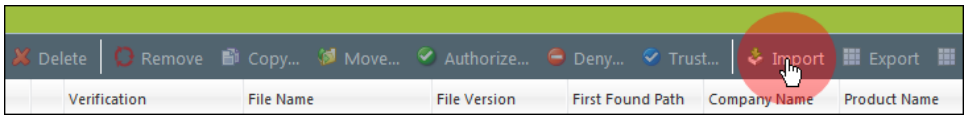
5. Complete the Application Scan wizard.



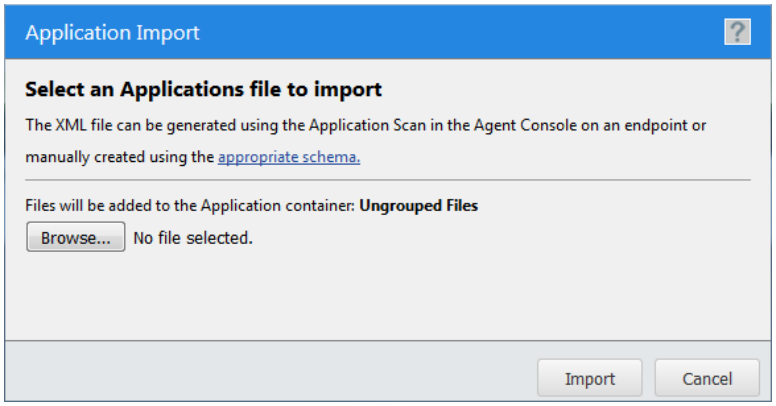
An XML file containing unique hashes (operating system signatures) for the application is generated. You can import it into the Application Library using the Import feature.

6. Select **Manage > Application Library**.

7. In the **Application Browser**, select **Applications**.
8. In the toolbar, click **Import**.



9. Complete the wizard.



Increase Monitored Endpoints

No two endpoints are the same. You have successfully migrated a small number of endpoints from Easy Auditor through policy creation and are ready for lockdown, but it does *not* mean you can lock down *all* the endpoints in your environment.

Different endpoints have different applications, different versions of applications, and different versions of application updaters. You'll need to maintain and update your policies to account for these differences.

Throughout this phase, increase the number of endpoints you are monitoring. You will lock down these endpoints in stages during the next phase.

Communicate with Users

As you increase the number of monitored endpoints, communicate with users so that they're aware of the changes and any impacts they may have. Advise users of any additional applications you've denied in this phase and advise users of alternate corporate-approved applications, as appropriate.

As you enforce Memory Protection, users may experience occurrences of applications being terminated unexpectedly, even with legitimate software usage. Provide users with an escalation procedure to follow.

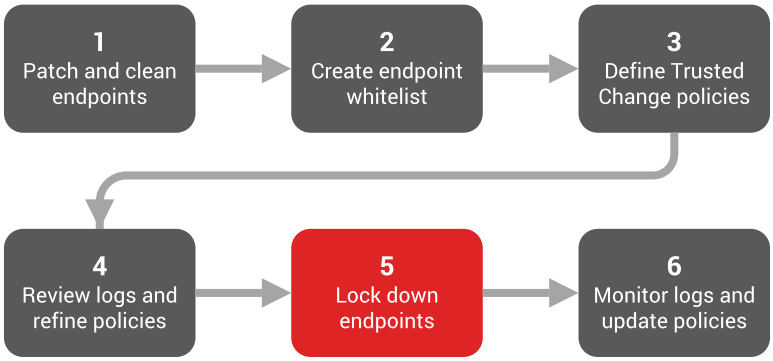
Finally, if you applied a Local Authorization policy in preparation for lockdown, let users know why this policy is applied, what they can expect and what action they should take. Provide users with an escalation procedure in the event they receive unexpected or excessive authorization requests.

See Appendix 2 for sample end user communications.

Phase 5: Lock Down Endpoints

You are ready to move endpoints into lockdown after the following:

- You've monitored the logs for the necessary period of time
- You've created the Trust policies required in your environment
- The logs have stabilized and you haven't seen any unexpected entries for at least one month



In this phase you will:

- Communicate with users so that they understand the upcoming changes and how to get assistance. See Appendix 2 for sample end user communications.
- Conduct a thorough antivirus scan prior to lockdown
- Lock down endpoints by applying the Easy Lockdown policy
- Authorize blocked applications when needed
- Use Local Authorization judiciously to provide flexibility

Once endpoints are locked down, the whitelist is enforced. Applications are blocked if they:

- Are not on the whitelist
- Are not allowed to execute by a Trusted Change policy

After lockdown, you can manage your Application Control deployment and authorize any blocked applications you want to allow in your environment.

Communicate with Users Prior to Lockdown

Communicate clearly with affected users so that they understand:

- Their endpoints are going into lockdown
- What the lockdown process means for users
- How users can get help if applications they need for their jobs are being blocked

If you have not already done so, customize the blocked notification dialog that appears on users' endpoints. This helps your users understand that the message came from your IT department and not from a suspicious or unknown third party.

See Appendix 2 for sample end user communications.

Conduct a Thorough Antivirus Scan

As a precautionary step, you should perform a thorough antivirus scan before starting Easy Lockdown, as a significant period of time has elapsed since you ran the Easy Auditor scan. It's important to re-scan your endpoints for any malware that may have entered your environment in the gap between scans.

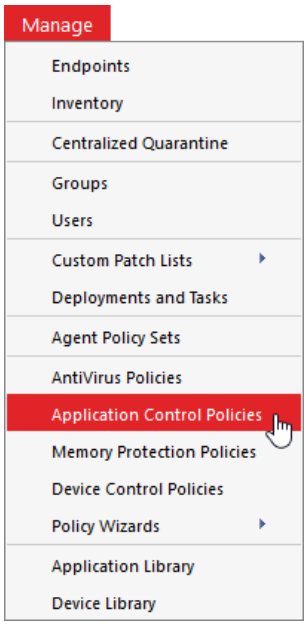
Apply the Easy Lockdown Policy

As with Easy Auditor, you should implement Easy Lockdown in phases, starting with a number of test endpoints. After the Easy Auditor logs have stabilized for that group, add additional groups and continue monitoring the logs between each addition.

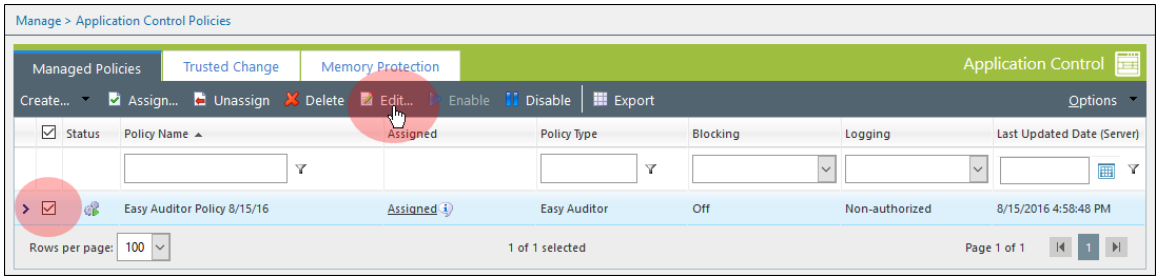
To move endpoints from Easy Auditor to Easy Lockdown, edit the Easy Auditor policy and convert it to an Easy Lockdown policy. Converting the existing policy avoids the need to re-create endpoint and group assignments.

