Application Control 8.6

User Guide

ivanti | Endpoint Security
powered by HEAT

Notices

Version Information

Ivanti Endpoint Security: Application Control User Guide - Ivanti Endpoint Security: Application Control Version 8.6 - Published: Dec 2020

Document Number: 02_205_8.6_171251657

Copyright Information

Table of Contents

Chapter 1

Application Control Overview

In this chapter:

Ivanti Application Control allows organizations to prevent unwanted or non-authorized applications from executing on IT assets. These applications include malware, unsupported versions of otherwise acceptable applications, resource- or productivity-sapping programs, or software known to increase the danger of unintentional or malicious data leakage. Application Control provides administrators with automatic methods to permit authorized and trusted changes, thus reducing the workload and increasing the uptime of IT assets.

About Application Control

Ivanti Application Control enables you to prevent 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 endpoints such as laptops, desktops, servers, and other IT resources.

A *whitelist* is a list of executable files (stored in the form of *hash values*) that are authorized to run on an endpoint. A whitelist is created when an application scan is performed on the endpoint during Easy Auditor or Easy Lockdown.

Ivanti Application Control also provides a centralized *blacklist*, a list of executable files that are forbidden to run. There are also *trust mechanisms* which automatically authorize applications to run, based on specific criteria.

Administrators create policies that define how whitelists, blacklists and trust mechanisms are applied across the enterprise. These policies can be assigned to individual endpoints, groups, and users.

When application control is enforced, an executable can only run on an endpoint if it is on that endpoint's whitelist or if it is permitted by one of the trust mechanisms. While it is running, its processes can be protected from external attack with a *Memory Injection policy*.

To minimize disruption to end user productivity, it is best to have an evaluation period prior to enforcing application control. During this period, administrators can monitor and analyze application usage, and create appropriate policies.

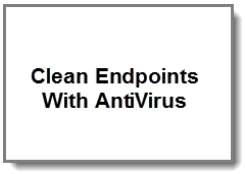
Main Features of Ivanti Application Control

The main features of Ivanti Application Control include *managed policies*, *trust mechanisms*, *memory protection*, the *Application Library*, and *event log queries*.

Managed Policies	• Easy Auditor - scans endpoints and creates whitelists of installed applications; records execution of non-whitelisted applications. • Easy Lockdown - scans endpoints and creates whitelists of installed applications; blocks nonwhitelisted applications from installing or running. • Supplemental Easy Lockdown/Auditor - adds applications to an endpoint's whitelist after Easy Auditor or Easy Lockdown. • Denied Applications - creates a centralized blacklist of applications that are not allowed to run.
Trust Mechanisms	• Trusted Updater - automatically adds files to an endpoint's whitelist of permitted applications. • Trusted Publisher - allows executable files with a digital certificate from a trusted source to run. • Trusted Path - allows executable files in a specified file system path to run. • Local Authorization - allows specified users to authorize nonauthorized applications.
Memory Protection	• Memory Injection Policies monitor running processes for reflective memory injection, where external (possibly malicious) code is executed within an authorized process. • Policies can run in Audit mode or exclude known good files that use memory injection as part of their normal operation.
Application Library	• Organizes executable files into relevant applications and application groups. • Helps assign policies to files, applications, and application groups.
Event Log Queries	• Predefined query types can be run against specified endpoints or groups. • Logs provide information to shape effective application control policies.

How Ivanti Application Control Works

An administrator usually begins the Ivanti Application Control process by removing any malware from a select group of endpoints and applying an Easy Auditor policy. This is followed by an evaluation period when trusted change policies can be defined, applied, and monitored. When conditions are right, an Easy Lockdown policy is applied, which restricts the installation of new applications to those permitted by trust mechanisms.

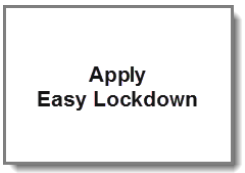


Clean: Scan endpoints for malware with Ivanti AntiVirus or other antivirus program.

Discover: Apply Easy Auditor to selected endpoints, with logging enabled. This builds a whitelist of existing application files without blocking new applications or updates to existing ones. These files are also added to Application Library where they can be organized into applications and application groups.

Define: Create and apply trusted change policies (Trusted Publisher, Trusted Updater, Trusted Path). Usage logs will now record changes that were authorized by these trusted change mechanisms.

Monitor: Review application control logs daily to see which applications would be blocked if enforcement was enabled. Adjust trust policies and use Local Authorization if needed in the transition to lockdown.



Enforce: Applying Easy Lockdown creates a new whitelist of installed applications and blocks the installation or upgrading of applications, except for those specified by trusted change policies.

Important: Easy Lockdown is a crucial phase in application control and should only be applied when you are confident that it will not adversely affect endpoints or users.

Manage: Continue monitoring the network and maintaining trusted change and Supplemental Easy Lockdown/Auditor policies that keep all required software running and up to date. This approach reduces the administrative overhead in maintaining application control.

Chapter 2

Installing Application Control

In this chapter:

Ivanti Endpoint Security is a platform that supports various modules, which are components that secure endpoints in unique ways. Before you can begin using a module, you must first install it.

Explaining Module Subcomponents

Ivanti Endpoint Security is a platform for *modules*, which are add-ons that protect your network using different methods. Each Ivanti Endpoint Security module is composed of two subcomponents: the server component and the endpoint component.

Server Component	This subcomponent is installed on the Ivanti Endpoint Security server. The server component must be installed before the endpoint component.
Endpoint Component	This subcomponent is installed on endpoints hosting a Ivanti Endpoint Security Agent. Endpoint components can be installed after the server component and agents are installed. Each installed endpoint subcomponent consumes an agent license for the applicable modules

Note: Ideally all endpoint agents should be the same version as the Ivanti Endpoint Security server.

New releases of the server support all currently supported versions of the endpoint agent. Older agent versions, however, are constrained to the features available when the agent was released and may not support new server functionality.

Installing the Application Control Module Server Component

To begin using Ivanti Application Control, you must first install the Application Control module server component on your Ivanti Endpoint Security Server.

Prerequisites:

You must be licensed for Ivanti Application Control.

Install the Application Control module server component using the Ivanti Installation Manager.

Tip: For additional information on using the Ivanti Installation Manager, refer to the Ivanti Endpoint Security: Wake on LAN User Guide (https://help.ivanti.com) .

1. Select **Tools** > **Launch Installation Manager**.

   Step Result: Installation Manager opens to the ***New/Update Components*** tab.

2. Select the **Application Control** check box for your version number of Ivanti Endpoint Security.
3. Click **Install**.

   Step Result: The ***Install/Update Components*** dialog opens.

4. Click **Install**.

   Step Result: A dialog opens, notifying you that installing the module may cause logged in user to lose their work.

5. Click **OK**.

   Step Result: The installation begins.

6. Click **Finish**.

   Tip: Select the **Launch Ivanti Endpoint Security** check box to relaunch Ivanti Endpoint Security after clicking **Finish**.

Result: The **Application Control** module server component is installed. To begin using the module, reopen Ivanti Endpoint Security.

After Completing This Task:

Complete Adding the Application Control Module Endpoint Component on page 17.

Uninstalling the Application Control Module

You can remove Application Control from Ivanti Endpoint Security. When uninstalling the module, both the server component and endpoint components are removed.

Uninstall Application Control from the Ivanti Installation Manager.

1. Select **Tools** > **Launch Installation Manager**.

   Step Result: The Ivanti Installation Manager opens to the ***New/Update Components*** tab.

2. Select the ***Existing Components*** tab.
3. Select the **LAC** check box.
4. Click **Uninstall**.

   Step Result: The ***Uninstall Components*** dialog opens.

5. Click **Uninstall**.

   Step Result: A dialog opens, warning you that uninstalling the module may cause logged in users to lose their work.

6. Click **Yes**.

   Step Result: Removal of the module begins.

7. Click **Finish**.

   Step Result:

   Tip: Select the **Launch Ivanti Endpoint Security** to relaunch Ivanti Endpoint Security after clicking finish.

Result: The module is uninstalled. Relaunch Ivanti Endpoint Security to complete the uninstall.

Adding the Application Control Module Endpoint Component

To enable application control functionality on Ivanti Endpoint Security endpoints, the Application Control module endpoint component must be added to the endpoints.

Prerequisites:

- The Application Control module server component must be installed on the Ivanti Endpoint Security Server.
- The Ivanti Endpoint Security Agent is installed on target endpoints.

Add the Application Control module endpoint component from the ***Endpoints*** page.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the ***All*** tab.

2. From the list, select the endpoints that you want to add the Application Control module endpoint component to.
3. Click **Manage Modules.**

   Step Result: The ***Add/Remove Modules*** dialog opens.

4. Select the **App Control** check box for all endpoints you want to install the component on.
5. Click **OK**.

Result: The ***Add/Remove Modules*** dialog closes. The Application Control module endpoint component begins installing, as denoted by the **LAC Installed** column **pending** status. The process is completed when the status changes to **Yes**.

Removing the Application Control Module Endpoint Component

You can remove Application Control module endpoint components from selected Ivanti Endpoint Security endpoints in your environment.

Prerequisites:

The Application Control module agent component must be installed on the endpoint.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the ***All*** tab.

2. Select the ***Application Control*** tab.

   Step Result: A list of all endpoints where the Application Control module endpoint component is running displays.

3. From the list, select the endpoints from which you want to remove the Application Control module endpoint component.
4. Click **Manage Modules**

   Step Result: The ***Add/Remove Modules*** dialog opens.

5. Clear the **App Control** check box for all endpoints you want to remove the component from.
6. Click **OK**.

Result: The ***Add/Remove Modules*** dialog closes. The Application Control module endpoint component is removed, as denoted by the **No** status of the **LAC Installed** column on the ***Endpoints*** page's ***All*** tab.

Chapter 3

Getting Started with Ivanti Application Control

In this chapter:

Application Control is a Ivanti Endpoint Security module that controls the applications and executable files that run on your managed network endpoints. To get started with Application Control, you should install the module's server and endpoint components.

By applying an Easy Auditor policy, you can make an inventory of the applications and files on the network. You can then create trust policies to maintain and update applications with minimal administrative overhead. By monitoring the effects of these policies on the network, you can modify them to improve their effectiveness.

With trust policies in place, you can roll out Easy Lockdown across the network to enforce application control. Policies are also available to temporarily or permanently authorize new applications when required. You should continue monitoring the network after lockdown to ensure that it remains secure and its applications are running properly and being updated when necessary.

Application Control at a Glance

Ivanti Application Control is a module that allows an administrator to authorize or block applications running on a network.

Benefits

- Uses *application whitelisting*, a security approach that allows only authorized applications to run.
- Blocks applications that are regarded as dangerous, unnecessary, or unproductive.
- Automates the process of maintaining and updating the authorized applications.
- Provides another layer of the *defence in depth* afforded by Ivanti Endpoint Security.
- Gives administrators complete visibility into all applications currently residing on network endpoints.
- Automatically blocks zero-day attacks, without waiting for the latest anti-virus definitions and patches.
- Provides continuous protection against *reflective memory injection* attacks.

Key Terms

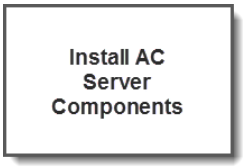
Application Control	A Ivanti Endpoint Security module that helps prevent the execution of malicious code and unwanted, unproductive software on a network. This module uses a security approach called *application whitelisting*, which allows only authorized applications to run on endpoints such as laptops, desktops, servers, and other IT resources.
application whitelisting	The security approach used by Ivanti Application Control to prevent the execution of malicious code and unwanted software by only allowing authorized applications to run. Such applications are either on an endpoint whitelist or permitted by a trust mechanism.
Easy Auditor	A managed policy that scans an endpoint and authorizes the applications it finds by creating a whitelist of those applications. It does not block other applications from subsequently installing and/or running, but it does not add these later applications to the whitelist.
Easy Lockdown	A managed policy that scans an endpoint and authorizes the applications it finds by creating a whitelist of those applications. It blocks other applications from subsequently installing or running, thereby enforcing application control.
Trusted Change policy	Any of the four policies that use the concept of trusted change to manage and authorize applications that are not on an endpoint's whitelist. These policies include Trusted Updater, Trusted Publisher, Trusted Path, and Local Authorization.

Managed Policy	An application control policy that creates or supplements a whitelist of authorized applications, or a blacklist of blocked applications. These policies include Easy Auditor, Easy Lockdown, Supplemental Easy Lockdown/Auditor, and Denied Applications.
Application Library	A central area for managing all applications and executable files under application control. The Application Library is populated when an application scan is performed during Easy Auditor or Easy Lockdown. The administrator can then organize the executable files into applications and application groups.
application control log	A log that records Ivanti Application Control events for a given set of endpoints. These events include applications being allowed to run or being blocked by specific Ivanti Application Control policies. The application control log is an important tool for introducing, implementing, and maintaining application control in the enterprise.
blacklist	A centralized list of executable files (stored in the form of hash values) that are forbidden to run on endpoints under application control.
Reflective Memory Injection	A technique for excuting external code within an authorized process, bypassing an endpoint's whitelist enforcement mechanism. This is sometimes (though not always) the result of a malware attack.
Memory Injection Policy	An Application Control policy that monitors running processes for reflective memory injection. It can be configured to audit and/or stop a process when memory injection is detected.

Getting Started with Ivanti Application Control

To use Ivanti Application Control, all Ivanti Endpoint Security components must be installed, along with the Application Control module. After installing all necessary components, review this chart to understand the Application Control work flow.

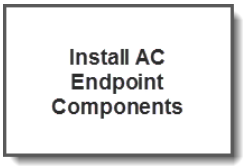
Important: While Ivanti Application Control has been designed to minimize the administrative burden, thorough preparation is needed for a successful implementation. It is especially important to have effective trusted change policies in place before endpoints are locked down in the Enforce phase.



Install Server Component: Install the Application Control module server component. This component is installed after initial Ivanti Endpoint Security installation.

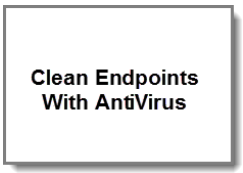
Note: If you purchased an Application Control license during your initial Ivanti Endpoint Security purchase, Application Control is installed during the initial Ivanti Endpoint Security installation by default.

For more information, see Installing the Application Control Module Server Component on page 16.



Install Endpoint Component: Install the Application Control module endpoint component on agents you want to support Application Control functions. Each agent you install the endpoint component on consumes an Application Control license.

For more information, see Adding the Application Control Module Endpoint Component on page 17.



Clean: Conduct a thorough virus scan of all endpoints with Ivanti AntiVirus or other antivirus program to ensure that no malware is added to the whitelist of applications allowed to run on the endpoints.

Discover: Apply Easy Auditor to selected endpoints. This runs an application scan that creates endpoint whitelists of installed files, adds these files to Application Library, and starts logging application activity. Organize files in Application Library into applications/application groups that reflect software usage. This enables you to deny applications to specified users at any point (even before lockdown).

For more information, see Working with Easy Auditor on page 76 and Working with Application Library on page 239.

Apply Trusted Change Policies

Define: Create the policies needed to support trusted change on endpoints - Trusted Updater, Trusted Publisher, and Trusted Path. Review Application Control logs to determine these policies.

- Trusted Updater enables administrators to automatically install and authorize patches and applications. This is the only trust policy that updates the endpoint whitelist.
- Trusted Publisher automatically authorizes software installers, updates or new applications to execute if the files have been signed by a trusted certificate.

Note: MSIs that are not Trusted Updaters are blocked automatically.

- Trusted Path authorizes applications in a specified location to run (optionally with ownership restrictions). Trusted Path should be used with caution as it is less restrictive than the other trust policies.

For more information, see Trusted Change Policies on page 141.

Monitor Application Control Behavior

Monitor: Continue reviewing application control logs and, if necessary, update the trusted change policies to prepare for lockdown. This phase should last at least a month. Assign Local Authorization policies to enable selected users to authorize applications that are not suitable for the other trusted change policies.

Note: You may need to refine trusted change policies, monitor the results, and (optionally) reapply Easy Auditor before moving into lockdown. Make the effort to put the optimum policies in place.

For more information, see Working with Application Control Log Queries on page 277 and Working with Local Authorization on page 206.

Apply Easy Lockdown

Enforce: Apply an Easy Lockdown policy to endpoints, creating whitelists of permitted applications and by enforcing application control, blocking new applications from installing or running.

Important: Easy Lockdown is a crucial phase and should only be applied when you are confident it will not adversely affect endpoints or users.

With appropriate Trusted Change policies in place, there will be an easy transition from Easy Auditor to Easy Lockdown. Individual users can be assigned Local Authorization policies, and new applications can be added with Supplemental Easy Lockdown/Auditor policies.

For more information, see Working with Easy Lockdown on page 89.

Manage: You now have a stable network of locked-down endpoints. With trusted change, applications update automatically without intervention, and selected users can install required applications themselves.

You still need to plan for maintenance and have a process to handle escalations associated with blocked applications. Continue reviewing logs for trends that will help you manage your software environment. Because of trusted change, however, the administrative burden will be very tolerable.

Chapter 4

Using the Ivanti Endpoint Security Console

In this chapter:

Within the Ivanti Endpoint Security console, you can use a number of common functions to navigate and operate the system. After you log in, Ivanti Endpoint Security opens to the ***Home Page***.

Ivanti Endpoint Security performs the following functions:

- Endpoint Detection
- Agent Installation
- Endpoint Management
- Endpoint Grouping
- Agent Policy Set Creation
- User and Role Creation and Management
- Server Module Management
- Report Generation

Ivanti Endpoint Security consists of a browser-based management console, which provides access to system management, configuration, reporting, and deployment options.

Common Functions

Ivanti Endpoint Security uses standard Web browser conventions and unique conventions. Familiarize yourself with these conventions to facilitate efficient product use.

From the **Navigation Menu** and system pages, you can access all features and functions you are authorized for.

Common Conventions

The Web console supports user interface conventions common to most Web applications.

Table 1: Common User Interface Conventions

Screen Feature	Function
Entry Fields	Depending on text, type data into these fields to either: • Retrieve matching criteria • Enter new information
Drop-Down Menus	Display a list of selectable values when clicked.
Command Buttons	Perform specific actions when clicked.
Check Boxes	A check box is selected or cleared to: • Enable or disable a feature • Initiate functions for list items Some lists include a **Select All** check box for selecting all items, including overflow items.
Radio Buttons	Select the button to select an item.
Sort	Data presented in tables can be sorted by clicking column headers. Columns can be sort in the following orders: • Ascending (default) • Descending
Mouseovers	Move your mouse over an item to display a text description.
Auto Refresh	Some pages feature an **Auto Refresh** check box. Select the check box to automatically refresh the page every 15 seconds.
Scrollbars	Drag scrollbars to see additional data.
Tabs	Select different tabs to display hidden information.
Bread Crumb	Displays the path to the page you are viewing. The breadcrumb lists: • The page you are viewing • Its parent page (if applicable) • The **Navigation Menu** item used to open the page If the breadcrumb contains a link, you can click it to retrace your steps.

Tip: Most pages support right-click.

The Navigation Menu

This menu appears on all Ivanti Endpoint Security pages. Use this menu to navigate through the console.

This menu organizes product features based on functionality. When you select a menu item, a new page, dialog, wizard, or window opens. You can access all system features from this menu (that your access rights authorize).

Note: The menu items available change based on modules you install.

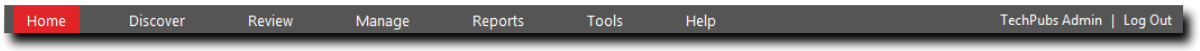


Figure 1: Navigation Menu

Table 2: Navigation Menus

Menu	Description
Home	Opens the ***Home*** page. This link contains no menu items.
Discover	Contains menu items related to running discovery scan jobs and virus and malware scans.
Review	Contains menu items related to reviewing security content, application event logs, virus and malware events, and discovery scan jobs.
Manage	Contains menu items related to managing system features.
Reports	Contains menu items related to creating reports.
Tools	Contains menu items related to system administration.
Help	Contains menu items related to help systems.

Mobile Device Management adds new **Navigation Menu** items.

Most navigation menus contain items. The following table lists each menu item in the **Discover** menu and the actions that occur when they are selected.

Table 3: Discover Menu Items

Menu Item	Description
Assets...	The ***Discover Assets*** dialog.
Assets and Install Agents...	The ***Install Agents*** dialog.
Assets and Uninstall Agents...	The ***Uninstall Agents*** dialog.

Menu Item	Description
Scan Now - Virus and Malware Scan	The ***Virus and Malware Scan*** dialog.

The following table lists each menu item in the **Review** menu and the actions that occur when they are selected.

Table 4: Review Menu Items

Menu Item	Description	
Custom Patch Lists	Opens a sub-menu. The sub-menu contains the following items.	
	Create Custom Patch List	The ***Create Custom Patch List*** dialog.
	Custom Patch List	The **Custom Patch Lists** sub-menu lists the last five custom patch lists that you have edited.
	All Lists	If you have created more than five custom patch lists, the navigation menu lists an **All Lists** item, which will open the ***Patch Content*** page with all custom patch lists displayed.
My Default View	The ***All Content*** page with your saved filters.	
Vulnerabilities	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show only critical vulnerabilities.
	Critical Vulnerabilities	The ***Patch Content*** page, filtered to show only critical vulnerabilities that are not superseded.
	New Vulnerabilities	The ***Patch Content*** page, filtered to show only critical but not superseded vulnerabilities released in the last 30 days.
	Top Vulnerabilities	The ***Patch Content*** page, filtered to show only critical but not superseded vulnerabilities sorted by the greatest number of applicable endpoints that are not patched.

Menu Item	Description	
Software	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show all software.
	Service Packs	The ***Patch Content*** page, filtered to show only service packs.
	Software Installers	The ***Patch Content*** page, filtered to show only software installers.
	Updates	The ***Patch Content*** page, filtered to show only software updates.
Other	Opens a sub-menu. The sub-menu contains the following items:	
	All	The ***Patch Content*** page, filtered to show all non-critical content.
	Detection Only	The ***Patch Content*** page, filtered to display **Detection Only** content.
	Informational	The ***Patch Content*** page, filtered to display only **Information** content.
	Packages	The ***Patch Content*** page, filtered to display only **Packages** content.
	Policies	The ***Patch Content*** page, filtered to display only **Policies** content.
	Recommended	The ***Patch Content*** page, filtered to display only **Recommended** content.
	System Management	The ***Patch Content*** page, filtered to display only **System Management** content.
	Tasks	The ***Patch Content*** page, filtered to display only **Task** content.
	Virus Removal	The ***Patch Content*** page, filtered to display only **Virus Removal** content.
Asset Discovery Job Results	Opens the ***Job Results*** page, which is filtered to display discovery job results.	
Agent Management Job Results	Opens the ***Job Results*** page, which is filtered to display Agent Management Job results.	

Menu Item	Description
Virus and Malware Event Alerts	Opens the ***Virus and Malware Event Alerts*** page.
Application Control Log Queries	Opens the ***Application Control Log Queries*** page, which allows users to create log queries that extract information on application activity.
Device Event Log Queries (Device Control only)	Opens the ***Device Event Log Queries*** page, which you can use to create, edit, or review device event log queries.

The following table lists each menu item in the **Manage** menu and the actions that occur when they are selected.

Table 5: Manage Menu Items

Menu Item	Description	
Endpoints	Opens the ***Endpoints*** page.	
Mobile Endpoints	Opens the ***Mobile Endpoints*** page.	
Inventory	Opens the ***Inventory*** page.	
Groups	Opens the ***Groups*** page.	
Users	Opens the ***Users*** page.	
Custom Patch Lists	Opens a sub-menu. The sub-menu contains the following items.	
	Create Custom Patch List	The ***Create Custom Patch List*** dialog.
	Custom Patch List	The **Custom Patch Lists** sub-menu lists the last five custom patch lists that you have edited.
	All Lists	If you have created more than five custom patch lists, the navigation menu lists an **All Lists** item, which will open the ***Patch Content*** page with all custom patch lists displayed.
Deployments and Tasks	Opens the ***Deployments and Tasks*** page.	
Agent Policy Sets	Opens the ***Agent Policy Sets*** page.	
Mobile Policies	Opens the ***Mobile Policies*** page.	
Antivirus Policies	Opens the ***Antivirus Policies*** page.	

Menu Item	Description	
Application Control Policies	Opens the ***Application Control Policies*** page, which contains the following tabs:	
	Managed Policies	Managed policies include Easy Auditor, Easy Lockdown, Denied Applications Policy, and Supplemental Easy Lockdown/ Auditor Policy. This tab is selected by default.
	Trusted Change	Trusted change policies include Trusted Publisher, Trusted Path, Trusted Updater, and Local Authorization.
	Memory Injection Policies	Memory Injection Policies.
Device Control: Policies (Device Control only)	Opens the ***Device Control Policies*** page, which you use to create, edit, or review Device Control policies.	
Policy Wizards	Opens a sub-menu. The sub-menu contains the following items:	
	Easy Auditor...	The ***Easy Auditor*** wizard.
	Easy Lockdown...	The ***Easy Lockdown*** wizard.
Application Library (Application Control only)	Opens the ***Application Library*** page, which lists the applications and files on your network endpoints.	
Device Library (Device Control only)	Opens the ***Device Library*** page, which lists all devices on your network endpoints.	

The following table lists each menu item in the **Reports** menu and the actions that occur when they are selected.

Table 6: Reports Menu Items

Menu Item	Description
All Reports	Opens the ***All Reports*** page.
AntiVirus	Opens the ***All Reports*** page with antivirus reports expanded.
Configuration	Opens the ***All Reports*** page with configuration reports expanded.
Deployments	Opens the ***All Reports*** page with deployments reports expanded.

Menu Item	Description
Device Control (Device Control only)	Opens the ***All Reports*** page with Device Control reports expanded.
Inventory	Opens the ***All Reports*** page with inventory reports expanded.
Management/Status	Opens the ***All Reports*** page with management/status reports expanded.
Policy and Compliance	Opens the ***All Reports*** page with policy and compliance reports expanded.
Power Management (Power Management only)	Opens the ***All Reports*** page with Power Management reports expanded.
Risks	Opens the ***All Reports*** page with risks reports expanded.
Vulnerabilities/Patch Content	Opens the ***All Reports*** page with vulnerabilities/patch content reports expanded.
Enhanced Reports	Opens a custom, user-defined URL. This URL is usually used to open a third-party reporting Web page.

The following table lists each menu item in the **Tools** menu and the actions that occur when they are selected.

Table 7: Tools Menu Items

Menu Item	Description
Users and Roles	Opens the ***Users and Roles*** page.
Change My Password...	Opens the ***Change My Password*** dialog.
Download Agent Installer...	Opens the ***Download Agent Installer*** dialog opens over the currently selected page.
Wake on LAN	Opens the ***Wake on LAN*** page.
Power Management (Power Management only)	Opens the ***Power Management*** page.
Directory Sync Schedule	Opens the ***Directory Sync Schedule*** page.

Menu Item	Description	
Device Control Device Control only)	Opens the **Device Control** submenu. The submenu includes the following items:	
	Recover Password	Opens the ***Recover Password*** dialog, which you can use to help network users recover forgotten passwords for encrypted devices.
	Grant Temporary Permissions	Opens the ***Grant Temporary Permissions*** dialog, which you can use to extend network users temporary access to certain network devices.
Launch Installation Manager...	Opens the ***Installation Manager*** in a new window.	
Subscription Updates	Opens the ***Subscription Updates*** page.	
Mobile Management Setup	Opens the ***Mobile Management Setup*** page.	
Mobile Endpoint Registration	Opens the ***Mobile Endpoint Registration*** dialog.	
Email Notifications	Opens the ***Email Notifications*** page.	
Options	Opens the ***Options*** page.	

The following table lists each menu item in the **Help** menu and the actions that occur when they are selected.

Table 8: Help Menu Items

Menu Item	Description
Help Topics...	Opens the ***Help*** page.
Knowledge Base...	Opens the Ivanti knowledge base.
New Users Start Here...	Opens the ***New Users Start Here*** page.
Technical Support	Opens the ***Technical Support*** page.
Product Licensing	Opens the ***Product Licensing*** page.

Menu Item	Description
About...	Opens the ***About*** dialog.

Note: Any unavailable or absent menus, menu items, or sub-menu items are due to restricted access rights or unavailable modules. Contact your network administrator if you require access to unavailable features.

The Page Banner

A page banner displays when the page is added for a new module. Use this banner to identify the module that the page belongs to.

Figure 2: Page Banner

For example, pages for Ivanti Patch and Remediation display a Patch and Remediation page banner. Page banners are color-coded by module.

List Pages

Most pages feature lists of selectable items. These items represent different product features that can be edited using menus and buttons.

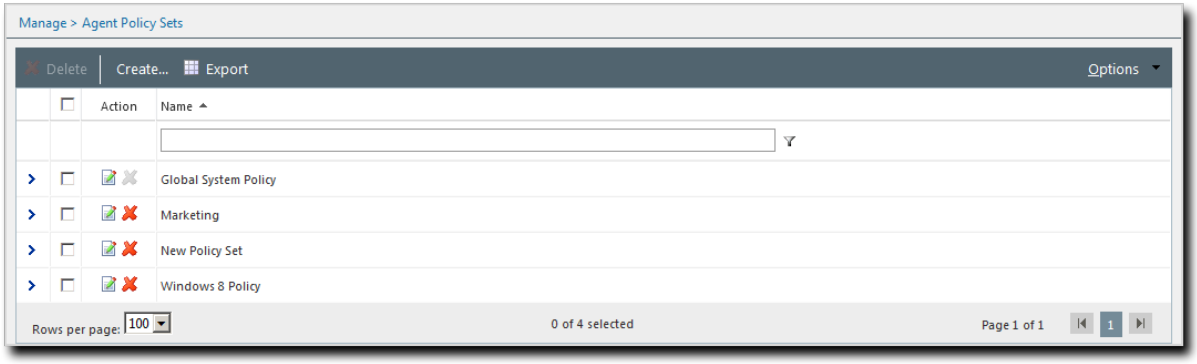


Figure 3: List Page

To select a single list item:

- Select a check box.
- Click a list row.

To select multiple list items:

- Select the **Select All** check box.
- Select multiple, concurrent items by using `SHIFT+Click` and mousing over list rows.

Toolbars

Toolbars appear on most Web console pages. They contain menus and buttons you can use to initiate page features.

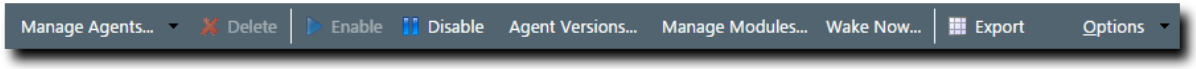


Figure 4: Toolbar

- The menus and buttons displayed vary according to page.
- Click the available menus and buttons to use them.
- User roles determine which buttons are available.

The Options Menu

Toolbars feature an **Options** menu. You can use these options to change how the page displays information.

Table 9: Options Menu Items

Option	Description
Show results on page load	Toggles automatic page results on and off. • When enabled, the page list automatically populates with results. • When disabled, you must define page filters and click **Update View** before results populate. For more information, see Filters on page 36.
Save as default view	Saves the current page settings as the default view.
Clear default view	Resets the saved view to the system default.
Show Filter Row[1]	Toggles the **Filter Row** on and off. For additional information, refer to Using Filter Rows on page 38
Show Group By Row[2]	Toggles the **Show Group By Row** on and off. For additional information, refer to Group By on page 40.
Enable Copy to Clipboard[3]	Toggles the ability to select text for clipboard copy.

1. This option title changes to **Hide Filter Row** when toggled.
2. This option title changes to **Hide Group By Row** when toggled.
3. Selecting this option disables other features, such as right-click context menus and list item dragging.

Filters

Filters appear on most list pages. You can use them to search pages for specific data.

Depending on which page you are viewing, you can filter pages using one of the following features. Only one feature appears per page.

- Filters
- Filter Row

Filters appear above page lists. They feature different fields, lists, and check boxes used for filtering. Filters vary according to page.

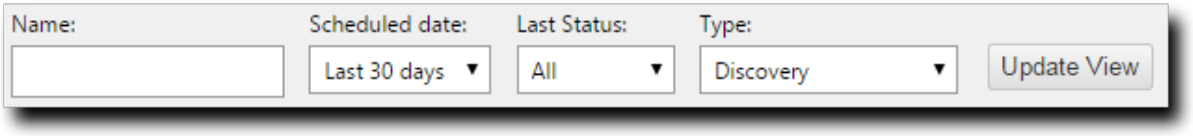


Figure 5: Filters

You can save frequently used filter settings as your default view. To save your settings, select **Options** > **Save as default view** from the toolbar. The toolbar **Options** menu contains the following options for filtering.

Table 10: Filter Options

Option	Function
Show results on page load	Automatically retrieves and displays results when selected.

Save as default view	Saves the active filter and sort criteria as the default view for the page.
	• The default view displays each time the page is accessed, including the following events:
	  • Browsing to a different page.
	  • Logging out of the Web console.
	• The default view is saved until you save a new one or you clear it.

Clear default view	Resets a saved default view to the system default view.

Filter Rows

Filter rows appear in the lists themselves. Rows feature a field for each column.

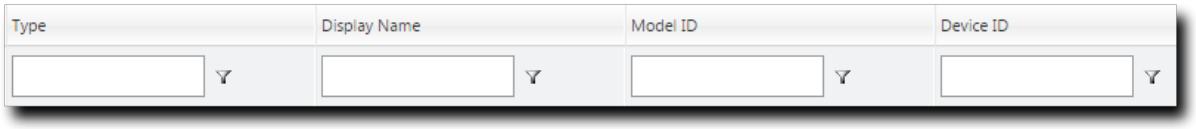


Figure 6: Filter Row

- Filters are not case sensitive.
- Columns can be filtered using a variety of data types. For example, you can use a **Contains** filter or a **StartsWith** filter.
- Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.

Supported Wildcards
When searching for or filtering vulnerabilities, you can use wildcards to make search results more specific and efficient.

Wildcards can be used anywhere within the search string. The following table lists the supported operators and wildcards in Ivanti Endpoint Security. Type any wildcards that you intend to use in the **Name or CVE-ID** field.

Table 11: Supported Wildcards

Wildcard	Description	Example
%	Any string. The string can be empty or contain any number of characters.	Typing `Microsoft%Server` in the **Name or CVE-ID** field returns any vulnerability with the words *Microsoft* and *Server* in any part of the name, such as: • MS12-043 Security Update for **Microsoft** Office SharePoint **Server** 2007 32-Bit Edition (KB2687497) • The 2007 **Microsoft** Office **Server**s Service Pack 3 (SP3), 32-bit Edition (KB2526299)
_ (underscore)	An underscore can be used as a Wildcard placeholder for any single character.	Typing `_itrix` or `Citri_` in the **Name or CVE-ID** field returns any vulnerabilities with *Citrix* in the name.
[ ]	Any single character within the brackets. You can also type a range ([a-f]) or set ([acegik]).	Typing `[m]ic` in the **Name or CVE-ID** field returns vulnerabilities with the string *mic* within the name (*Microsoft* and *Dynamic*). Typing `200[78]` in the **Name or CVE-ID** field returns vulnerabilities with 2007 or 2008 within the name.