To Convert an Easy Auditor Policy to an Easy Lockdown Policy

1. From the Endpoint Security Console, select **Manage > Application Control Policies**.

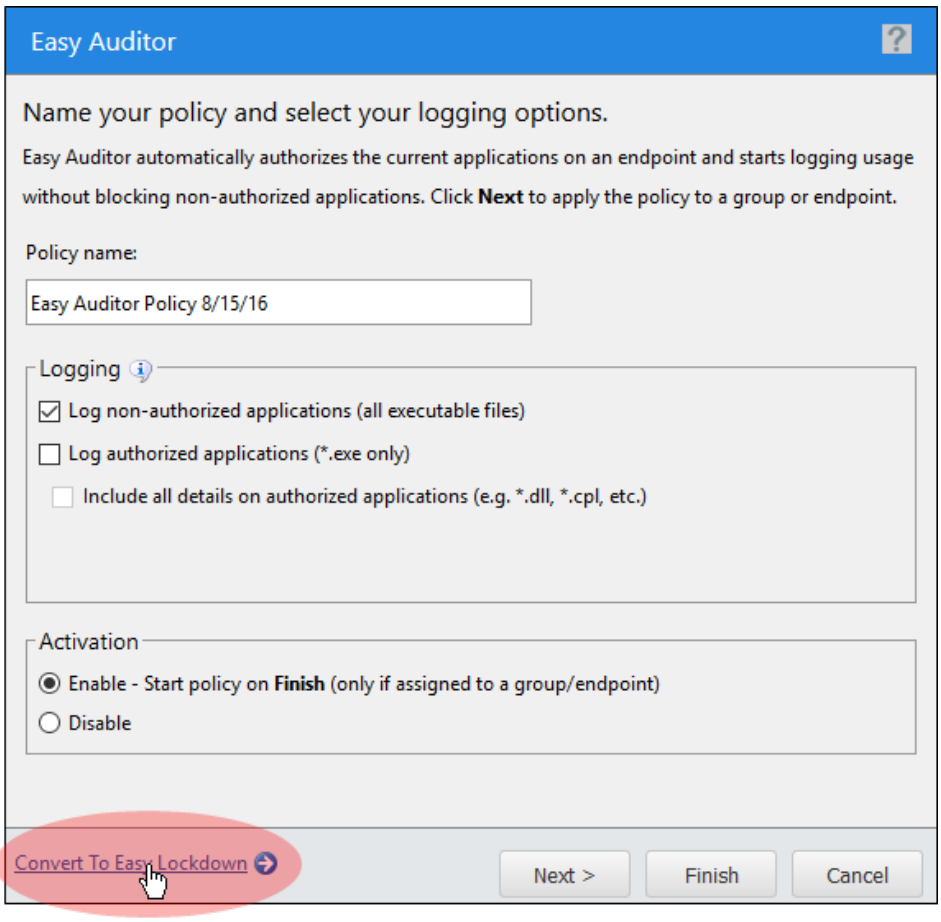


2. On the **Managed Policies** tab, select the Easy Auditor policy that you want to convert to Easy Lockdown and click **Edit**.



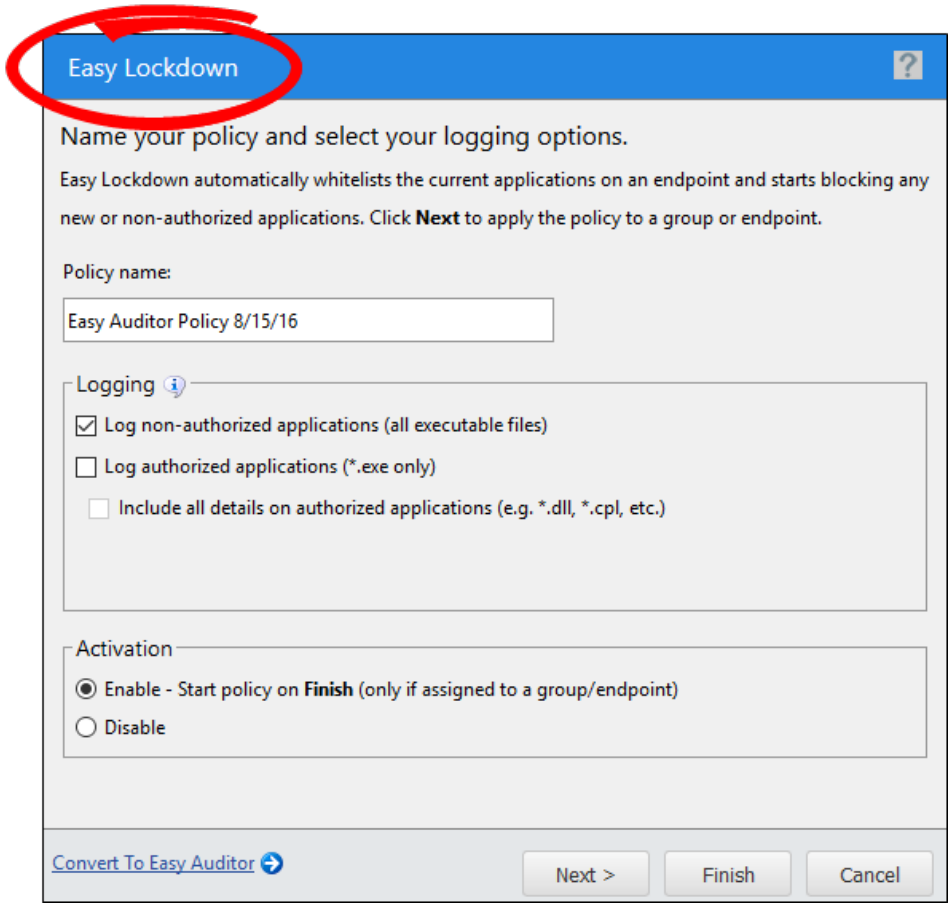
The Easy Auditor wizard opens.

3. Click the **Convert to Easy Lockdown** link at the bottom of the wizard.



The wizard converts to the Easy Lockdown wizard.

4. Progress through the Easy Lockdown wizard. See Converting an Easy Auditor Policy in the Application Control User Guide for detailed steps.