Wildcard	Description	Example
[^]	Any single character **not** specified within the brackets. You can also type a range ([^a-f]) or set ([^acegik]).	Typing `M[^i]cro` in the **Name or CVE-ID** field returns results that: • Replace *i* with all remaining alphanumeric and symbolic characters (a, $, and so on). • Include all other characters remaining in the string (m, c, r, o). Results would include Macro, Mecro, M$cro, and so on. If a vulnerability contains Micro and a valid combination like Macro in its name (e.g. `MS99-999 Microsoft Word 2010 Vulnerability Could Enable Macros to Run Automatically`), it will be returned in the results.

Using Filters
When list pages are overpopulated with items, use filters to search for specific list items. Use this feature to filter list pages by criteria specific to the page.

Filters are available on most list pages.

1. Select a list page. For additional information, refer to List Pages on page 34.
2. Ensure filters are displayed.
   If filters are not displayed, click **Show Filters**.
3. Define filter criteria.

   Note: Available filters differ by page.

   - In filter fields, type the desired criteria.
   - From filter lists, select the desired list item.
4. If applicable, select the **Include sub-groups** check box.

   Note: This check box only appears on list pages related to groups.
5. Click **Update View**.

   Step Result: The list is filtered according to the filter criteria.
6. [Optional] Save the filter criteria by selecting **Options** > **Save as default view** from the toolbar.

Using Filter Rows
Some list pages use filter rows rather than filters. Use these rows, which are the first row of applicable lists, to filter column results. Filter column results to search for specific list items.

These rows appear on several list pages.

1. Select a page featuring the filter row.
2. Ensure the filter row is displayed.
   a) If the filter row is not displayed, select **Options** > **Show Filter Row** from the toolbar.
3. Type criteria in a filter row field.
4. Apply a filter type.
   a) Click the **Filter** icon.

      Step Result: A menu opens.

   b) Select a filter type.

      The following table describes each filter type.

      Table 12: Data Filtering Types

Type	Description
NoFilter	Removes previously applied filtering.
Contains	Returns results that contain the value applied to the filter.
DoesNotContain	Returns results that do not contain the value applied to the filter.
StartsWith	Returns results that start with the value applied to the filter.
EndsWith	Returns results that end with the value applied to the filter
EqualTo	Returns results equal to the value applied to the filter.
NotEqualTo	Returns results that are not equal to the value applied to the filter.
Greater Than	Returns results that are greater than the value applied to the filter.
Less Than	Returns results that are less than the value applied to the filter.
GreaterThanOrEqualTo	Returns results that are greater than or equal to the value applied to the filter.
LessThanOrEqualTo	Returns results that are less than or equal to the value applied to the filter.
Between	Returns results that are between two values. Place a space between the two values.
NotBetween	Returns results that are not between two values. Place a space between the values.
IsEmpty	Returns results that are empty.
NotIsEmpty	Returns results that are not empty.
IsNull	Returns results that have no value.

Type	Description
NotIsNull	Returns results that have a value.

Note:

- Filters are not case sensitive.
- Date columns filter at the lowest level of granularity. Higher levels of granularity return no filter results.
- The availability of filtering options depends on the type of data displayed in the column. For example, filtering options that can only apply to numeric data are available in columns that contain text data.

Result: The list column is filtered according to the criteria. If desired, repeat the process to filter additional columns.

Using a Custom Date Range Filter

Use the Custom Date Range filter on Virus and Malware Event pages and tabs to display events that have occurred over a specific time period.

Prerequisites:

You must have launched the **Custom Date Range** dialog from the **Last Date Detected** filter field of a Virus and Malware Event page or tab.

1. Enter Start and End dates and times that cover the period you want to view alerts for, then click **OK**.

   Calendar and Time View popups can be opened to facilitate the entry of dates and times. Times that can be selected are provided in 30-minute intervals.

   Note: Your Start date should be less than 90 days from the current date, as event alerts raised outside that range are removed from view.

2. Click **Update View** to display the filtered results.

Result: The list is filtered according to the custom date range criteria you entered. Last Detected Dates are always displayed using server time.

Tip: As Malware and Virus Event alerts can be removed from view, the results list may not display all alerts that occurred within your custom date range. However, removed alerts are not deleted from the database and can therefore be viewed by generating an appropriate report.

Group By

The **Group By** row lets you sort list items into groups based on column headers. Use this feature to see which list items share similarities.

To use the **Group By** row, ensure **Options** > **Show Group By Row** is selected from the toolbar, and then drag a column header into the row. You may drag multiple columns to the row, but you may only drag one column into the row at a time.

To ungroup the list, right-click on the row and select **Cancel All Groupings**. To hide the **Group By** row, select **Options** > **Hide Group By Row**.

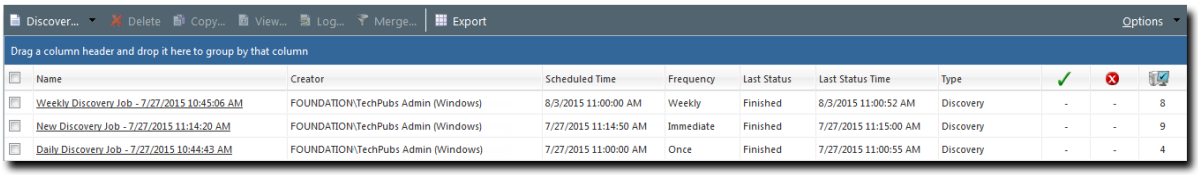


Figure 7: Group By Row

Expanding and Collapsing Structures

Certain structures in the Web console are expandable and collapsible. Expand structures to view additional information or options. Collapse them to conserve screen space.

Click available **Plus** icons (+), **Minus** icons (-), and **Rotating Chevron** icons (>) to expand or collapse a structure.

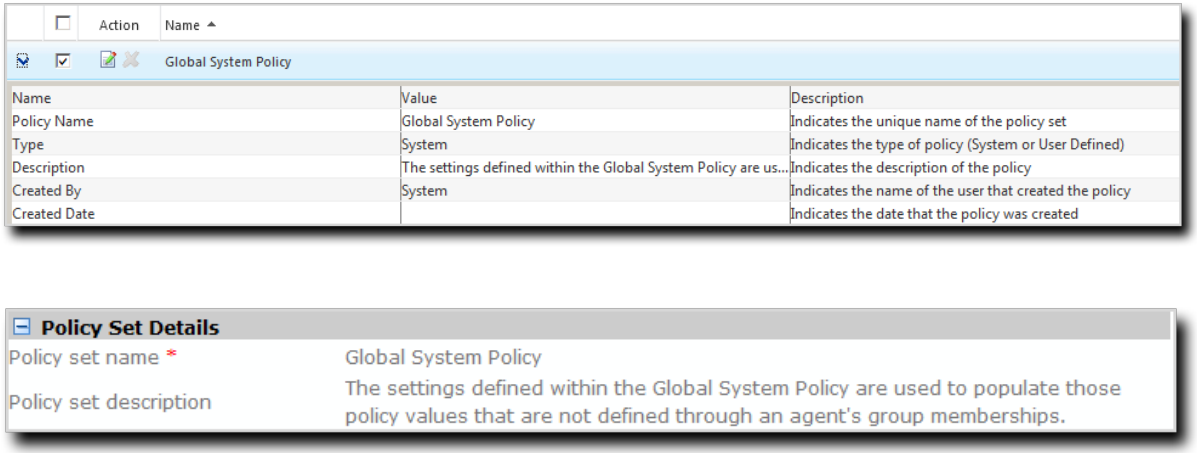


Figure 8: Expandable Structure Examples

Advancing Through Pages

When a list page contains an overflow of items, pagination links are created to manage the overflow. Click these links to advance through list items.

The number of list items and the page you are viewing determines the number of pagination links.

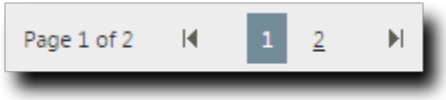


Figure 9: Pagination Feature

Table 13: Pagination Feature Functions

Icon or Link	Title	Function
	**Final Page Link**	Advances to the final page of list items.
	**First Page Link**	Returns to the first page of list items.
...	**Next Ten/Previous Ten Pages Link**	Displays the next ten or previous ten page links available. Fewer page links will display if the remaining list items cannot populate ten pages.
1 2 3 4 5	**Pagination Links**	Advances or returns to the selected pagination link.

Each page also features a **Rows Per Page Drop-Down List**. This list modifies the number of list items displayed on a single page (25, 50, 100, 200, 500).

Help

Ivanti Endpoint Security contains context-sensitive HTML help that includes feature explanations, step-by-step procedures, and reference materials.

Accessing Help differs according to context.

- From a page, select **Help** > **Help Topics**.
- From a dialog, click the **Question Mark** icon (**?**).

Use the following features to navigate through Help:

- From the ***Content*** tab, expand the bookmarks and click links to display Help topics.
- From the ***Search*** tab, type criteria in the **Keywords** field and click **Search** to display Help topics related to your search.

Exporting Data

On many system pages, you can export the listed data to a comma-separated value file (`.csv`) available for use outside of the Web console. Use this exported data for management purposes (reporting, noting trends, and so on).

You can export data from a variety of pages.

Important: The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.

1. Open a system page or dialog that you can export information from.
2. [Optional] Use the page filters to refine the items listed.
3. Click **Export**.

   Step Result: The ***File Download*** dialog opens.
4. Use the browser controls to complete the data export.

Result: The data is exported. All data results export, including data on overflow pages.

The Home Page

The entry point to Ivanti Endpoint Security is the ***Home Page***. From this page you can view the dashboard, which features drag-gable widgets that display information about Ivanti Endpoint Security and agent-managed endpoints.

Some widgets display general information about the system, others provide links to documentation, and still others summarize activity for Ivanti Endpoint Security modules you are licensed for.

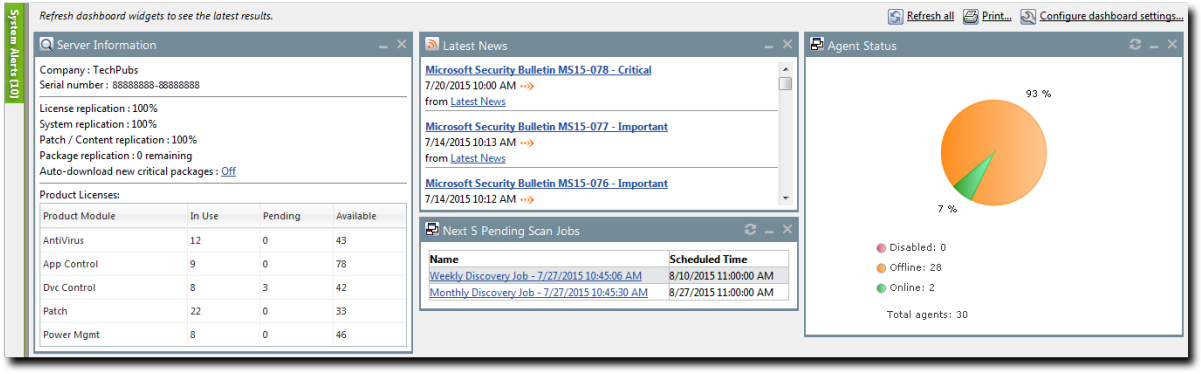


Figure 10: The Home Page

The Dashboard

The **dashboard** displays widgets depicting the activity on your protected network. Located on the ***Home*** page, the dashboard provides convenient information you can use to ensure your network protection is up to standard. Additionally, you can customize the dashboard to display the widgets most applicable to your network environment.

Widget graphs are generated based on the latest data and statistics available from endpoints, groups, module-specific data, and so on.

The following ***Dashboard*** widgets are available:

The Agent Module Installation Status Widget

This widget displays the installation and licensing stats of each agent module.

A graph bar displays for each installed module. The following table describes the widget graph.

Table 14: Graph Bar Color Descriptions

Bar Color	Description
Blue	The number of endpoints with the module pending install or uninstall.
Green	The number of endpoints with the module installed.
Red	The number of endpoints without the module installed.

Tip: Click the graph to open the ***Endpoints*** page.

Note: Endpoints with an agent version that does not support a module are not counted.

The Agent Status Widget

This widget displays all agents grouped by agent status.

Table 15: Agent Status Widget Fields

Field	Description
Online	The number of agents that are online.
Offline	The number of agents that are offline. **Tip:** Offline status is determined by the amount of time since the agent last communicated as determined on the ***Options*** page.
Disabled	The number of agents that are disabled.
Total Agents	The total number of agents in your environment.

Tip: Click the graph to open the ***Endpoints*** page. The page is filtered to display all agents.

The Applicable Content Updates Widget

This widget displays applicable content updates grouped by content type. View this widget when determining what content is applicable to endpoints in your network.

Table 16: Applicable Content Updates Widget Graph Bars

Bar	Description
Critical	The number of critical content items that are applicable to the your endpoints.

Bar	Description
Recommended	The number of recommended content items that are applicable to your endpoints.
Optional	The number of optional software, informational, and virus removal content items that are applicable to your endpoints.

Tip: Click the widget graph to open the ***Content*** page, which is filtered to display all applicable non-patched content.

Table 17: Applicable Content Updates Widget Fields

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.
Endpoints	The total number of endpoints with applicable updates.

Note:

- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.
- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

The Critical Patch Status by Endpoint Widget
This widget depicts the patch status of all managed endpoints. Each bar indicates the number of managed endpoints with applicable vulnerabilities within a given release date range.

The following table describes the **Critical Patch Status By Endpoint** widget. Green bars indicate endpoints that are patched for critical vulnerabilities, while red bars indicate endpoints that are not patched for critical vulnerabilities.

Table 19: Critical Patch Status By Endpoint Bars

Graph Bar	Description
<30 days	The number of endpoints with applicable critical vulnerabilities fewer than 30 days old.
30 - 120 days	The number of endpoints with applicable critical vulnerabilities between 30 to 120 days old.
>120 days	The number of endpoints with applicable critical vulnerabilities greater than 120 days old.

The following table describes the widget fields.

Table 20: Critical Patch Status By Endpoint Fields

Field	Description
Endpoints	The total number of endpoints with applicable critical vulnerabilities.
Critical vulnerabilities	The total number of critical vulnerabilities applicable to your environment.

Tip: Click the graph to open the ***Critical Vulnerabilities*** content page.

Note:

- If an endpoint is marked as *Do Not Patch* for a critical vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved critical vulnerabilities.
- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the **Critical vulnerabilities** count.

The Discovery Scan Results: Agents Widget
This widget displays the number of endpoints capable of hosting agents discovered in the latest Discovery Scan Job. The endpoints are classified in to two groups: endpoints with agents and endpoints without agents.

Table 21: Discovery Scan Results: Agents Widget Fields

Field	Description
As of	The name of the Discovery Scan Job used to generate the widget graph and statistics. This job is the job most recently run.
Endpoints with agents	The number of agent-compatible endpoints discovered that have agents installed.
Endpoints without agents	The number of agent-compatible endpoints discovered that have no agents installed.
Endpoints	The total number of agent-compatible endpoints discovered.

Tip: Click the widget to open the ***Results*** page for the most recently run Discovery Scan Job.

The Endpoints with Unresolved Updates Widget
This widget displays all endpoints with unapplied applicable content updates, grouped by content type. View this widget when determining if an endpoint requires deployment.

An unresolved update is an occurrence of an endpoint that has not had an applicable content item installed.

Bar	Description
Critical	The number of endpoints that have unresolved critical content updates.
Recommended	The number of endpoints that have unresolved recommended content updates.
Optional	The number of endpoints that have unresolved software, informational, and virus removal content updates.

Tip: Click a widget graph bar to open the ***Content*** page, which is filtered to display all unapplied applicable content.

Field	Description
Endpoints	The number of endpoints with applicable updates within your network.

Field	Description
Applicable updates	The total number of content items applicable to your endpoints.

Note:

- If an endpoint is marked as *Do Not Patch* for an applicable update, that update is no longer considered applicable. Therefore, that endpoint is only included in the graph bars and the **Endpoints** count if it has other unresolved updates.
- Updates that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Applicable updates** count.
- Updates that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Applicable updates** count.

The Incomplete Deployments Widget

This widget displays all deployments with elapsed start dates and a status of *not started* or *in progress*.

Table 22: Incomplete Deployment Widget Fields

Field	Description
<25%	The number of deployments that are less than 25 percent complete. This field includes deployments that have not started.
25% - 49%	The number of deployments that are 25 to 49 percent complete.
50% - 69%	The number of deployments that are 50 to 69 percent complete.
70% - 79%	The number of deployments that are 70 to 79 percent complete.
80% - 89%	The number of deployments that are 80 to 89 percent complete.
>90%	The number of deployments that are more than 90 percent complete.
Total	The total number of deployments that have a status of *in progress* or *not started* with an elapsed start time.
Total affected endpoints	The total number of endpoints receiving pending or in-progress deployments.

The Last 5 Completed Scan Jobs Widget

This widget contains information about the last five completed discovery scan jobs. Each job name is a link to the associated ***Result*** page.

Table 23: Last 5 Completed Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the name to open the ***Results*** page for the job.

Column	Description
Completed Date	The date and time the job completed on the server.
Status	The status of the completed job.

The Latest News Widget
This widget displays important announcements and other information in Ivanti Endpoint Security.

Click a link to view additional details about an announcement.

The Mandatory Baseline Compliance Widget
This widget displays the Mandatory Baseline status for all endpoints that have the Patch and Remediation module installed.

Table 24: Mandatory Baseline Compliance Widget Fields

Field	Description
Compliant	The number of endpoints with all Mandatory Baseline content installed. **Note:** Endpoints that don't have Mandatory Baseline content installed that's marked *Do Not Patch* are considered compliant.
In process	The number of endpoints currently downloading Mandatory Baseline content.
No baseline	The number of endpoints with no content assigned to their Mandatory Baselines.
Non compliant	The number of endpoints that do not have all content in their Mandatory Baselines installed.
Total number of endpoints	The number of endpoints with an agent installed.

The Mobile Endpoint Last Check In Widget
This widget displays your mobile endpoints, which are grouped by the duration or their last check in.

The total number of mobile endpoints is grouped into six different time categories. Click the graph to open the ***Mobile Endpoints*** page, which will be sorted by date with the oldest endpoints listed on top.

Graph Bar	Description
1 day (Green)	The number of mobile endpoints that last checked in one day ago.
2 days (Light Green)	The number of mobile endpoints that last checked in two days ago.
3 days (Blue)	The number of mobile endpoints that last checked in three days ago.
4-7 days (Yellow)	The number of mobile endpoints that last checked in four to seven days ago.

Graph Bar	Description
8-14 days (Orange)	The number of mobile endpoints that last checked in 8 to 14 days ago.
14+ days (Red)	The number of mobile endpoints that last checked in 14 days ago or more.

The Mobile Endpoint Status Widget
This widget shows the last known status of all registered mobile endpoints. A pie chart displays the percentage of endpoints in each status.

Status	Description
Online	The number of endpoints that have checked in within the set communication interval without issue.
Online Jailbroken	The number of jailbroken iOS endpoints that have checked in within the set communication interval.
Online Rooted	The number of rooted Android endpoints that have checked in within the set communication interval.
Offline	The number of endpoints that have not checked in within the set communication interval.
Disabled	The number of disabled mobile endpoints.
Unmanaged	The number of mobile endpoints that have their profile removed or the app uninstalled.
Expired	The number of endpoints issued an expired license.
Wiped	The number of endpoints that have been sent a command to revert to factory settings.
Total mobile endpoints	The total number of mobile endpoints registered with Ivanti Endpoint Security.

Tip: Click an endpoint status to open the ***Mobile Endpoints*** page, which is filtered to display the clicked endpoint status.

The Mobile Endpoints with Policy Widget
This chart displays all mobile endpoints and their policy assignment status.

This table describes each widget bar.

Bar	Description
No Policy	The number of mobile endpoints that have no policy assignments.

Bar	Description
Blocked	The number of mobile endpoints that have policy assignments that are not being enforced because the endpoint has a status of **Unmanaged**, **Offline**, or **Expired**.
Pending	The number of mobile endpoints that have had a policy assignment that has not yet been applied.
Applied	The number of mobile endpoints that have a policy assignment applied successfully.

The Next 5 Pending Scan Jobs Widget
This widget displays information about the next five pending discovery scan jobs.

Table 25: Next 5 Pending Scan Jobs Widget Columns

Column	Description
Name	The job name. Click the link to view the ***Discovery Scan Jobs*** page ***Scheduled*** tab.
Scheduled Time	The date and time the job is scheduled for on the server.

Tip: Click a job name link to view the ***Discovery Scan Jobs*** page ***Scheduled*** tab.

The Offline Patch Endpoints Widget
This widget displays all offline Patch and Remediation endpoints. These endpoints are grouped by time ranges since they last checked in.

Table 26: Offline Agents Widget Fields

Field	Description
< 48 hours	The number of Patch and Remediation endpoints offline fewer than 48 hours.
48 - 72 hours	The number of Patch and Remediation endpoints offline 48 to 72 hours.
> 72	The number of Patch and Remediation endpoints offline greater than 72 hours.
Total number of offline agents	The number of Patch and Remediation endpoints that are offline (since their last scheduled Discover Applicable Updates task).

Tip: Clicking the **Offline Patch Endpoints** widget pie chart opens the ***Endpoints*** page ***Patch and Remediation*** tab, which is filtered to display offline patch endpoints.

The Patch Agent Module Status Widget

This widget displays all endpoints with the Patch and Remediation module installed, which are grouped by Patch and Remediation status.

Table 27: Patch Agent Module Status Widget Fields

Field	Description
Working	The number of Patch and Remediation endpoints that are working on a deployment task.
Idle	The number of Patch and Remediation endpoints that are idle.
Disabled	The number of Patch and Remediation endpoints that are disabled.
Sleeping	The number of Patch and Remediation endpoints that are sleeping.
Offline	The number of Patch and Remediation endpoints that are offline.
Disabled	The number of Patch and Remediation endpoints that are disabled.
Agents with PR module installed.	The number of endpoints with the Patch and Remediation module installed.
Total Agents	The total number of Patch and Remediation endpoints in your network.

Tip: Click the graph to open the ***Endpoints*** page ***Ivanti Patch and Remediation*** tab.

The Scheduled Deployments Widget

This widget displays endpoints that have not-yet installed applicable content. These endpoints are divided in to two categories: endpoints with deployments scheduled and endpoints with deployments not scheduled. These categories are further divided into three categories: endpoints with not-yet applied critical content, endpoints with not-yet applied recommended content, and endpoints with not-yet applied optional content.

Orange graph bars indicate endpoints that are not scheduled to receive applicable content, while blue graph bars indicate endpoints that are scheduled to receive applicable content.

Table 28: Scheduled Deployments Widget Graph Bars

Graph Bar	Description
Critical	The number of endpoints scheduled or not scheduled to receive deployments for critical content.
Recommended	The number of endpoints scheduled or not scheduled to receive deployments for recommended content.

Graph Bar	Description
Optional	The number of endpoints scheduled or not scheduled to receive deployments for optional content.

Tip: Clicking the **Scheduled Deployments** widget opens the ***Deployments and Tasks*** page, which is filtered to display scheduled deployments.

Table 29: Scheduled Deployments Widget Field

Field	Description
Endpoint with unresolved updates	The number of endpoints with unresolved updates.

The Server Information Widget

This widget lists your serial number, number of licenses available, number of licenses in use, and information about current license usage and availability.

Table 30: Server Information Widget Fields

Field Name	Description
Company	The company your server is registered to as defined during installation.
Serial Number	The license number (serial number) assigned to your server.
License Replication	The subscription status between your server and the Global Subscription Service (GSS).
System Replication	The system replication status between your server and the GSS.
Patch / Content Replication	The replication status between your server and the GSS.
Package Replication	The number of packages remaining for replication.
Auto-download New Critical Packages	The indication of whether your automatically downloads packages for critical vulnerabilities. Click the link to open the ***Subscription Service Configuration*** dialog. For additional information refer to Configuring the Service Tab.

Table 31: Product Licenses Table Columns

Column	Description
Product Module	The module for which you purchased licenses.
In Use	The number of module licenses in use.

Column	Description
Pending	The number of licenses pending use or pending removal. Licenses pending removal become available upon removal completion.
Available	The number of licenses available.

Note: A license expiration notice displays if all available licenses are expired.

The Time Since Last DAU Scan Widget
This widget displays all active agents (not including *disabled* or *offline*) grouped by the amount of time since their last Discover Applicable Updates task.

Table 32: Time Since Last Agent Scan Widget Fields

Field	Description
< 24 hours	The number of agents that last performed a Discover Applicable Updates (DAU) task and checked in fewer than 24 hours ago.
24 - 47 hours	The number of agents that last performed a DAU task and checked in 24 to 47 hours ago.
48 - 72 hours	The number of agents that last performed a DAU task and checked in 48 to 72 hours ago.
> 72 hours	The number of agents that performed a DAU task and last checked in greater than 72 hours ago.
Never checked in	The number of agents that have registered yet have not completed a DAU task.
Total active agents	The total number of active agents.

Tip: Click the **Time Since Last Agent Scan** widget graph to open the ***Endpoints*** page, which is filtered to display enabled endpoints.

The Un-remediated Critical Vulnerabilities Widget
This widget displays the total number of unremediated critical vulnerabilities that are applicable to your environment grouped by age.

Table 33: Un-remediated Critical Vulnerabilities Widget Graph

Graph Bar	Description
<30 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network fewer than 30 days old.

Graph Bar	Description
30 - 120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network that are 30 to 120 days old.
>120 days	The number of unremediated critical but not superseded vulnerabilities applicable in your network greater than 120 days old.

Tip: Click the graph to open the ***Vulnerabilities*** page, which is filtered to display critical but not superseded applicable vulnerabilities.

Table 34: Un-remediated Critical Vulnerabilities Widget Fields

Field	Description
Critical Vulnerabilities	The number of critical but not superseded vulnerabilities applicable in your network.
Endpoints	The number of endpoints with critical but not superseded applicable vulnerabilities.

Note:

- Vulnerabilities that are globally disabled (or marked *Do Not Patch* for *all* endpoints) are excluded from the widget bars and **Critical vulnerabilities** count.
- Vulnerabilities that are marked *Do Not Patch* for at least one endpoint (but not all) are still included in the widget bars and **Critical vulnerabilities** count.
- If an endpoint is marked as *Do Not Patch* for an applicable vulnerability, that vulnerability is no longer considered applicable. Therefore, that endpoint is only included in the **Endpoints** count if it has other unresolved updates.

The Endpoints with Unresolved AV Alerts Widget

This widget displays the number of endpoints with unresolved antivirus event alerts.

There are two types of unresolved antivirus event alerts, *not cleaned* and *quarantined*. If an endpoint has multiple not cleaned event alerts, it is counted only once in the **Not Cleaned** column. Likewise, if it has multiple quarantined event alerts, it is counted only once in the **Quarantined** column. However,

if an endpoint has both not cleaned and quarantined event alerts, it is counted twice (once in each column).

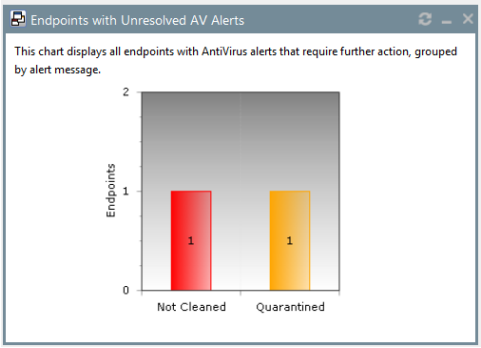


Figure 12: Endpoints with Unresolved AV Alerts Widget

The following table describes each graph bar.

Bar	Description
Not Cleaned	The number of endpoints with not cleaned event alerts.
Quarantined	The number of endpoints with quarantined event alerts.
Tip: Clicking a widget graph bar opens the ***Virus and Malware Event Alerts*** page, which is filtered on the endpoint name.	

The Top 10 Infected Endpoints Widget
This widget displays the 10 endpoints which have received the most event alerts in the last 10 days, and a breakdown of each endpoint's alert status.

The widget lists all event alert types, including cleaned, not cleaned, deleted, and quarantined.

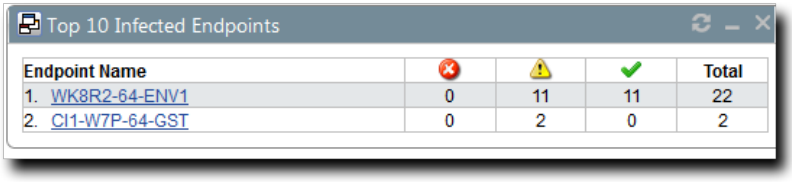


Figure 13: Top 10 Infected Endpoints Widget

The following table describes each column in the widget.

Column	Description
Endpoint Name	The name of the endpoint, with a link to its ***Details*** page.
Not Cleaned	The number of alerts on the endpoint where it was not possible to clean a suspect file.

Column	Description
Quarantined	The number of alerts on the endpoint where the file was moved to quarantine.
Cleaned	The number of alerts on the endpoint where a file was successfully cleaned.
Deleted	The number of alerts on the endpoint where a suspect file was deleted.
Total	The total number of all alerts on the endpoint. This is the number on which the ranking of the list is based.

The Top 10 Virus/Malware Threats Widget

This widget displays the 10 types of virus or malware that have generated the most event alerts in the last 10 days.

The malware types are listed from the top down in descending order of frequency, and the number of endpoints affected is displayed along the bottom of the widget.

Note: The display is based on the number of event alerts generated by each virus/malware type, regardless of how the event was handled (cleaned, not cleaned, deleted, or quarantined).

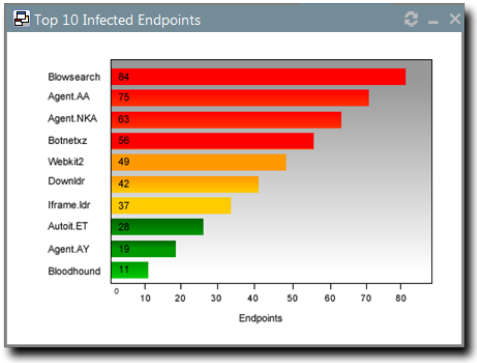


Figure 14: Top 10 Virus/Malware Threats

Clicking on any virus/malware bar will bring you to its ***Virus/Malware Details*** page.

The Estimated Energy Savings: Daily Widget

This widget displays the energy savings for the previous day. This calculation is based on your endpoints actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

Table 35: Estimated Energy Savings: Daily Widget Fields

Field	Description
Results for the day of	The date for which the widget displays the results.
Desktop count	The number of monitored desktops.

Field	Description
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Estimated Energy Savings: Weekly Widget
This widget displays the energy savings of the past seven days based on your endpoints' actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

Table 36: Estimated Energy Savings: Weekly Widget Fields

Field	Description
Results for the week from	The dates for which the widget displays the results.
Desktop count	The number of monitored desktops.
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Estimated Energy Savings: Monthly Widget

This widget displays the energy savings of the past 30 days based on your endpoints actual power consumption compared to the energy usage if the same endpoints were in an always-on state.

The following table describes the fields in the **Estimated Energy Savings: Monthly** widget.

Table 37: Estimated Energy Savings: Monthly Widget Fields

Field	Description
Results for the month from	The month for which the widget displays the results.
Desktop count	The number of monitored desktops.
Total usage	The percentage of time that the monitored desktops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for desktops.
Laptop count	The number of monitored laptops.
Total usage	The percentage of time that the monitored laptops are switched on versus desktops in an always-on state. The value in parenthesis is the kilowatt hours of electricity used.
Total savings	The total savings amount for laptops.

The Device Control Denied Actions Widget

This widget displays the users with the highest number of actions blocked by device control policies. View this widget when determining the lists of users for whom action block occurred due to the device control policies.

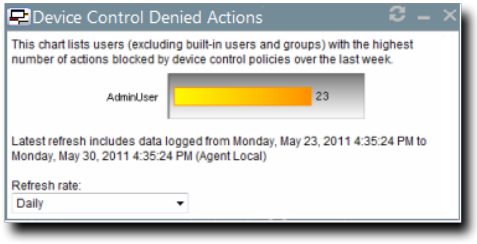


Figure 15: Device Control Denied Actions Widget

The chart displays the users with the highest number of actions blocked by device control policies. The widget can displays five users with the highest number of actions blocked by device control policies.The count on the bar displays the number of times the user actions were blocked by the device control policies.

The Devices Connected to Endpoints Widget

This widget displays the number of peripheral device classes that were connected to endpoints. View this widget when determining which devices were connected to endpoints over the last week.

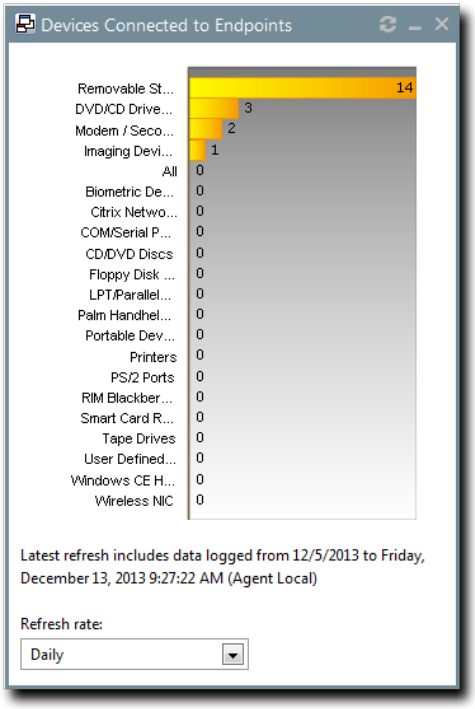


Figure 16: Devices Connected to Endpoints Widget

The chart displays the number of devices in each device class connected to the endpoints. The count on the bar displays the number of devices in a particular device class that were connected to the endpoints.

Dashboard Setting and Behavior Icons

Setting and behavior icons are UI controls used to manage the dashboard. Click these icons to maximize, minimize, hide, and refresh the dashboard and widgets.

The following table describes each icon action.

Table 38: Widget Setting and Behavior Icons

Icon	Action
	Opens the ***Dashboard Settings*** dialog.
	Opens the dashboard in print preview mode.

Icon	Action
	Collapses the associated widget.
	Expands the associated collapsed widget.
	Hides the associated widget.
	Refreshes the associated widget (or the entire dashboard).

Note: Not all widgets contain **Refresh** icons.

Previewing and Printing the Dashboard

When viewing the dashboard, you can reformat it for printing. This reformat omits the Web site header and footer, reorganizing the dashboard to display only the selected widgets, making it ideal for printing.

1. From the **Navigation Menu**, select **Home**.
2. Click  .

   Step Result: The dashboard print preview opens in a new Web browser window.
3. [Optional] Use your Web browser controls to print the dashboard.

Editing the Dashboard

You can customize how widgets are arranged and prioritized. Edit the dashboard to display only the widgets useful in your environment.