Authorize Blocked Applications When Needed

Although you've created the various Trusted Change policies and you've monitored the logs prior to going into Easy Lockdown, there may still be situations where applications are blocked and you need to authorize them. Examples of these situations include:

- **Infrequently updated applications**

  Some applications update very infrequently and may have been missed because the monitoring period was not long enough for you to see an update occurrence. The updated application is now blocked and you'll need to authorize it using a Supplemental Easy Lockdown/Auditor policy. You'll also need to apply a Trusted Updater policy (or other Trust policy) to handle future updates of this application.

- **Applications that are required to view a file**

  A user may receive a file from a customer, such as a video clip, that requires a specific application or plugin in order to view it. Since you are controlling which applications your users can execute, this needed application may be blocked. You should implement a process for users to request approval for new applications.

  - For simple applications, you can authorize the blocked files directly from the logs. See Authorizing, Denying, and Trusting Files from Logs in the Application Control User Guide for detailed steps.
  - For complex applications that use an application installer, add the installer as a Trusted Updater from the logs so that any associated files are whitelisted once they're installed.

- **Unusual/unsupported application update patterns**

  Application Control is designed to minimize your administrative workload by providing mechanisms such as Trusted Updater to add applications to the endpoint whitelist automatically, without any action from you.

  However, as detailed earlier, there is no standard method by which applications are updated, and vendors may issue different update mechanisms for major and minor releases. Applications that update in an unusual manner may be blocked and you'll need to authorize them separately. You may want to consider disabling automatic updates in these applications, where possible, to avoid such occurrences. You can then deploy approved updates to your endpoints using your normal software update tools.

Use Local Authorization Judiciously

If you apply a Local Authorization policy in Easy Lockdown, the user has the option to authorize blocked applications that they may need. This helps ease your users through the transition from Easy Auditor to Easy Lockdown.

How long should you leave Local Authorization in place? You have a couple options:

- If you have been using Local Authorization with Easy Auditor, you could **leave the Local Authorization policy in place for a short period** after you've applied the Easy Lockdown policy. With Local Authorization in place during Easy Lockdown, you help prevent user issues with blocked applications and avoid disrupting productivity.
- You could **leave the Local Authorization policy in place indefinitely** to maintain flexibility and minimize your workload. Leaving the policy in place limits the spread of potential malware to just the endpoint that locally authorized the malware, protecting other endpoints in your environment.

Important Considerations

As you consider using Local Authorization, keep in mind the following important factors:

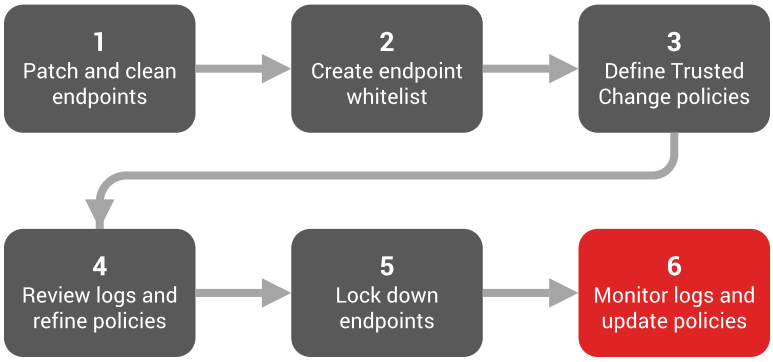
- Any executables that users authorized via Local Authorization will no longer be authorized once you have un-assigned the Local Authorization policy. These applications will be blocked if the user attempts to execute them. If you plan to remove the Local Authorization policy after going into lockdown, monitor the logs carefully and authorize any executables that will be needed after removing the Local Authorization policy.

  Alternatively, reapply the Easy Lockdown policy so that the endpoint whitelist is recreated for that endpoint.

- The Local Authorization is specific to the user to whom it is assigned. Any exeutables that a user authorizes are authorized for that user on that endpoint only. If multiple users share an endpoint, the users who don't have Local Authorization permissions will be unable to launch any executables that were locally authorized by others. However, you can authorize blocked files directly from the logs. See Authorizing, Denying, and Trusting Files from Logs in the Application Control User Guide for detailed steps.

Phase 6: Monitor Logs and Update Policies

Now that your endpoints are locked down, you can control which applications can execute in your environment.



In this phase you will:

- Continue to monitor logs and update Trusted Updater policies as needed
- Organize files in the Application Library so that you can authorize them
- Authorize applications centrally using a Supplemental Easy Lockdown/Auditor policy
- Use Local Authorization to authorize applications in time-critical situations or to support disconnected users
- Ensure you've implemented a process for users to request approval for new or blocked applications
- Remove old Application Control events to maintain a smaller, faster database

Maintain Trust Policies

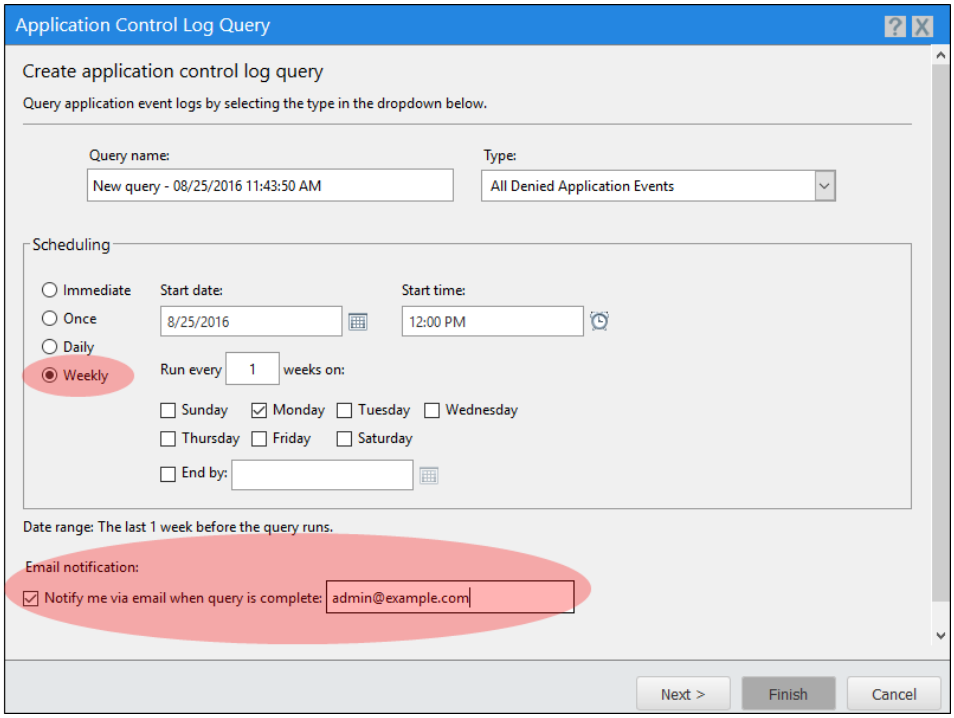
Continue monitoring logs during Easy Lockdown to determine whether policies need updates. In particular, review the **All Denied Application Events** and **Most Frequently Denied Application Events** logs to determine:

- Any blocked executables that you'd like to authorize
- Whether you'd like to offer approved applications for users to use in place of blocked applications

Schedule Log Queries

To help you remember to review the logs occasionally, we recommend that you schedule the log queries and have the results emailed to you. The scheduling frequency that you choose depends on the size of the logs and the number of endpoints in your environment.