Edit the dashboard from the ***Dashboard Settings*** dialog.

1. From the **Navigation Menu**, select **Home**.
2. Click  .

   Step Result: The ***Dashboard Settings*** dialog opens.
3. Choose which widgets you want to display on the dashboard.
   - Select widget check boxes to display them.
   - Clear widget check boxes to hide them.
4. Prioritize the widgets in the desired order.
   - Click  to increase a widget priority.
   - Click  to decrease a widget priority.

   Highly prioritized widgets are more prominently placed.

5. Display or hide widget descriptions.
   - Click to display descriptions.
   - Click to hide descriptions.
6. Choose a widget layout.
   - Click to display widgets in two columns.
   - Click to display widgets in three columns.
7. Click **OK**.

Result: Your dashboard settings are saved. The ***Home*** page displays the selected widgets in the priority you defined.

The System Alert Pane

The ***System Alert*** pane displays information about changing conditions in your environment. This pane alerts you to required actions and links to related help topics.

The **System Alert** pane displays in the dashboard and shows the number of alerts that require your attention.

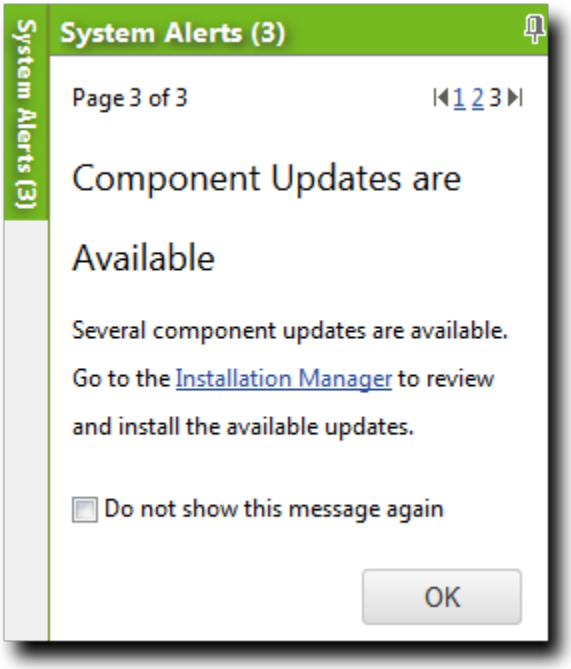


Figure 17: The System Alert Pane

The following functions can be found in the ***System Alert*** pane.

Table 39: Options Menu Items

Option	Description
Pin (icon)	Docks the ***System Alert*** pane. Clicking this icon again collapses it.
Pagination Links	Allows you to navigate between alerts. For more information, see Advancing Through Pages on page 42.
Action Link	Opens the appropriate application page, external Web page, or context-sensitive help topic, depending on the action specified in the alert.
Don't show this again (check box)	Collapses the ***System Alert*** pane. The alert shown in the ***System Alert*** pane when this check box is selected will no longer be shown.
OK (button)	Collapses the ***System Alert*** pane.

Note:

- Dismissing a notification only dismisses the notification for logged in user. The notification still displays for others.
- The system automatically dismisses alerts as you complete their related actions, regardless of whether you dismiss the alerts.

License Expiration

When licensing for a module expires, the module behavior changes. All functionality is restored when the licensing is renewed.

Note: When a subscription expires, the module history and configuration is retained. No work is lost when the module is renewed.

Table 40: License Expiration Scenario and Events

Scenario	Event(s)
Server Module Expiration	• Endpoint module functionality is partially disabled. • The module cannot be installed on additional endpoints. • The ***Endpoints*** page list the module status as `Expired`. • The ***Home*** page lists the **Available** license count as `Expired`.
Endpoint Module Expiration	• Endpoint module functionality is partially disabled. • The module cannot be installed on additional endpoints. • The ***Endpoints*** page list the module status as `Expired`. • The ***Home*** page lists the **Available** license count as `Expired`. • The Patch and Remediation endpoint module component continues to inventory its host, but no longer enforces Patch and Remediation policies or downloads deployments. • The AntiVirus endpoint module continues enforcing policies and completing scans, but no longer downloads new virus definitions. • The Application Control endpoint component stops enforcing all policies, no longer blocking or logging applications. • The Device Control endpoint component allows all actions and stop logging activity.

Table 41: License Expiration Scenario and Events for Mobile Endpoints

Scenario	Event

Mobile Endpoint Module Expiration	• The ***Mobile Endpoints*** page list the module status as `Expired`.
	  • Endpoints with the oldest check ins expire first.
	  • Endpoints that attempt to register when your license count is depleted are listed with a status of `Expired`.
	  • Endpoints cannot be issued commands with the exception of **Delete**.
	  • Any push notifications available on expired endpoints are removed.
	  • Any policy events queued or issued to expired endpoints have display a status of `Expired`.
	• Endpoints cease communications with the server and the cloud.
	• The ***Home*** page lists the available license count as `0`.

	Note: Endpoints in an `Offline` or `Wiped` status hold their license until deleted.

To reactivate your licenses following renewal, open the ***Subscription Updates*** page and click **Update Now**. Your server replicates updated subscription information. The page refreshes when the update completes, and all previous module functionality is restored.

Note: For more information about renewing or adding licenses, contact Ivanti Sales Support (sales@ivanti.com) .

Chapter 5

Using Managed Policies

In this chapter:

Ivanti Application Control provides *managed policies* for creating whitelists of authorized applications and blacklists of blocked applications.

Easy Auditor is a managed policy that creates a whitelist of authorized applications already on an endpoint, without blocking any applications that are installed later. *Easy Lockdown* also creates a whitelist, but it blocks any applications subsequently installed on the endpoint. A *Supplementary Easy Lockdown/Auditor* policy adds subsequent applications to the endpoint's whitelist. A *Denied Applications* policy blocks specified applications from running by adding them to a centralized blacklist.

Managed Policies

Managed Policies are used to authorize applications to run, and block them from running, on endpoints.

Easy Auditor	Easy Auditor scans endpoints and adds the applications it finds to each endpoint's whitelist. Applications installed later are neither blocked nor added to the whitelist. Logging is enabled so that application usage can be monitored. See Working with Easy Auditor on page 76.
Easy Lockdown	Easy Lockdown scans endpoints and adds the applications it finds to each endpoint's whitelist. Any later attempts to install new applications are blocked. They can only run if added to the whitelist by a Supplemental Easy Lockdown/Auditor policy, or permitted by a trust mechanism. See Working with Easy Lockdown on page 89.
Supplemental Easy Lockdown/Auditor Policy	A Supplemental Easy Lockdown/Auditor policy adds an application to an endpoint's existing whitelist of permitted applications. See Working with Supplemental Easy Lockdown/Auditor Policy on page 123.

Denied Applications Policy	A Denied Applications policy adds an application to a centralized blacklist which stops the application from running with specified endpoints or users. See Working with Denied Applications Policy on page 108.

Implementing application control usually begins with Easy Auditor followed by an evaluation period. Other Managed Policies can then be applied, along with Trusted Change policies. For more information, see Trusted Change Policies on page 141.

Ivanti Application Control and Windows 8

Ivanti Application Control policies can be applied to most applications that run on Windows 8, but some Windows 8 applications are script-based and can not be controlled by Application Control.

Windows 8 can run both conventional Windows applications and Windows Store (formerly Metro) apps, which are developed specifically for Windows 8.

Most Windows Store apps are written in programming languages such as C# or VB.NET, and comprise executable files such as .exes and .dlls. Ivanti Application Control can scan such files, enabling an administrator to apply Application Control policies to them, just like conventional Windows applications.

Some Windows Store apps are created with combination of JavaScript and HTML. These script-based applications are not scanned by Ivanti Application Control, so it is not possible to apply Application Control policies to them.

Blocking Windows Store Apps

When Ivanti Application Control blocks a Windows Store app, Windows 8 displays the app's splash screen before the blocking dialog opens.

When you click an app tile to launch a Windows Store app, you see the application's *splash screen*. This is a graphic that Windows 8 uses to indicate that the application is being activated, and it is displayed before the application loads into memory.

If Ivanti Application Control blocks the app from running, the splash screen will display briefly before the ***Non-Authorized Application Detected*** dialog is displayed. This is normal Windows 8 behavior, and does not mean that any part of the application was loaded into memory.

Excluding Files from Application Scanning

Easy Auditor and Easy Lockdown carry out application scanning on endpoints. Excluding certain file types from the scan can improve its performance.

Both Easy Auditor and Easy Lockdown run an application scan on the endpoint to create a list of all executable files to add to the whitelist. The scan time varies, depending on the number and size of files found. In particular, processing files that contain large numbers of other files (for example, archive files such as .zip and virtual machine files) can prolong scan times.

Ivanti Application Control can exclude specific file types from the scan so that it completes in a reasonable time and does not impact the endpoint's performance. There are three mechanisms for excluding files from the scan:

The built-in exclusion list	This predefined list contains many common non-executable file types such as graphics, documents, and virtual machine files. See File Types Excluded from Application Scan on page 71 for more information.
Archive files	Most types of archive files are excluded from application scanning. CAB and MSI archive files are an exception in some cases. For more information of archive file exclusions and exceptions, see Excluding Archive Files on page 71 for more information.
The ACAPPSCANEXCLUDE variable	You can set a Windows environment variable (ACAPPSCANEXCLUDE) on the endpoint, which specifies paths and/or file extensions to exclude from the scan. See Excluding Files with ACAPPSCANEXCLUDE on page 72 for more information.

File Types Excluded from Application Scan

A number of file types are automatically excluded from the application scan carried out during Easy Auditor and Easy Lockdown.

Excluded file types	`.bmp`, `.cfg`, `.config`, `.cur`, `.db`, `.dmp`, `.doc`, `.docx`, `.gif`, `.gpd`, `.htm`, `.html`, `.ico`, `.idx`, `.inf`, `.ini`, `.ISO`, `.jpg`, `.lnk`, `.log`, `.manifest`, `.mp3`, `.msg`, `.nls`, `.pdf`, `.pls`, `.pm`, `.pnf`, `.png`, `.rtf`, `.svg`, `.txt`, `.vmdk`, `.vmem`, `.wav`, `.wmf`, `.xls`, `.xlsx`, `.xml`, `.xsd`, `.xsl`, `.xslx`.

Note: These are not executable files, so excluding them from the scan simply decreases the scan time without changing what files end up on the endpoint's whitelist.

Excluding Archive Files

Most types of archive file are excluded from application scanning.

By default, when Easy Lockdown or Easy Auditor performs an application scan, archive files such as ZIPs and RARs are not scanned. Archive files must be expanded and stored in a temporary location before their contents can be scanned. This process takes time and consumes large amounts of disk space.

Note: As an exception, CAB and MSI archive files are scanned *only* when all of the following conditions are met:

- The file resides in the `%SystemRoot%` folder. If the file is in any other folder or disk, it is excluded.
- The file has extracted.
- The file has been added to the whitelist and report to the Application Library.

Excluding Files with ACAPPSCANEXCLUDE

You can use the Windows variable ACAPPSCANEXCLUDE to exclude specific file types or locations from an application scan.

Certain non-executable file types are automatically excluded from an application scan to reduce scan time. If you have large numbers of files that are not excluded by default, you can exclude them using the ACAPPSCANEXCLUDE variable.

Tip: Compare the list of automatically excluded files with the types of file that are prevalent on the endpoint. For example, the common graphics files `.gif`, `.png`, and `.jpg` are excluded from the scan. If your endpoint has large numbers of other graphic file types (such as Photoshop `.psd` files) you can reduce the scan time by explicitly excluding these files.

You can set the ACAPPSCANEXCLUDE variable using location, file type, or a combination of the two.

Examples:

Location	C:\Windows\Temp\; C:\Custom\
File type	*.vmsd;*.vmxf;*.psd
Combination	C:\OldPrograms*.zip

Important: Be careful about specifying archive file types such as `.zip` or `.rar`. When you exclude a file from the application scan, it is not added to the endpoint's whitelist. When application control is enforced (after Easy Lockdown, for example) that file will be blocked from running. This will cause problems if the operating system or another application needs the file at any stage.

Setting the ACAPPSCANEXCLUDE Environment Variable

The ACAPPSCANEXCLUDE environment variable can be set to exclude specific paths and file types from the application control scan. This can have the benefit of speeding up the scan and reducing impact on the endpoint.

The following steps describe how to set the ACAPPSCANEXCLUDE environment variable on an individual endpoint running Windows 7 or Windows 8. The procedure is slightly different on other versions of Windows; check the Windows documentation for details on how to set the variable.

Note: With large numbers of endpoints, setting the variable individually on each endpoint is time-consuming. A better approach is to use a mechanism such as Group Policy Objects (GPO), which enable administrators to control the working environments.

1. Open ***Windows Control Panel***.
2. From the **View by** list, ensure **Category is selected**.
3. Click **System and Security**.

   Step Result: The **System and Security** options open.
4. Click **System**.

   Step Result: The **System** options open.

5. Click **Advanced system settings**.

   Step Result: The ***System Properties*** dialog opens to the ***Advanced*** tab.

6. Click **Environment Variables**.

   Step Result: The ***Environment Variables*** dialog opens.

7. In the **System Variables** section click **New**.

   Step Result: The ***New System Variable*** dialog opens.

8. In the **Variable name** field, type `ACAPPSCANEXCLUDE` and press ENTER.
9. In the **Variable value** field, type all file path(s) and/or file type(s) to be excluded from the scan. Press ENTER after you finish typing variables.

   Note: When defining multiple entries, use a semicolon (;) to separate them.

10. Click **OK** to close the ***New System Variable*** dialog.
11. Close the ***Environment Variables*** dialog, ***System Properties*** dialog, and ***Control Panel***.
12. Reboot the endpoint to enable the new system environment variables.

Result: The ACAPPSCANEXCLUDE environment variable has been set to exclude specific paths and/or file types from the application control scan.

Logging Managed Policies

Managed Policies include Easy Auditor and Easy Lockdown, which have logging options that help monitor application usage. The logging options also influence logging of other policies (including Trusted Change policies).

Easy Auditor and Easy Lockdown logging options are based on *authorized* and *non-authorized* applications. An authorized application is one that was whitelisted during Easy Auditor or Easy Lockdown, or authorized through a trust mechanism. A non-authorized application is not on the whitelist, nor authorized through a trust mechanism, or has been added to the blacklist.

Easy Auditor and Easy Lockdown have the following logging options:

Log non-authorized applications (all executable files)	All non-authorized applications the user attempts to run are logged. All executable file types are logged, not just `.exe` files. This is the default option for Easy Auditor.
Log authorized applications (*.exe only)	All authorized applications the user runs are logged. Only the initial executable is logged by default, subsequent files or dependent libraries loaded are not logged. Use the **Include all details** option below to log those events as well.

Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	Detailed information on every executable file and library loaded will be logged (only available if the **Log authorized applications** option is selected). This should be treated with caution as it can generate very large log files.

These options can also affect the other Application Control policies. Trusted Updater and Trusted Publisher do not have their own logging options, but events associated with these policies can be logged. Denied Applications and Trusted Path do have their own logging options, but they can be affected by the Easy Auditor/Easy Lockdown options selected.

The Easy Lockdown and Easy Auditor logging options have the following effects on the other Application Control policies:

Log non-authorized applications (all executable files)	
Denied Applications	Logs attempts to run applications blocked by Denied Applications policies. This overrides the setting in the Denied Applications policy.
Trusted Updater	Logs when applications are added to the whitelist by Trusted Updater.
Trusted Publisher	No effect
Trusted Path	No effect

Log authorized applications (*.exe only)	
Denied Applications	No effect
Trusted Updater	Logs when applications are added to the whitelist by Trusted Updater. Logs when applications whitelisted by Trusted Updater are allowed to run.
Trusted Publisher	Logs when applications are allowed to run by Trusted Publisher policies.
Trusted Path	Logs when applications are allowed to run by Trusted Path policies. This overrides the setting in the Trusted Path policy.

Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	
Denied Applications	No effect
Trusted Updater	No effect
Trusted Publisher	No effect

Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	
Trusted Path	Detailed information on applications allowed to run by the Trusted Path policy is logged (every executable file and library loaded will be logged). This overrides the setting in the Trusted Path policy.

Unassigning Multiple Policies

You can unassign multiple application control policies at the same time, removing the association between them and their assigned endpoints and users. Policies that are no longer assigned to an endpoint remain in the system as unassigned policies, which you can re-assign at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click either the **Managed Policies** tab or the **Trusted Change** tab.
3. Select all the policies you want to unassign on that page.

   Note: You can select any combination of the policy types available on the page.

   Step Result: The selected policies are highlighted.

4. Click **Unassign**.

   Step Result: The Unassign Policy confirmation dialog is displayed.

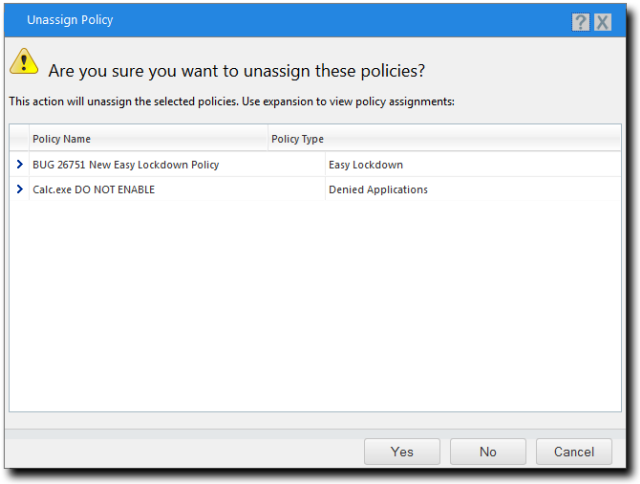


Figure 18: Unassign Multiple Application Control Policies

5. Review the policies to be unassigned. If necessary, click a chevron (**>**) to expand the display of the endpoints and users that a policy is assigned to.
6. Click **Yes**.

Result: The application control policies are unassigned.

Working with Easy Auditor

An Easy Auditor policy authorizes applications currently on an endpoint by adding them to the whitelist, without blocking applications that are installed afterwards.

An Easy Auditor policy has three main functions:

- Adding applications currently on the endpoint to the endpoint's whitelist
- Allowing non-authorized applications to run (application control *enforcement* is off)
- Enabling logging (optional)
  - log non-authorized applications (this is on by default for Easy Auditor)
  - log authorized applications (initial executable only)
  - log all associated executables and library files

Warning: Logging authorized applications will generate very large log files. This option should only be used for trouble-shooting purposes.

You can use Easy Auditor to start implementing application control on the network. It creates a whitelist of authorized applications without blocking any later applications or updates. This allows you to build up a picture of application usage on the network without affecting users' ability to run the applications they need.

Note: Easy Auditor is similar to Easy Lockdown in that both create a whitelist of permitted applications, but the crucial difference between them is that Easy Auditor subsequently permits non-authorized applications to run, whereas Easy Lockdown blocks them.

Creating an Easy Auditor Policy

You can create an Easy Auditor policy and assign it to endpoints or groups. It creates a whitelist on each endpoint of the applications installed on that endpoint, without blocking non-authorized applications and updates that are subsequently installed.

Tip: Easy Auditor carries out an application scan of the endpoint, which can impact its performance. To lessen this impact, you can do the following:

- Reduce the scan time by excluding certain files from the scan (although these files will not then be added to the endpoint whitelist). See Excluding Files with ACAPPSCANEXCLUDE on page 72 for more information.
- Reduce the effect on users by running the scan outside business hours.

1. Select **Manage** > **Policy Wizards** > **Easy Auditor**.

   Step Result: The ***Easy Auditor Wizard*** opens to the ***Name and Logging Options*** page.

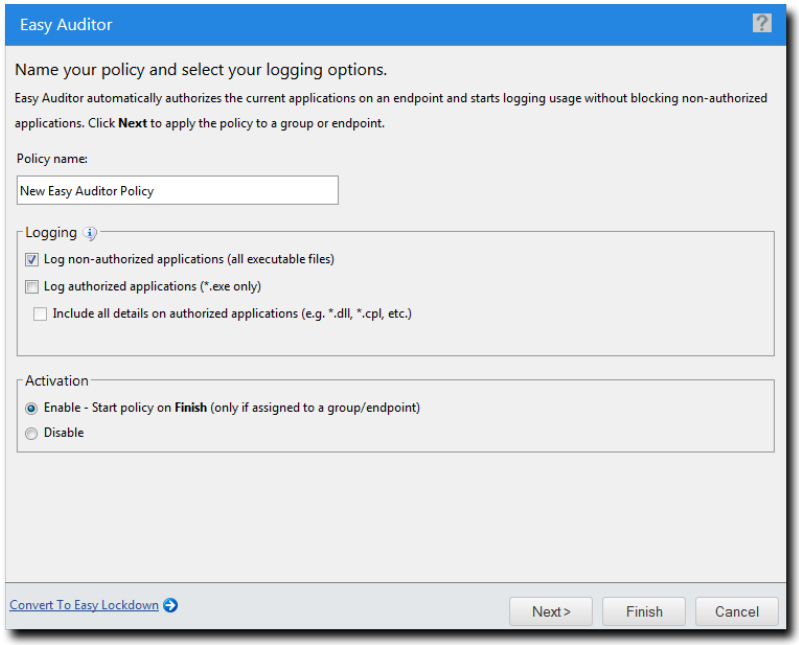


Figure 19: Easy Auditor Wizard - Name and Logging Options Page

2. Type a **Policy Name** for the new Easy Auditor policy.

Note: Try to give the policy a descriptive name. For example, if this Easy Auditor policy relates to a group of endpoints used by the product managers you could name it `Product Management - Audit`.

3. Select the **Logging** options. As the focus of Easy Auditor is recording application activity on the endpoint, you must select at least one logging option.

Note: An *authorized* application is one that was added to the endpoint's whitelist when Easy Auditor was applied, or one that is authorized through any trust mechanism. A *non-authorized* application is one that is not on the whitelist and is not authorized through any trust mechanism.

Log non-authorized applications (all executable files)	All non-authorized applications the user attempts to run are logged. By default, this option is selected for Easy Auditor. **Note:** All executable file types will be logged, not just `.exe` files. This option also logs Trusted Updater policy "Added to whitelist" events.

Log authorized applications (*.exe only)	All authorized applications the user runs are logged. **Note:** Only the initial executable is logged. Use the **Include all details** option below to log subsequent executable files or dependent libraries loaded later. This option also logs all events related to Trusted Updater, Trusted Publisher, and Trusted Path policies.
Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	Detailed information on authorized applications is logged (every executable file and library loaded will be logged). This option is only available if the **Log authorized applications** option is selected.

Caution: The authorized application options should only be used for monitoring a limited number of endpoints for a short time. If selected for multiple endpoints for multiple days, the database will quickly grow to an unmanageable size.

To create a log query and view the log results refer to Using Application Control Log Queries on page 277.

Note: These logging options can affect other Application Control policies. See Logging Managed Policies on page 73 for more information.

4. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

5. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time.

Tip: If you think that an Easy Lockdown policy is more appropriate at this point than Easy Auditor you can quickly switch to the relevant wizard by clicking **Convert to Easy Lockdown**. See Creating an Easy Lockdown Policy on page 92 for more information.

Step Result: The ***Easy Auditor Wizard*** opens to the ***Assign Groups and Endpoints*** page.

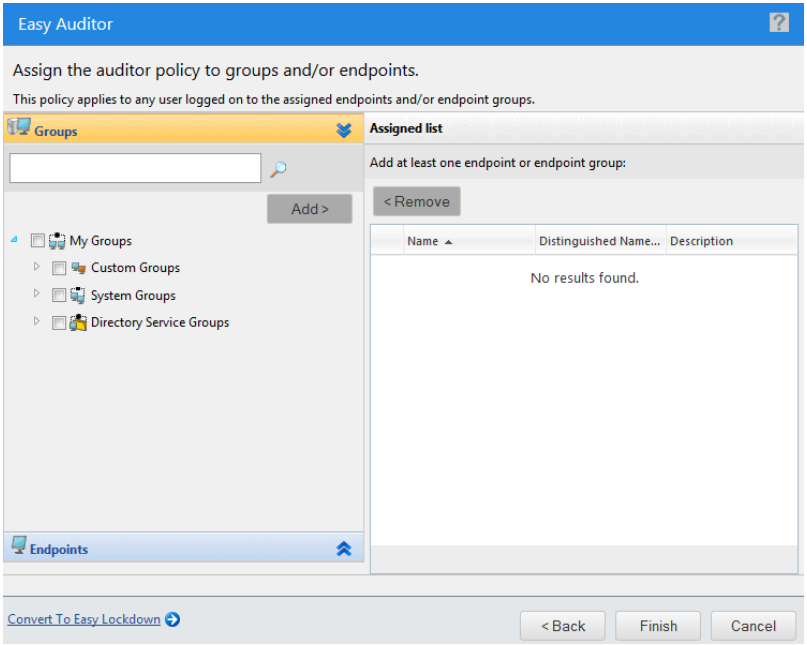


Figure 20: Easy Auditor Wizard - Assign Groups and Endpoints Page

6. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

7. Click **Finish**.

Result: The Easy Auditor policy is created and assigned to the selected groups or endpoints. The new policy is displayed on the ***Managed Policies*** tab, with a **Policy Type** of *Easy Auditor*.

Assigning an Easy Auditor Policy

You can select an Easy Auditor policy and assign it to endpoints and/or groups of endpoints.

1. Select **Manage** > **Application Control Policies**.

   Step Result: The ***Managed Policies*** tab on the ***Application Control Policies*** page is displayed.

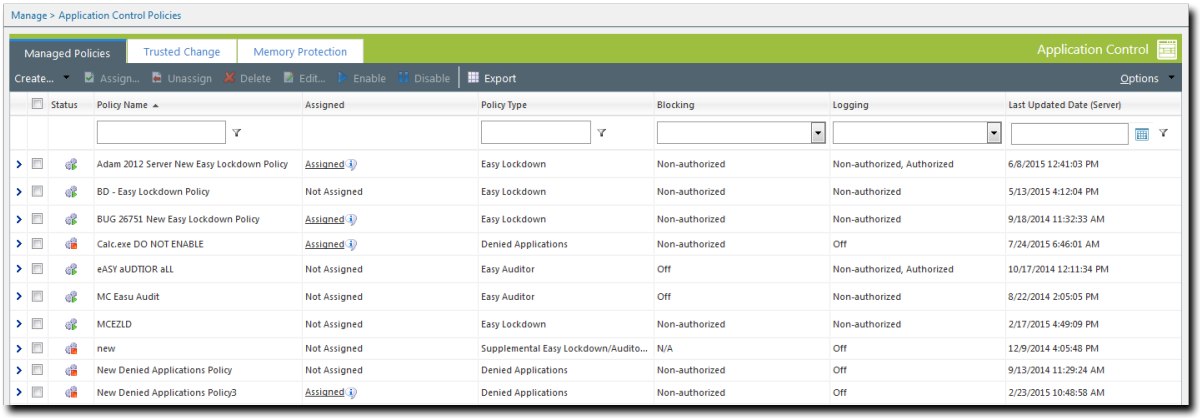


Figure 21: Application Control - Managed Policies

2. Select an Easy Auditor policy.

Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

Step Result: The selected policy is highlighted.

3. Click **Assign**.

   Step Result: The ***Assign Easy Auditor*** dialog is displayed.

4. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

5. Click **OK**.

Result: The Easy Auditor policy is assigned to selected endpoints and/or groups of endpoints.

Assigning an Easy Auditor Policy to a Group

You can assign an Easy Auditor policy to a group of selected endpoints using the ***Assign Policy*** dialog.

Note: The ***Assign Policy*** dialog is also used to assign an Easy Auditor policy to a selected endpoint. See Assigning an Easy Auditor Policy to an Endpoint on page 83 if you are assigning the policy to an endpoint.

1. Select **Manage** > **Groups**.

   Step Result: The ***Groups*** page is displayed.

2. Select a group from the **Browser** tree.

3. From the **View** list, select **Application Control Policies**.

   Step Result: The Application Control policies for the selected group are displayed.

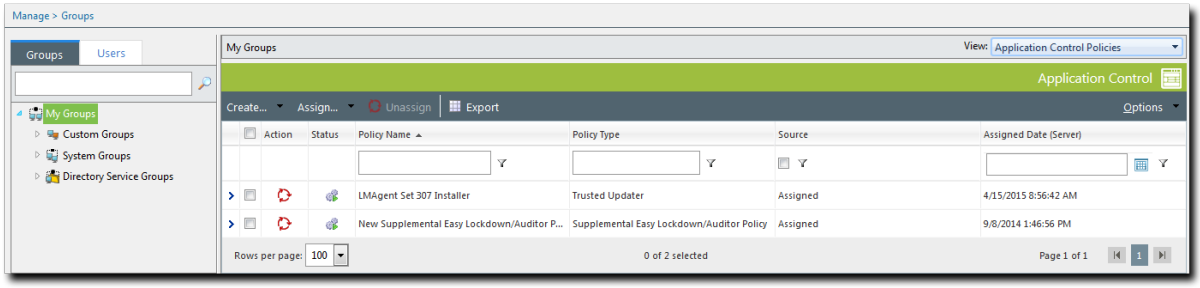


Figure 22: Groups - Application Control Policies View

> **Note:** Inherited policies can not be selected. In addition, the **Source** column reads *Inherited*.

4. Select **Assign** > **Easy Auditor**.

   Step Result: The ***Assign Policy*** dialog is displayed.

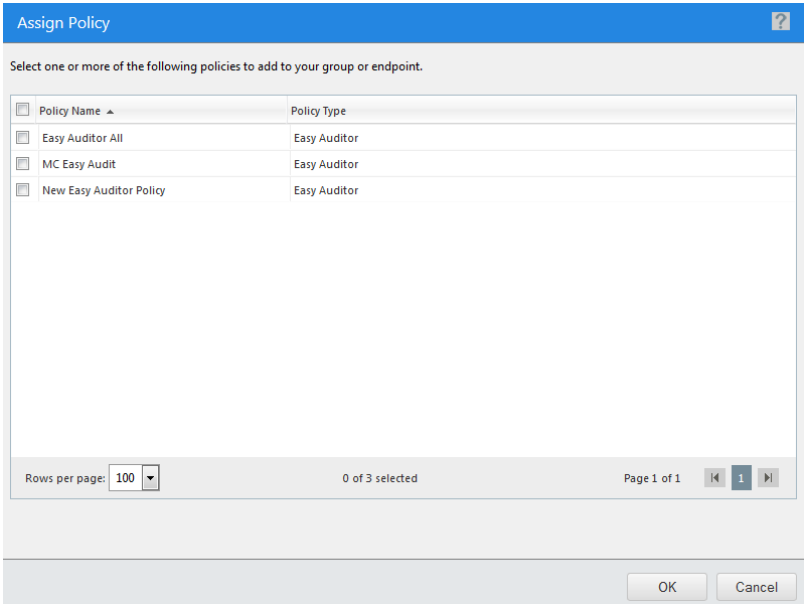


Figure 23: Assign Policy

5. Select an Easy Auditor policy.
6. Click **OK**.

Result: The Easy Auditor policy is assigned to the group.

Assigning an Easy Auditor Policy to an Endpoint

You can assign an Easy Auditor policy to a selected endpoint.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.

2. In the **Endpoint Name** column, click an endpoint link.

   Step Result: Detailed information for the selected endpoint is displayed.

3. Select the ***Application Control Policies*** tab.

   Step Result: A list of Application Control policies assigned to the endpoint is displayed.

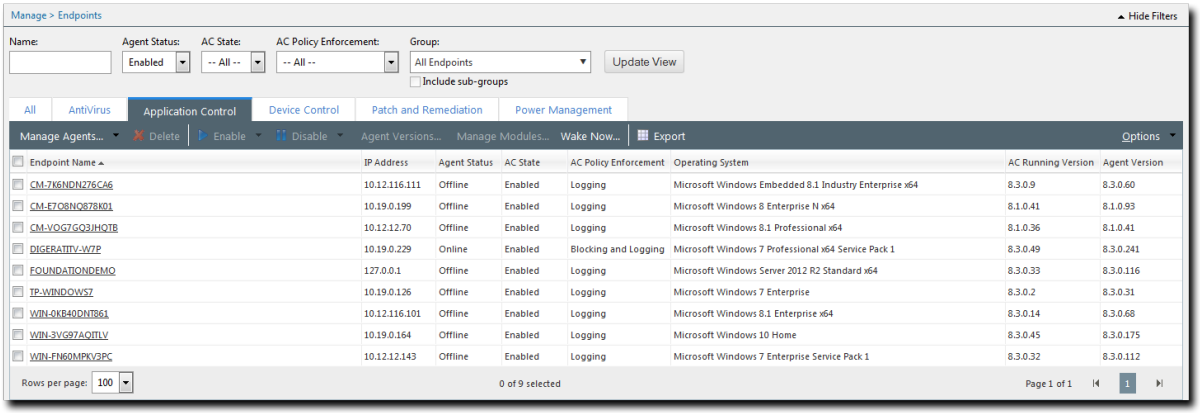


Figure 24: Application Control Policies Tab

4. Select **Assign** > **Easy Auditor**.

   Step Result: The ***Assign Policy*** dialog is displayed.

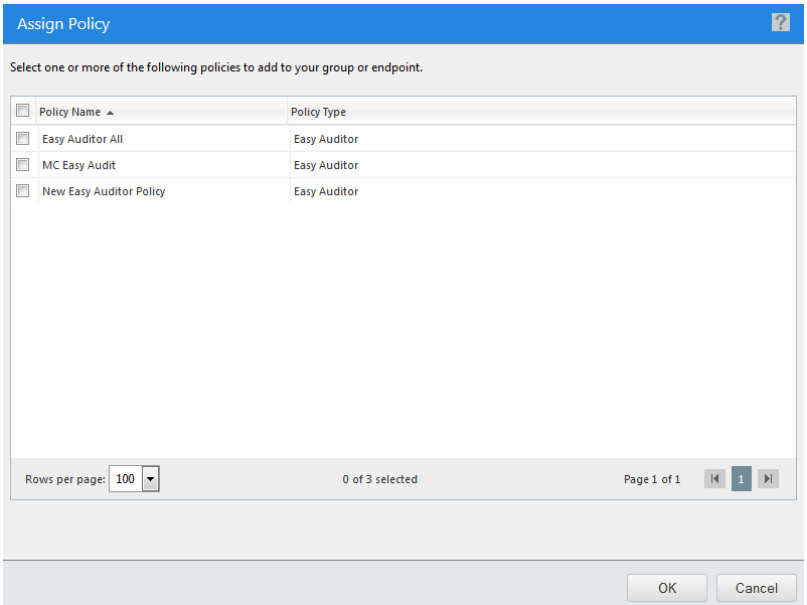


Figure 25: Assign Policy

5. Select an Easy Auditor policy.
6. Click **OK**.

Result: The Easy Auditor policy is assigned to the endpoint.