We recommend reviewing the logs weekly if you have an escalation process in place for users to request blocked applications (thereby providing a quick turnaround to avoid disrupting productivity). Remember, you want to review trends and understand user behavior so that you can best serve your users while maintaining a secure environment.



Organize Files in the Application Library

Prior to lockdown, your focus in the Application Library is on denying executables that you want to block in your environment. After lockdown, you'll also need to authorize applications, which might include:

- Applications that were blocked and need to be authorized for a specific user or group of users
- Applications that were locally authorized by a user for their endpoint that you want to authorize for other users

In both cases, you'll need to organize the files in the Application Library into Applications and Application Groups so that you can authorize them.

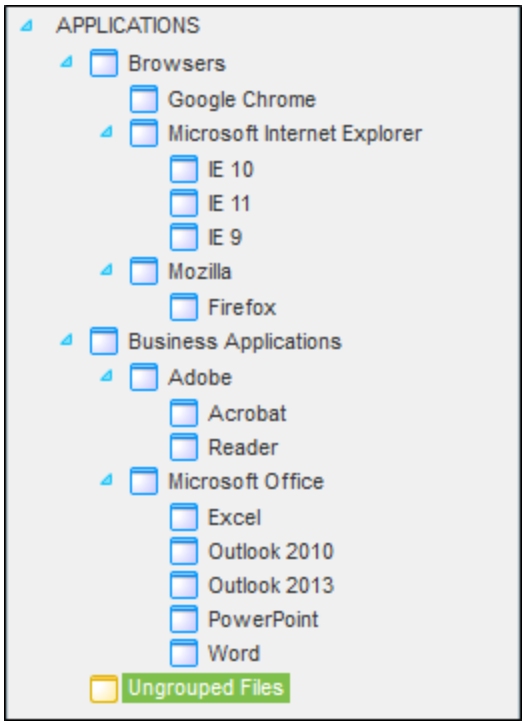
Organize Files into Applications

You can organize files in a number of different ways and nest folders up to three levels deep. Identify the best strategy for your organization. A common structure is as follows:

Level 1: Application Category (e.g., Browsers, Operating Systems, Games, Business Applications)

Level 2: Application Vendor and Product (e.g., Internet Explorer, Microsoft Office, Apple iTunes)

Level 3: Sub-Product and/or Version (e.g., IE10, Excel 2013, iTunes 12.4)

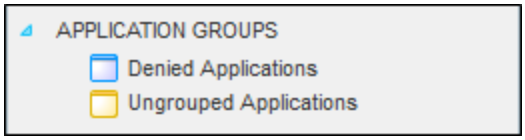


Application names must be unique at each level (e.g., you cannot list "Apple" under both Browsers and Business Applications). This is necessary because these applications will be organized into Application Groups.

For more information on organizing files into applications, see Organizing Application Library by Application in the Application Control User Guide.

Organize Applications into Application Groups

After you organize your files into Applications, organize Applications into Application Groups. Grouping programs allows you to deny them as a group rather than individually.



For more information on organizing Applications into Application Groups, see Organizing Application Library by Application Group in the Application Control User Guide.

Authorize Applications Centrally

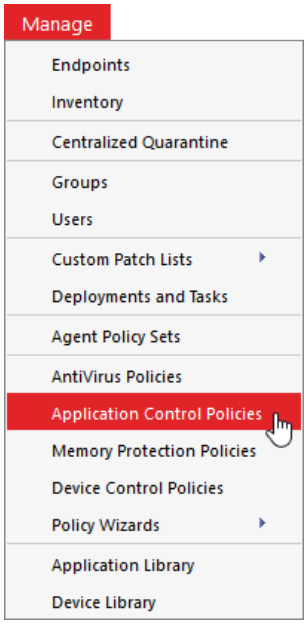
Use a Supplemental Easy Lockdown/Auditor policy to centrally authorize executables or applications and update the endpoint whitelists for the users to which the policy is assigned. You'll find this policy helpful when you want to:

- Authorize executables or applications when they have been blocked on users' endpoints
- Authorize executables or applications for users or endpoints *regardless* of whether the applications have already been installed on the endpoints. This means that if the files are not already on the endpoints and are added later, the files are already whitelisted and so they will be allowed to execute.

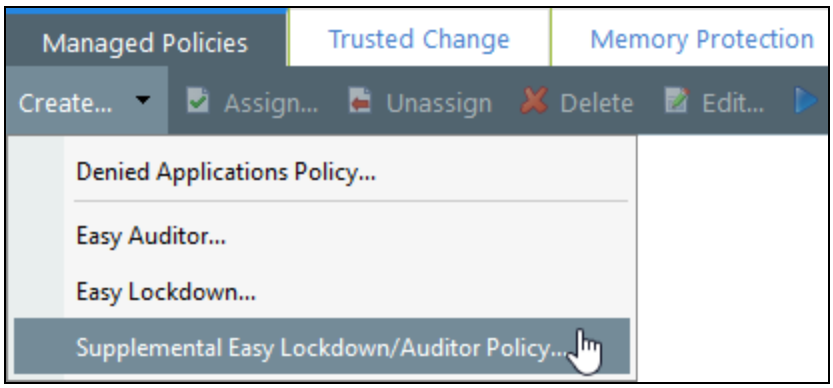
After you've organized files into Applications and Application Groups, you can authorize specific Applications or Application Groups for users and endpoints using a Supplemental Easy Lockdown/Auditor policy. This policy works in conjunction with the Easy Auditor or Easy Lockdown policy by supplementing the endpoint whitelist you created in Easy Auditor and Easy Lockdown.

To Create a Supplemental Easy Lockdown/Auditor Policy

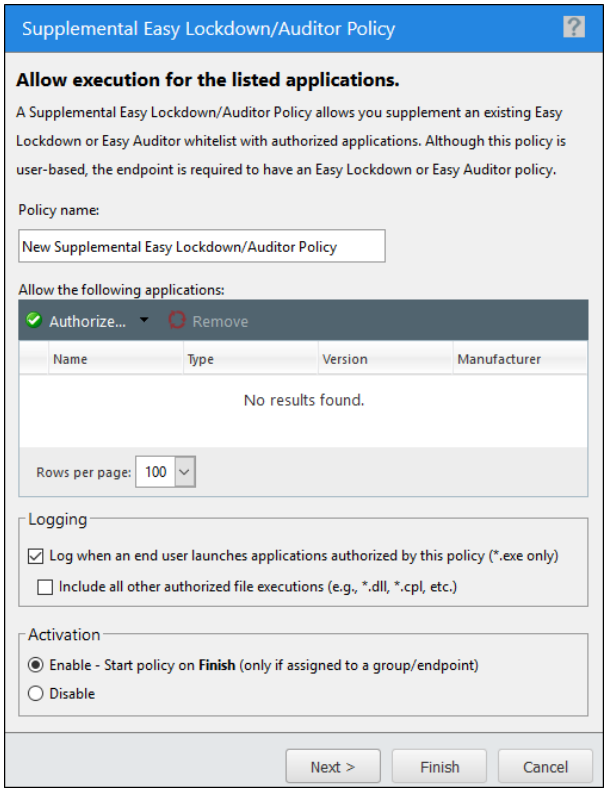
1. From the Endpoint Security Console, select **Manage > Application Control Policies**.



2. Select **Create > Supplemental Easy Lockdown/Auditor Policy**.

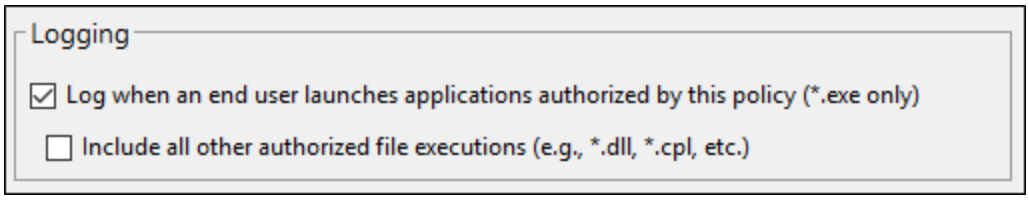


The Supplemental Easy Lockdown/Auditor Policy wizard opens.



3. Complete the wizard. See Creating a Supplemental Easy Lockdown/Auditor Policy in the Application Control User Guide for detailed steps.

   Under **Logging**, select **Log when an end user launches applications authorized by this policy** to determine whether certain applications are used in your environment. This is useful when you want to remove certain applications or application versions from your environment. However, don't select this option generally for all applications authorized by the policy, as this results in large numbers of logs for widely used applications.

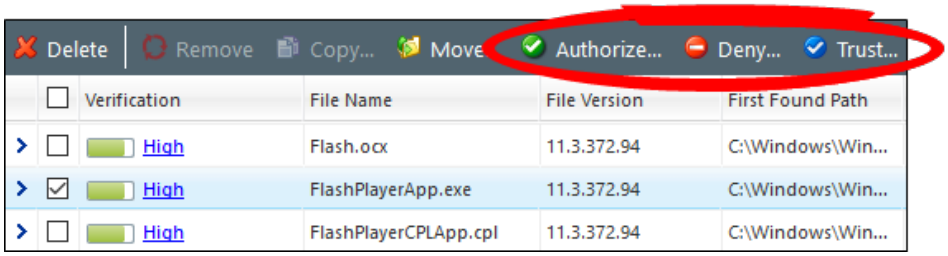


Maintain a Test Endpoint

Executables must be in the Application Library so that you can authorize or deny them. If you have not already established a test endpoint to scan new applications, set one up now so that any applications you want to authorize can be scanned and added to the Application Library.

Authorize, Deny, or Trust Executables Directly from the Application Library

You can quickly authorize, deny, or trust files, Applications, and Application Groups from within the Application Library. Select the item you wish to authorize, deny, or trust and click the associated button on the toolbar.



For more information, see Authorizing Files, Applications, and Application Groups in Application Library and Denying Files, Applications, and Application Groups in Application Library in the Application Control User Guide.

Authorize Applications with Local Authorization

While your endpoints are in Easy Lockdown, there may be situations where assigning a Local Authorization policy is the best option to quickly authorize blocked applications for your users. Use Local Authorization:

- In time-critical situations (such as when a user needs an application within minutes)
- In situations where a user is disconnected from the corporate network and needs to install new software (for example, when a sales engineer visits a customer site). In this case, you need to assign the Local Authorization policy before the user disconnects from the network.

Prior to unassigning the Local Authorization policy, review the logs and decide whether you should add locally authorized executables to either Authorized or Denied Applications policies.

Windows installer packages (MSIs) that are not Trusted Updaters are blocked automatically; users cannot authorize them locally. If a user needs to install an application using an MSI file, add the blocked MSI file as a Trusted Updater. The installation will then complete successfully without needing local authorization.

Allow Users to Request Applications

Change is inevitable and you need to manage evolving user and business needs. In addition to creating a reactive escalation process for addressing blocked applications, you also need to implement a more proactive process for introducing change. Decide how much flexibility to provide and how you'll approach balancing security with flexibility across the organization. As an IT administrator, your goal is to enable (rather than inhibit) business.

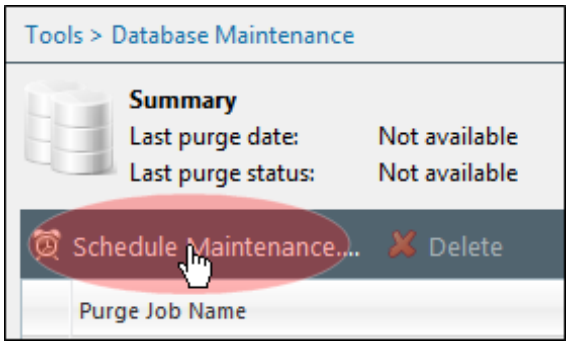
After you've defined the change control process, communicate it to your users so that they understand how to request approval for new or blocked applications ahead of time.

See Appendix 2 for sample end user communications.

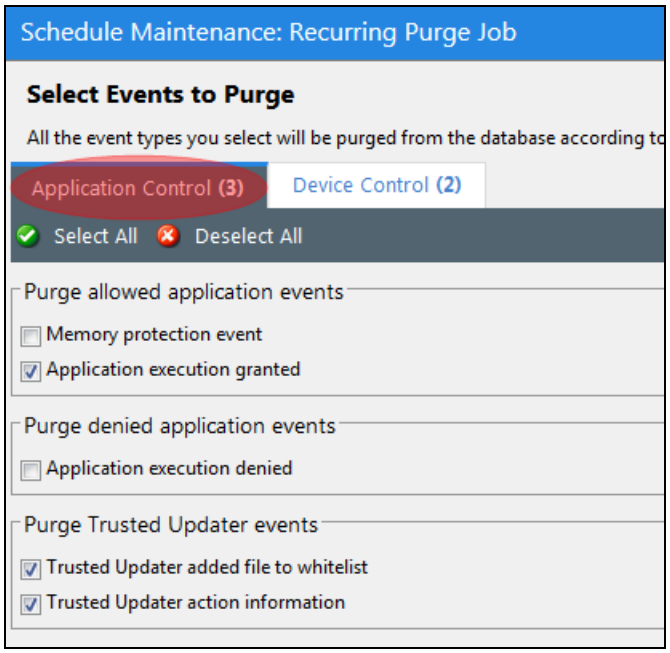
Maintain Your Database

Configure recurring purge jobs that safely remove old Application Control events and keep a smaller, faster database. Stored events become less useful and relevant over time, and their build-up can lead to performance issues.