Unassigning an Easy Auditor Policy

You can unassign an Easy Auditor policy, removing the association between it and any endpoints. Policies that are no longer assigned remain in the system as unassigned policies, which you can re-assign to endpoints at a later time.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select one or more Easy Auditor policies.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

3. Click **Unassign**.

   Step Result: One of two confirmation dialogs is displayed, depending on whether you selected a single policy or multiple policies.

Figure 26: Unassign Application Control Policy

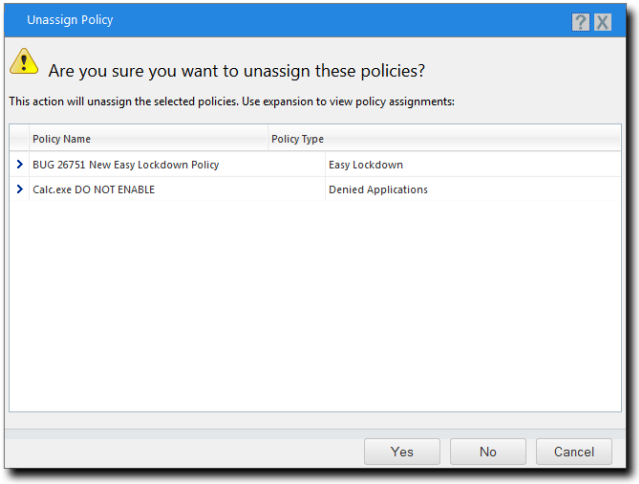


Figure 27: Unassign Multiple Application Control Policies

4. Click **Yes**.

Result: One or more Easy Auditor policies are unassigned.

Editing an Easy Auditor Policy

You can edit an Easy Auditor policy and, for example, change the logging options or the endpoints to which it is assigned.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select an Easy Auditor policy.

Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

3. Click **Edit**.

   Step Result: The ***Easy Auditor Wizard*** opens to the ***Name and Logging Options*** page.

4. [Optional] Edit the **Policy Name**.

Note: Give the policy a descriptive name. For example, if this Easy Auditor policy relates to a group of endpoints used by the product managers you could name it `Product Management - Audit`.

5. Select the **Logging** options. As the focus of Easy Auditor is recording application activity on the endpoint, you must select at least one logging option.

Note: An *authorized* application is one that was added to the endpoint's whitelist when Easy Auditor was applied, or one that is authorized through any trust mechanism. A *non-authorized* application is one that is not on the whitelist and is not authorized through any trust mechanism.

Log non-authorized applications (all executable files)	All non-authorized applications the user attempts to run are logged. By default, this option is selected for Easy Auditor. **Note:** All executable file types will be logged, not just `.exe` files. This option also logs Trusted Updater policy "Added to whitelist" events.
Log authorized applications (*.exe only)	All authorized applications the user runs are logged. **Note:** Only the initial executable is logged. Use the **Include all details** option below to log subsequent executable files or dependent libraries loaded later. This option also logs all events related to Trusted Updater, Trusted Publisher, and Trusted Path policies.
Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	Detailed information on authorized applications is logged (every executable file and library loaded will be logged). This option is only available if the **Log authorized applications** option is selected.

Caution: The authorized application options should only be used for monitoring a limited number of endpoints for a short time. If selected for multiple endpoints for multiple days, the database will quickly grow to an unmanageable size.

To create a log query and view the log results refer to Using Application Control Log Queries on page 277.

Note: These logging options can affect other Application Control policies. See Logging Managed Policies on page 73 for more information.

6. [Optional] Edit the **Activation** options.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

7. Click **Next**.

   Step Result: The ***Easy Auditor Wizard*** opens to the ***Assign Groups and Endpoints*** page.

8. [Optional] Edit the list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

9. Click **Finish**.

Result: The Easy Auditor policy is edited.

Disabling an Easy Auditor Policy

You can disable Easy Auditor policies without deleting them. The details of the policies are retained and you can enable them again at a later time.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select the enabled Easy Auditor policy or policies that you want to disable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

3. Click **Disable**.

Result: One or more Easy Auditor policies are disabled.

Enabling an Easy Auditor Policy

You can enable an Easy Auditor policy that is currently disabled.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control Policies is displayed.

2. Select the disabled Easy Auditor policy or policies that you want to enable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

3. Click **Enable**.

Result: One or more Easy Auditor policies are enabled.

Deleting an Easy Auditor Policy

You can delete an Easy Auditor policy, as long as it is not assigned to an endpoint.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select an Easy Auditor policy that is not assigned to an endpoint (**Assigned** column value of *Not Assigned*).

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

3. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned.

4. Click **Yes**.

Result: The Easy Auditor policy is deleted.

Exporting an Easy Auditor Policy

You can export a list of policies to a csv (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a csv file with the following columns:

Name	Description
Status	Enabled or Disabled
Policy Name	The name of the policy
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)
Policy Type	The type of policy (Easy Lockdown, Trusted Updater, and so on)
Blocking	Off, On, Authorized, Non-authorized, or (Authorized, Non-authorized)
Logging	Authorized, Non-authorized, or Off
Last Updated Date	The date the policy was last changed

Working with Easy Lockdown

An Easy Lockdown policy authorizes applications currently on an endpoint by adding them to a whitelist, and blocks any applications that are installed afterwards.

An Easy Lockdown policy has three main functions:

- Allowing applications currently on the endpoint to run by adding them to the endpoint's whitelist
- Applying application control *enforcement* - non-authorized applications are blocked
- Enabling logging (optional; no logging options are selected for Easy Lockdown by default)
  - log non-authorized applications
  - log authorized applications (initial executable only)
  - log all associated executables and library files

You can use Easy Lockdown to consolidate application control on the network after an appropriate evaluation period. It creates a whitelist of authorized applications and blocks any later applications.

Note: Easy Lockdown is similar to Easy Auditor in that both create a whitelist of permitted applications, but the crucial difference between them is that Easy Lockdown subsequently blocks all non-authorized applications, whereas Easy Auditor permits them.

Easy Lockdown is performed when an Easy Lockdown policy is assigned to selected groups or endpoints. It is also performed when a disabled Easy Lockdown policy is enabled.

Important: You should only apply Easy Lockdown when you are confident that it will not adversely affect endpoints or users. This usually means having appropriate *trust mechanisms* in place to authorize applications and updates that are necessary for the continuing operation of the endpoints and installed software.

Easy Lockdown in Practice

Thorough preparation is the key to successfully applying Easy Lockdown to an endpoint.

Applying Easy Lockdown is a major step in implementing application control as it authorizes a set of approved applications on the endpoint's whitelist. Therefore, before you apply Easy Lockdown, you should carry out a thorough auditing process to evaluate the patterns of software use on the endpoint.

After evaluating the audit results you should:

- Install all applications that will be needed on the endpoint.
- Uninstall all unwanted and unnecessary applications.

  Note: Installing or uninstalling software at a later stage may require removing and re-applying Easy Lockdown. This can entail considerable effort, and should be avoided if possible.

- Identify applications that are revised frequently or that self-update dynamically. Ensure that you have trust mechanisms in place that will automate these processes.
- Identify web applications and other programs which use ActiveX controls and change frequently. If digitally signed, these are ideal candidates for a Trusted Publisher policy.

  Note: If a program attempts to install a new ActiveX control on a locked-down endpoint, you will see a warning that the ActiveX control failed to load. You then have a problem because the control is only partially installed. See Handling Partial ActiveX Installation on page 90 for information on how to handle this.

- Run an antivirus scan to ensure that no malware or viruses are present on the endpoints.

These actions provide the basis for successfully applying Easy Lockdown, and reduce the administrative overhead after lockdown.

Tip: You can convert an existing Easy Auditor policy to an Easy Lockdown policy. This can save time if a lot of effort has been invested in creating the group/endpoint assignments. See Converting Easy Auditor to Easy Lockdown on page 95 for more information.

Handling Partial ActiveX Installation

If an attempt is made to install a new ActiveX control on a locked-down endpoint, the control will only partially install and an error message is displayed.

You can have ActiveX controls on an endpoint's whitelist just like any other type of executable file. But if you try to install a new ActiveX control after Easy Lockdown (or run an application that attempts

to install such a control), you will see a message such as "ActiveX control failed to load! The <*control name*> could not get user credentials. Please check browser security settings."

Figure 28: ActiveX Warning

Important: If you see this message, there is no point attempting to change the browser settings. Application Control will simply continue to block the unauthorized control.

What happens here is that the ActiveX control is only partially installed and is stuck in an unregistered intermediate state. You will continue to see the warning message in the browser even if you remove Easy Lockdown.

At this point, you need to do the following:

1. Open the folder "C:\WINDOWS\Downloaded Program Files".
2. Identify and delete the ActiveX control identified in the warning message.

You now have the following options to get the ActiveX control working:

Authorize with Trusted Publisher	If the ActiveX control has been digitally signed, it can be added to a Trusted Publisher policy that allows it to execute on the endpoint. For more information, see Working with Trusted Publisher on page 166.
Authorize with Trusted Path	The ActiveX control can be kept in a location designated as a Trusted Path. For more information, see Working with Trusted Path on page 185.
Remove/Re-apply Easy Lockdown	1. Remove Easy Lockdown from the endpoint. 2. Re-install the ActiveX control. The control should install and register itself correctly. 3. Re-apply Easy Lockdown to the endpoint. **Caution:** Removing and re-applying Easy Lockdown can pose a considerable security risk. In the period since the original lockdown, dangerous or unapproved software may have been downloaded or copied to the endpoint. Easy Lockdown should always be preceded by an auditing process to ensure that undesirable files are not added to the endpoint's whitelist.

Creating an Easy Lockdown Policy

You can create an Easy Lockdown policy and assign it to endpoints or groups. It creates a whitelist on each endpoint of the applications installed on that endpoint, and blocks all non-authorized applications and updates that are subsequently installed.

Important: You should only apply Easy Lockdown when you are confident that it will not adversely affect endpoints or users. This usually means having appropriate *trust mechanisms* in place to authorize applications and updates that are necessary for the continuing operation of the endpoints and installed software.

Tip: Easy Lockdown carries out an application scan of the endpoint, which can impact its performance. To lessen this impact, you can do the following:

- Reduce the scan time by excluding certain files from the scan (although these files will not then be added to the endpoint whitelist). See Excluding Files with ACAPPSCANEXCLUDE on page 72 for more information.
- Reduce the effect on users by running the scan outside business hours.

1. Select **Manage** > **Policy Wizards** > **Easy Lockdown**.

   Step Result: The ***Easy Lockdown Wizard*** opens to the ***Name and Logging Options*** page.

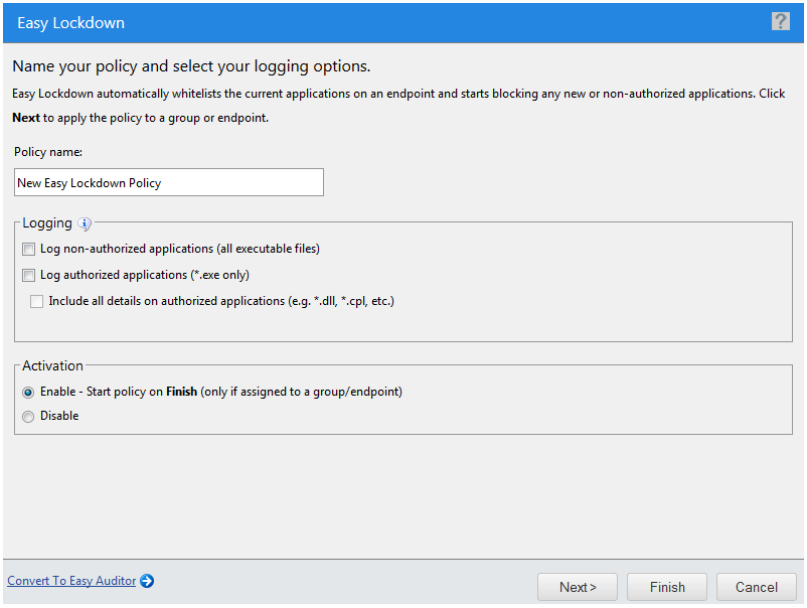


Figure 29: Easy Lockdown Wizard - Name and Logging Options Page

2. Type a **Policy Name** for the new Easy Lockdown policy.

Note: Give the policy a descriptive name. For example, if this Easy Lockdown policy relates to a group of endpoints used by the product managers you could name it `Product Management - Lockdown`.

3. Select the **Logging** options.

Note: An *authorized* application is one that was on the endpoint when Easy Auditor or Easy Lockdown was applied, or one that is authorized through any trust mechanism. A *non-authorized* application is one that was not part of the lockdown and is not authorized through any trust mechanism.

Log non-authorized applications (all executable files)	All non-authorized applications the user attempts to run are logged. By default, this option is not selected for Easy Lockdown. **Note:** All executable file types will be logged, not just `.exe` files. This option also logs Trusted Updater policy "Added to whitelist" events.
Log authorized applications (*.exe only)	All authorized applications the user runs are logged. **Note:** Only the initial executable is logged. Use the **Include all details** option below to log subsequent executable files or dependent libraries loaded later. This option also logs all events related to Trusted Updater, Trusted Publisher, and Trusted Path policies.
Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	Detailed information on authorized applications is logged (every executable file and library loaded will be logged). This option is only available if the **Log authorized applications** option is selected.

Caution: The authorized application options should only be used for monitoring a limited number of endpoints for a short time. If selected for multiple endpoints for multiple days, the database will quickly grow to an unmanageable size.

To create a log query and view the log results refer to Using Application Control Log Queries on page 277.

Note: These logging options can affect other Application Control policies. See Logging Managed Policies on page 73 for more information.

4. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

5. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time.

Tip: At this point, if you think that an Easy Auditor policy is more appropriate than Easy Lockdown you can quickly switch to the relevant wizard by clicking **Convert to Easy Auditor**. See Creating an Easy Auditor Policy on page 76 for more information.

Step Result: The ***Easy Lockdown Wizard*** opens to the ***Assign Groups and Endpoints*** page.

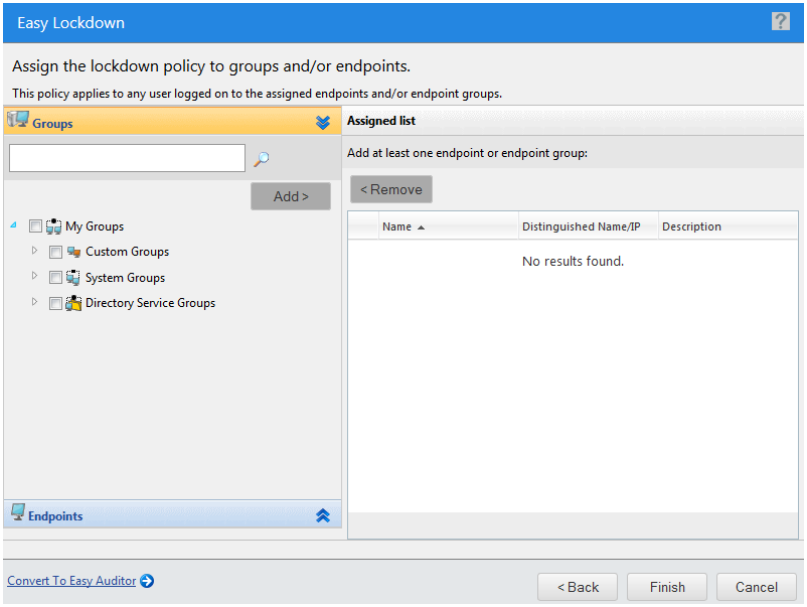


Figure 30: Easy Lockdown Wizard - Assign Groups and Endpoints Page

6. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows () to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

7. Click **Finish**.

Result: The Easy Lockdown policy is created and assigned to the selected groups or endpoints. The policy is displayed on the ***Managed Policies*** tab, with a **Policy Type** of *Easy Lockdown*.

The new policy is sent to the endpoint(s) or group(s), each endpoint is scanned, and a unique whitelist is created for each endpoint. Once the whitelist is created, enforcement will start and new or changed executables will not be allowed to run on the endpoints (unless explicitly permitted by a trust mechanism).

Note: If an application is installed while Easy Lockdown is running, there is no guarantee that all of its files will be added to the endpoint's whitelist. This can lead to unpredictable results when the application is launched, so ensure that no applications are installed during Easy Lockdown.

If an application is installed during Easy Lockdown and then fails to operate correctly, you must regenerate the whitelist. Disable, then enable the Easy Lockdown policy (or alternatively unassign, then assign the policy). The application should then work normally.

Converting Easy Auditor to Easy Lockdown

You can convert an existing Easy Auditor policy to an Easy Lockdown policy. This may save time if a lot of work has already been done creating the group/endpoint assignments.

It can be convenient to convert an existing Easy Auditor policy to Easy Lockdown rather than creating an Easy Lockdown policy from scratch. You may have invested a lot of time and effort creating the group and endpoint assignments, and fine-tuning them over the length of time the Easy Auditor policy has been in use. Converting the policy avoids repeating this work.

When activated, the Easy Lockdown policy carries out a scan to generate a new whitelist, and then starts enforcing application control. The new whitelist is necessary because applications may have been added to the endpoint after the original Easy Auditor policy was created. While these applications can run under Easy Auditor, they are not on the endpoint's whitelist, so they will not run under Easy Lockdown.

Note: You can also convert an existing Easy Lockdown policy to an Easy Auditor policy, but this is less likely to provide a benefit.

Converting an Easy Auditor Policy
You can convert an existing Easy Auditor policy to an Easy Lockdown policy. This regenerates the whitelist on each endpoint and enforces application control, thereby blocking non-authorized applications.

1. Select **Manage** > **Application Control Policies**.

   Step Result: The ***Managed Policies*** page opens.