1. From the Endpoint Security Console, select **Tools > Database Maintenance**.
2. Click **Schedule Maintenance**.



3. Complete the wizard. You'll see a new tab for Application Control events on the **Select Events to Purge** panel. The three most common event types are selected by default.



Events become eligible for purging when they exceed the minimum age you specify in the **Purge events older than X days** field.

Though purge jobs can run while Application Control is processing new events, we recommend that you schedule them for off-peak hours. Use a purge job's Maximum purge duration to manage purge time (minutes) and server load. At time-out the system finishes the event batch it's purging and then stops.

Purging is irreversible! Use care when configuring a purge job to avoid removing necessary data by accident.

Summary

You have worked through the best practice phases for implementing Application Control in your environment, and you've created a manageable state with minimal administrative burden.

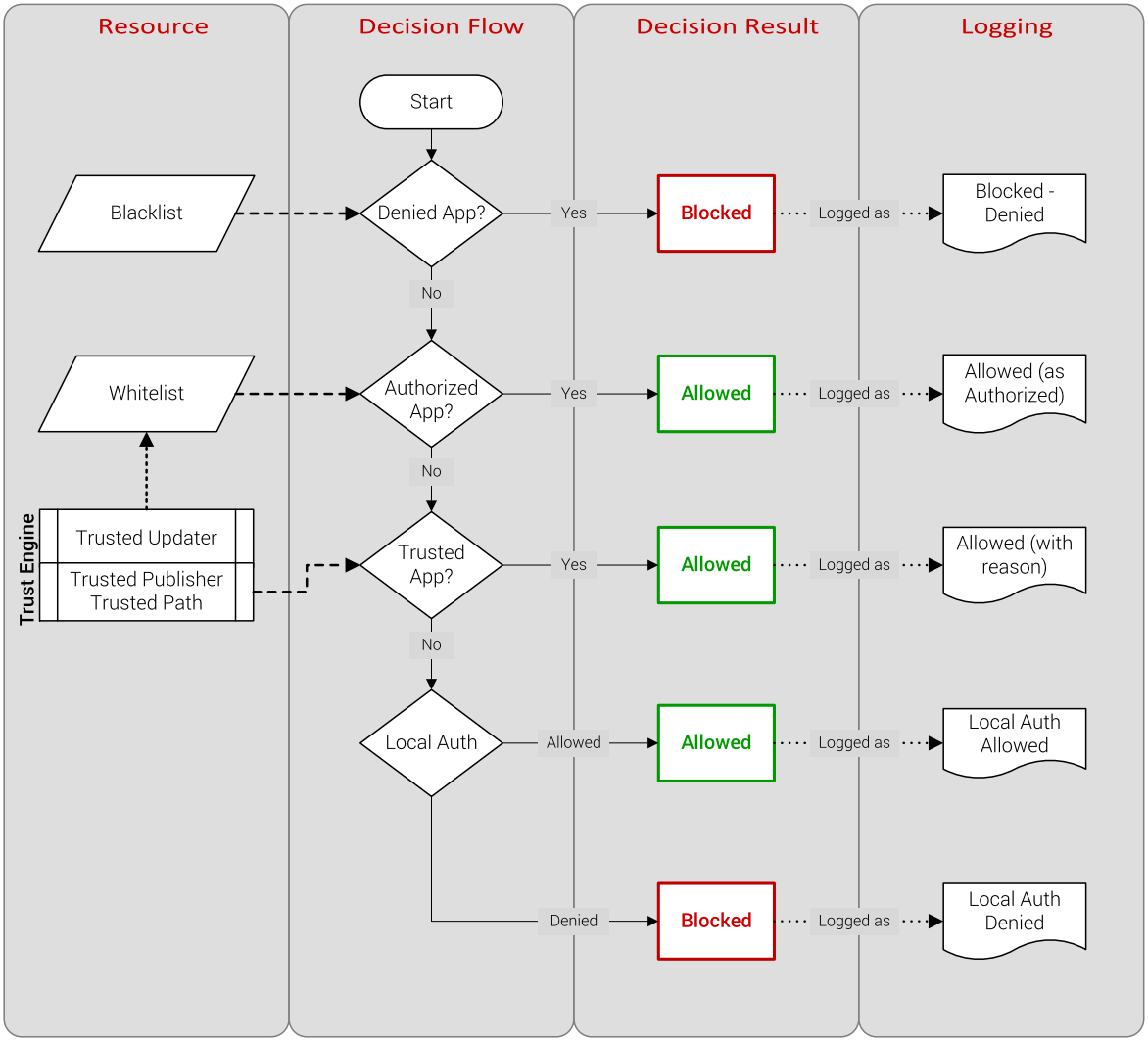
Going Forward

Keep in mind that in order to maximize the effectiveness of Application Control, you'll still need to:

- Plan for ongoing change and maintenance
- Maintain your process for handling user requests for blocked applications
- Review logs for trends to help you strategize for the software that is authorized for use in your environment

Appendix 1: Decision Flow at the Endpoint

To help you better understand how Application Control works, the following diagram illustrates the workflow that determines whether to allow or block an executable or application.



Appendix 2: Sample End User Communications

The following are some sample communications that you can customize and provide to your end-users as you roll out Application Control.

Introduction to Application Control: Sample Communication

Over the coming weeks, your IT team will introduce Application Control as an additional layer of defense against viruses and malware. IT is taking this step because of an increased number of infections and the rising cost of remediating them. These infections impact your productivity and leave confidential company information vulnerable to theft.

What is Application Control and how does it help?

Application Control prevents virus and malware attacks without impacting productivity. Application Control accomplishes this goal by only allowing use of applications that the company has approved. Approved applications are added to a "whitelist." The applications that you use are likely already on this list.

However, any unauthorized applications that are not whitelisted or violate the Application Control rules engine are blocked from executing. This is an effective security model that will reduce the frequency and cost of virus and malware incidents.

What does this mean for me?

There are a number of phases to the Application Control rollout. Your IT team will communicate with you at each phase so that you know what to expect and any potential impact it might have on you. The key phases are as follows:

1. **Patch and Clean Endpoints**

   To ensure we start from a “known good” state, all endpoints are patched to eliminate any known vulnerabilities. Endpoints are also scanned for malware.

2. **Create Endpoint Whitelist**

   Your computer is scanned to create a whitelist containing all the executable files on your computer. During this phase your computer is audited while we define policies that govern how changes (e.g., patches, application updates, etc.) can take place on your computer in the future.

   (Optional) Application Controlalso provides the ability to block application usage, and we plan to block the use of software unrelated to business, including games and music streaming software. A full list of restricted applications (and corporate approved alternatives, where appropriate) will be distributed in the future.

3. **Define and Review Trusted Change Policies**

   Until we are satisfied that your productivity will not be adversely affected by Application Control enforcement, your computer will continue to operate in audit mode. During this audit, we will update policies to account for unexpected events.

4. **Lock Down Endpoints**

   Once we are prepared, we will enable enforcement for Application Control, giving you significantly improved protection against virus and malware attacks. Any files that are not on the whitelist or are not authorized to run by an Application Control policy will be blocked.

5. **Monitor Logs and Update Policies**

   Once enforcement is active, there will be a process available to request approval for any applications denied by corporate policy.

The rollout will proceed in phases across the organization, with additional groups of users being added over time. For a given group of users, the rollout process is expected to last one month.

If you have any questions or concerns about the proposed rollout, you should contact your manager, who will relay these concerns to the IT team.

Patch and Clean: Sample Communication

The first step in introducing Application Control is patching our endpoints to eliminate any known vulnerabilities and remove any known malware.

We'll conduct two separate scans of your computer:

- The first will identify applications that are not updated with available patches. These patches will be applied to eliminate known vulnerabilities.
- The second scan will identify and remove any known malware present on your computer.

To minimize the effect on your productivity during these scans, we plan to complete scans off business hours when possible. These scans will be scheduled to take place this week. Please ensure that you leave your computer turned on and connected to the network when you leave the office.

If we are unable to complete the scan off business hours, we will need to schedule the scan for normal business hours. We will try to minimize the effect of this scan on your productivity, but you may notice some slowdown while the scan is running. For example, normal operations such as opening applications or copying files may be slower.

Endpoint Whitelist: Sample Communication

The next phase in our Application Control rollout is to generate a whitelist based on the applications that are currently installed on your computer. Your computer will be scanned to identify all of the executable files, and these files will then form the initial whitelist for your computer.

To minimize the effect on your productivity while this scan takes place, we plan to conduct the scan off business hours if possible. The scan will be scheduled to take place this week. Please ensure that you leave your computer turned on and connected to the network when you leave the office.

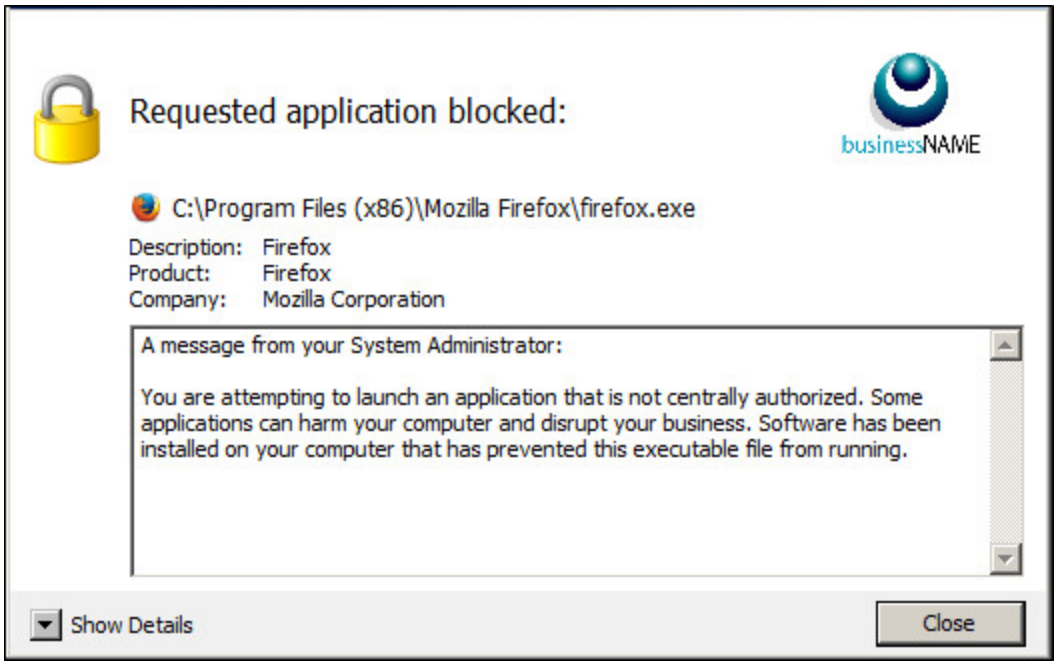
If your computer is powered down before or during the scan, it will start over from the beginning once the computer is powered on. Depending on the size of your hard drive, the scan may take several hours to complete. While the scan is running, you may notice some slowdown for normal operations such as opening applications and copying files.

Once the scan has completed, your computer will continue to operate as normal. Your computer will be in audit mode, and your IT team will monitor your computer for application file changes. IT will also create and apply policies that enable trusted change to occur on your computer.

Denied Applications: Sample Communication

As part of our Application Control rollout, we will block software that doesn't comply with corporate policy. This includes non-productivity related applications, such as games or unapproved audio and video streaming applications that consume network bandwidth. A list of blocked applications and application categories is available here <add link>. This list will be updated as we identify additional applications that are not permitted.

If you attempt to execute a denied application, you will receive a blocked dialog that looks like this <customize the dialog by adding your corporate logo, updating the message text and adding a URL>:



If you need this application to do your job, you should submit an approval request to the IT helpdesk. The application will be authorized once it has been approved. You can also obtain approved software from here: <add URL>.

Memory Protection: Sample Communication

Application Control includes Advanced Memory Protection as a security feature to protect against memory-based attacks, including memory injection. Memory injection is becoming a prevalent way to infect enterprise computers. Advanced Memory Protection provides us with an additional layer of defense to keep your computer safe.

However, some legitimate software vendors also use memory injection techniques. Application Control may block this software from operating. If you experience issues, such as an application shutting down repeatedly when you perform certain actions, you should log a case with the IT helpdesk to have this investigated and resolved.

Preparation for Lockdown with Local Authorization: Sample Communication

We are nearing the end of our rollout phase for Application Control. Your computer has been in audit mode for the past few weeks, and we have been updating the policies that allow your applications to be updated once your computer is locked down. We are now ready to take that final step and move into lockdown.

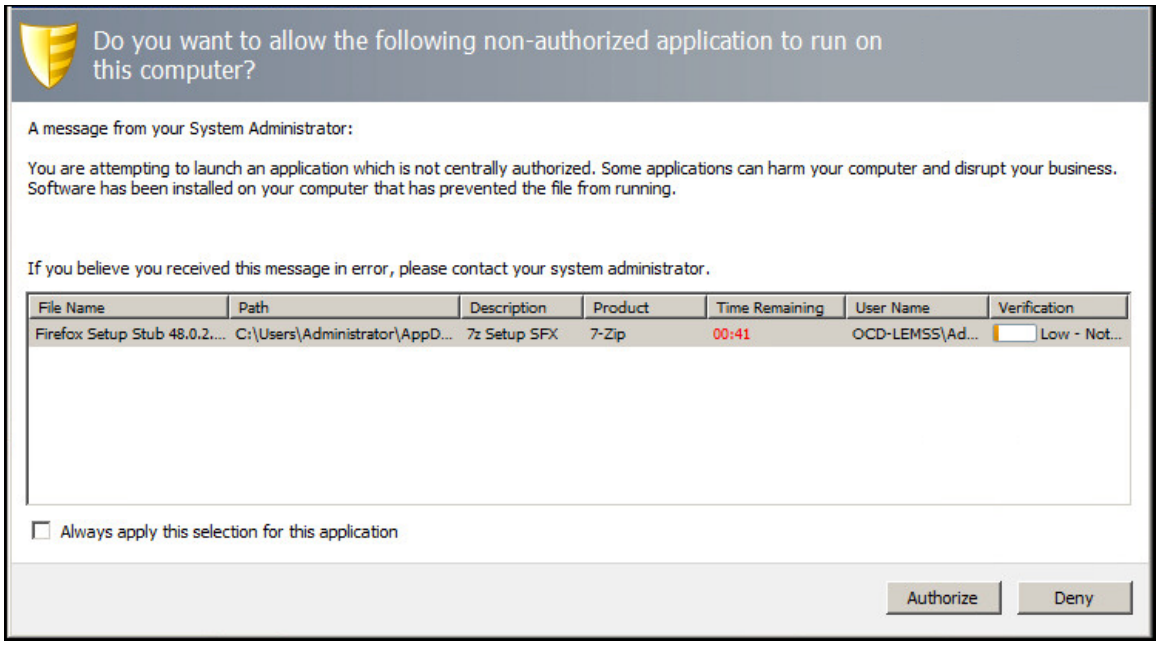
For the initial lockdown period, we are going to provide you with the ability to authorize any new or updated applications locally. We are allowing this local authorization to:

- Ensure that the lockdown process doesn't affect your productivity
- Provide assurance that Application Control in lockdown will not result in many support calls

Before enabling local authorization, we will scan your computer once again to ensure that we have captured any new applications that were installed since the original scan was conducted. To minimize the effect on your productivity while this scan takes place, we plan to conduct the scan off business hours if possible. The scan will be scheduled to take place this week. Please ensure that you leave your computer turned on and connected to the network when you leave the office.

If your computer is powered down before or during the scan, it will start over from the beginning once the computer is powered on again. Depending on the size of your hard drive, the scan may take several hours to complete. While the scan is running you may notice some slowdown for normal operations, such as opening applications and copying files.

Once the scan has completed, your computer should continue to operate as normal. However, if you attempt to install or run a new application, you will receive an authorization dialog that looks like this:



The purpose of implementing Application Control is to prevent malware from executing, so please authorize files judiciously. Please review the filename to confirm that this is an application that you expect to execute.

Moving into Lockdown: Sample Communication

Following several weeks of preparation, your computer is now ready to take the final step in the introduction of Application Control, which is to move into full lockdown. We've implemented policies to support trusted change on your computer. Changes on your computer will be seamless as patches are applied, applications are updated, and new applications are rolled out. However, once we are in lockdown, any unplanned or unauthorized changes will be blocked. For example, you will no longer be able to download and install software directly from the Internet. You will need to submit a request to the IT helpdesk to obtain approval for this new software. More importantly, lockdown protects your computer by blocking any viruses or malware.

Before we lock down your computer, we will scan it once again to capture any new applications that were added since the original scan. To minimize the effect on your productivity while this scan occurs, we plan to conduct the scan off business hours if where possible. The scan will be scheduled to take place this week. Please ensure that you leave your computer turned on and connected to the network when you leave the office.

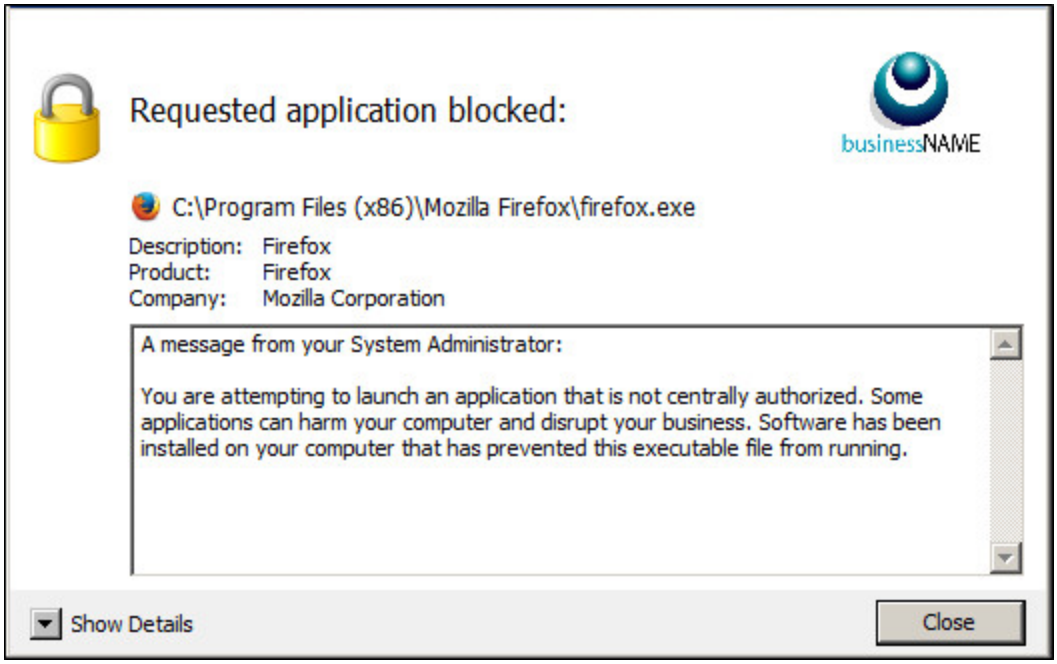
If your computer is powered down before or during the scan, it will start over from the beginning once the computer is powered on again. Depending on the size of your hard drive, the scan may take several hours to complete. While the scan is running, you may notice some slowdown for normal operations, such as opening applications and copying files.

Once the scan has completed, your computer should continue to operate as normal. However, if you experience any issues, please submit a case to the IT Helpdesk.

Thank you for your cooperation and support during the rollout period.

Files Blocked: Sample Communication

If Application Control blocks a file from executing, you will receive a dialog that looks like this <customize the dialog by adding your corporate logo, updating the message text and adding a URL>:



If you need this application to do your job, first check the approved software list to see if similar, alternative software is already supported. If it is, you can go ahead and install the application. If it is not on the list and there is not a suitable alternative application on the list, submit an approval request to the IT helpdesk. The application will be authorized once it has been approved.

You can obtain approved software from here: <add URL>.