2. Select the Easy Auditor policy you want to convert to Easy Lockdown.
3. Click **Edit**.

   Step Result: The ***Easy Auditor Wizard*** page opens.

4. Click **Convert to Easy Lockdown**.

   Step Result: The ***Easy Auditor Wizard*** changes to the ***Easy Lockdown Wizard***.

5. If required, change the name for the new Easy Lockdown policy.
6. If required, change the **Logging** options. By default, Easy Lockdown does not have any logging options selected.

   Note: An *authorized* application is one that was added to the endpoint's whitelist when Easy Lockdown was applied, or one that is authorized through any trust mechanism. A *non-authorized* application is one that is not on the whitelist and is not authorized through any trust mechanism.

Log non-authorized applications (all executable files)	All non-authorized applications the user attempts to run are logged. **Note:** All executable file types will be logged, not just `.exe` files. This option also logs Trusted Updater policy "Added to whitelist" events.

Log authorized applications (*.exe only)	All authorized applications the user runs are logged. **Note:** Only the initial executable is logged. Any subsequent executable files or dependent libraries loaded by the initial executable are not logged. Use the **Include all details** option below to log those events as well. This option also logs all events related to Trusted Updater, Trusted Publisher, and Trusted Path policies.
Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	Detailed information on authorized applications is logged (every executable file and library loaded will be logged). This option is only available if the **Log authorized applications** option is selected. **Caution:** This option should only be used for monitoring a limited number of endpoints for a short time. If this option is selected for multiple endpoints for multiple days, the database will quickly grow to an unmanageable size.

To create a log query and view the log results refer to Using Application Control Log Queries on page 277.

Note: These logging options can affect other Application Control policies. See Logging Managed Policies on page 73 for more information.

7. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

8. Click **Next**.

   Step Result: The ***Easy Lockdown Wizard*** opens to the ***Assign Groups and Endpoints*** page.

9. If required, modify the list of targets (groups or endpoints) for the policy.

Note: A common reason for converting an Easy Auditor policy to Easy Lockdown is to make use of the work that has been put into creating the group/endpoint assignments. It is unlikely, therefore, that you will be making major modifications to this list.

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

10. Click **Finish**.

Result: The Easy Lockdown policy is created and assigned to the selected groups or endpoints. The new policy is displayed on the ***Managed Policies*** tab, with a **Policy Type** of *Easy Lockdown*. If the **Activation** option is set to **Enable**, the policy is applied immediately, a new whitelist is generated, and application control is enforced.

Assigning an Easy Lockdown Policy

You can select an Easy Lockdown policy and assign it to endpoints and/or groups of endpoints.

Important: You should only apply Easy Lockdown when you are confident that it will not adversely affect endpoints or users. This usually means having appropriate *trust mechanisms* in place to authorize applications and updates that are necessary for the continuing operation of the endpoints and installed software.

1. Select **Manage** > **Application Control Policies**.

   Step Result: The ***Managed Policies*** tab on the ***Application Control Policies*** page is displayed.

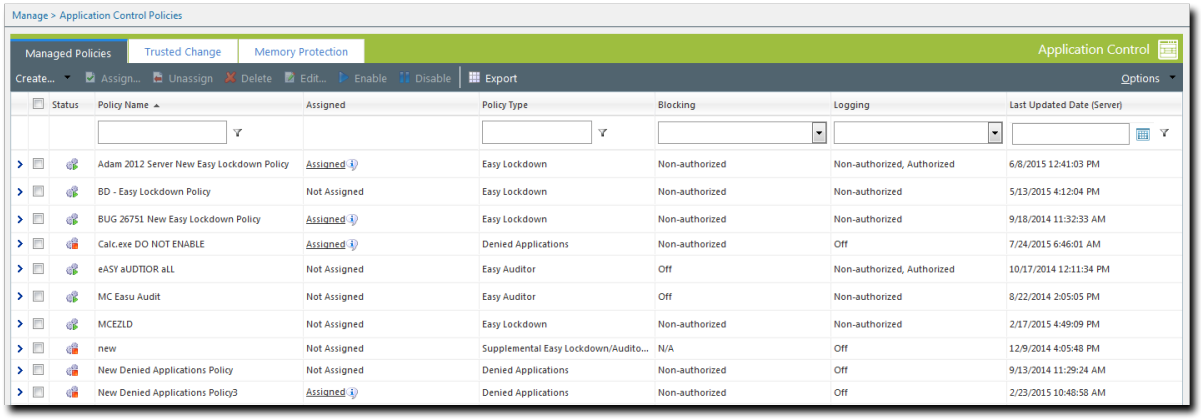


Figure 31: Application Control - Managed Policies

2. Select an Easy Lockdown policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

3. Click **Assign**.

   Step Result: The ***Assign Easy Lockdown*** dialog is displayed.

4. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows () to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

5. Click **OK**.

Result: The Easy Lockdown policy is assigned to endpoints and/or groups of endpoints.

Assigning an Easy Lockdown Policy to a Group

You can assign an Easy Lockdown policy to to a group of selected endpoints using the ***Assign Policy*** dialog.

Note: The ***Assign Policy*** dialog is also used to assign an Easy Lockdown policy to a selected endpoint. See Assigning an Easy Lockdown Policy to an Endpoint on page 101 if you are assigning the policy to an endpoint.

Important: You should only apply Easy Lockdown when you are confident that it will not adversely affect endpoints or users. This usually means having appropriate *trust mechanisms* in place to authorize applications and updates that are necessary for the continuing operation of the endpoints and installed software.

1. Select **Manage** > **Groups**.

   Step Result: The ***Groups*** page is displayed.

2. Select a group from the **Browser** tree.

3. From the **View** list, select **Application Control Policies**.

   Step Result: The Application Control policies for the selected group are displayed.

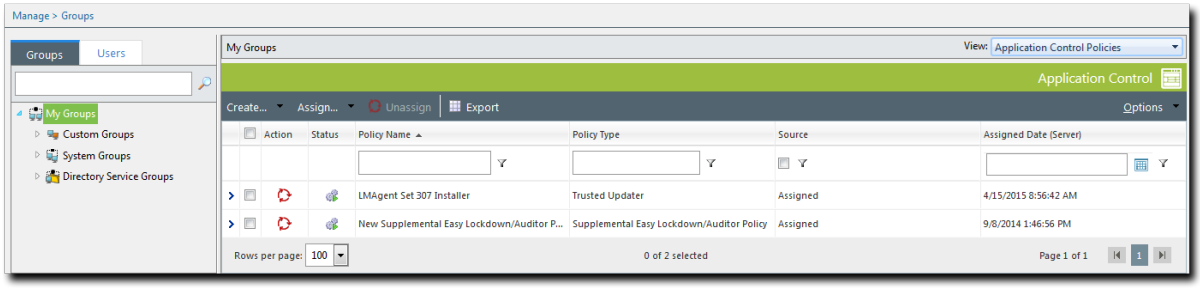


Figure 32: Groups - Application Control Policies View

> **Note:** Inherited policies can not be selected. In addition, the **Source** column reads *Inherited*.

4. From the toolbar, select **Assign** > **Easy Lockdown**.

   Step Result: The ***Assign Policy*** dialog is displayed.

5. Select an Easy Lockdown policy.
6. Click **OK**.

Result: The Easy Lockdown policy is assigned to the group.

Assigning an Easy Lockdown Policy to an Endpoint

You can assign an Easy Lockdown policy to a selected endpoint.

> **Important:** You should only apply Easy Lockdown when you are confident that it will not adversely affect endpoints or users. This usually means having appropriate *trust mechanisms* in place to authorize applications and updates that are necessary for the continuing operation of the endpoints and installed software.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.

2. In the **Endpoint Name** column, click an endpoint link.

   Step Result: Detailed information for the selected endpoint is displayed.

3. Select the ***Application Control Policies*** tab.

   Step Result: A list of Application Control policies assigned to the endpoint is displayed.

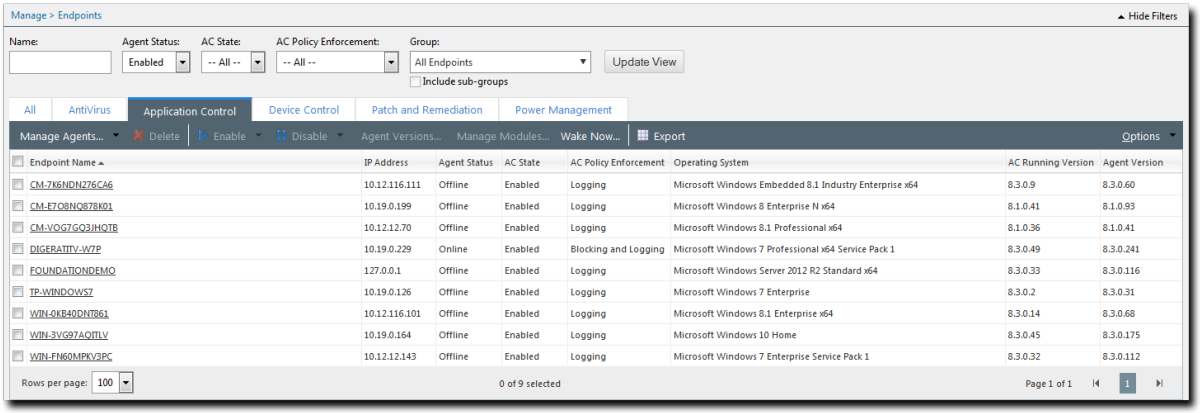


Figure 33: Application Control Policies Tab

4. From the toolbar, select **Assign** > **Easy Lockdown**.

   Step Result: The ***Assign Policy*** dialog is displayed.

5. Select an Easy Lockdown policy.
6. Click **OK**.

Result: The Easy Lockdown policy is assigned to the endpoint.

Unassigning an Easy Lockdown Policy

You can unassign an Easy Lockdown policy, removing the association between it and any endpoints. Policies that are no longer assigned remain in the system as unassigned policies, which you can re-assign to endpoints at a later time.

Note: When you unassign an Easy Lockdown policy from an endpoint, enforcement is no longer applied and the whitelist is effectively discarded. When you assign (or re-assign) an Easy Lockdown policy, a new whitelist is generated.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select one or more Easy Lockdown policies.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy or policies are highlighted.

3. Click **Unassign**.

   Step Result: One of two confirmation dialogs is displayed, depending on whether you selected a single policy or multiple policies.

Figure 34: Unassign Application Control Policy

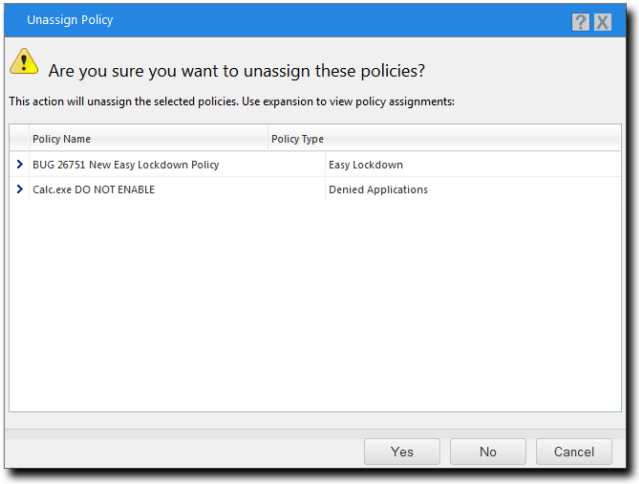


Figure 35: Unassign Multiple Application Control Policies

4. Click **Yes**.

Result: One or more Easy Lockdown policies are unassigned.

Editing an Easy Lockdown Policy

You can edit an Easy Lockdown policy and, for example, change the logging options or the endpoints to which it is assigned.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of application control policies is displayed.

2. Select an Easy Lockdown policy.

Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

3. Click **Edit**.

   Step Result: The ***Easy Lockdown Wizard*** opens to the ***Name and Logging Options*** page.

4. [Optional] Edit the **Policy Name**.

Note: Try to give the policy a descriptive name. For example, if this Easy Lockdown policy relates to a group of endpoints used by the product managers you could name it `Product Management - Lockdown`.

5. [Optional] Edit the **Logging** options.

Note: An *authorized* application is one that was on the endpoint when Easy Auditor or Easy Lockdown was applied, or one that is authorized through any trust mechanism. A *non-authorized* application is one that was not part of the lockdown and is not authorized through any trust mechanism.

Log non-authorized applications (all executable files)	All non-authorized applications the user attempts to run are logged. By default, this option is not selected for Easy Lockdown. **Note:** All executable file types will be logged, not just `.exe` files. This option also logs Trusted Updater policy "Added to whitelist" events.
Log authorized applications (*.exe only)	All authorized applications the user runs are logged. **Note:** Only the initial executable is logged. Use the **Include all details** option below to log subsequent executable files or dependent libraries loaded later. This option also logs all events related to Trusted Updater, Trusted Publisher, and Trusted Path policies.
Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	Detailed information on authorized applications is logged (every executable file and library loaded will be logged). This option is only available if the **Log authorized applications** option is selected.

Caution: The authorized application options should only be used for monitoring a limited number of endpoints for a short time. If selected for multiple endpoints for multiple days, the database will quickly grow to an unmanageable size.

To create a log query and view the log results refer to Using Application Control Log Queries on page 277.

Note: These logging options can affect other Application Control policies. See Logging Managed Policies on page 73 for more information.

6. [Optional] Edit the **Activation** options.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

7. Click **Next**.

   Step Result: The ***Easy Lockdown Wizard*** opens to the ***Assign Groups and Endpoints*** page.

8. [Optional] Edit the list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

9. Click **Finish**.

Result: The Easy Lockdown policy is edited.

Disabling an Easy Lockdown Policy

You can disable Easy Lockdown policies without deleting them. The details of the policies are retained and you can enable them at a later time.

Note: When you disable an Easy Lockdown policy on an endpoint, enforcement is no longer applied and the whitelist is effectively discarded. When you enable (or re-enable) an Easy Lockdown policy, a new whitelist is generated.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control policies is displayed.

2. Select the enabled Easy Lockdown policies that you want to disable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

3. Click **Disable**.

Result: The selected Easy Lockdown policies are disabled.

Enabling an Easy Lockdown Policy

You can enable an Easy Lockdown policy that is currently disabled.

Important: You should only apply Easy Lockdown when you are confident that it will not adversely affect endpoints or users. This usually means having appropriate *trust mechanisms* in place to authorize applications and updates that are necessary for the continuing operation of the endpoints and installed software.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select the disabled Easy Lockdown policy or policies that you want to enable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

3. Click **Enable**.

Result: The selected Easy Lockdown policies are enabled.

Note: If an application is installed while Easy Lockdown is running, there is no guarantee that all of its files will be added to the endpoint's whitelist. This can lead to unpredictable results when the application is launched, so ensure that no applications are installed during Easy Lockdown.

If an application is installed during Easy Lockdown and then fails to operate correctly, you must regenerate the whitelist. Disable, then enable the Easy Lockdown policy (or alternatively unassign, then assign the policy). The application should then work normally.

Deleting an Easy Lockdown Policy

You can delete an Easy Lockdown policy, as long as it is not assigned to an endpoint.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control Policies is displayed.

2. Select an Easy Lockdown policy that is not assigned to an endpoint (**Assigned** column value of *Not Assigned*).

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

3. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned from the endpoints or groups indicated.

4. Click **Yes**.

Result: The Easy Lockdown policy is deleted.

Exporting Easy Lockdown Policies

You can export a list of policies to a `csv` (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a `csv` file with the following columns:

Name	Description
Status	Enabled or Disabled
Policy Name	The name of the policy
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)
Policy Type	The type of policy (Easy Lockdown, Trusted Updater, and so on)
Blocking	Off, On, Authorized, Non-authorized, or (Authorized, Non-authorized)
Logging	Authorized, Non-authorized, or Off

Name	Description
Last Updated Date	The date the policy was last changed

Working with Denied Applications Policy

Administrators can use a Denied Applications policy to add applications to a blacklist of applications that are not authorized to run. It can be used to block applications that are considered dangerous, unnecessary, or unproductive in the enterprise.

The Denied Applications feature is implemented through the ***Denied Applications Wizard***. The administrator can specify what is to be blocked at file, application, and application group level.

Note: The file, application, and application group structure is configured in the Application Library. See Working with Application Library on page 239 for more information.

The policy is then applied to specified endpoints or endpoint groups, and users. Whenever a user attempts to run a blacklisted application, a warning dialog is displayed, explaining that the application can not run on that endpoint (or for that user).

Denied Applications in Practice

A Denied Applications policy that blocks an application from running can be applied at any time and always overrides any permission the application has to run.

Denied Applications policies are often applied after an administrator reviews application usage on the network. The process usually begins with Easy Auditor and continues through Easy Lockdown. Easy Auditor allows new applications to run even though it does not add them to the whitelist. If an administrator decides that an application is undesirable, it can be added to a Denied Applications policy so that attempts to run it will be blocked.

You can also use Denied Applications policies to block undesirable applications (such as hacking tools, music streaming software, or unapproved messaging programs) even if they are not currently on the network. To do this, you install the unwanted software on a test endpoint, scan with Easy Auditor, group it in Application Library, and apply a Denied Applications policy.

Important: A Denied Applications policy always overrides any permission to run granted by any other Application Control policy.

Note: Some Windows 8 applications are developed with JavaScript/HTML. It is not possible to block these script-based applications.

Creating a Denied Applications Policy

You can create a Denied Applications policy that blocks execution of specific applications on endpoints and groups, for specified users.

1. Select **Manage** > **Application Control Policies**.

2. Select **Create** > **Denied Applications Policies**.

   Step Result: The ***Denied Applications Wizard*** opens to the ***Deny execution for the listed applications*** page.

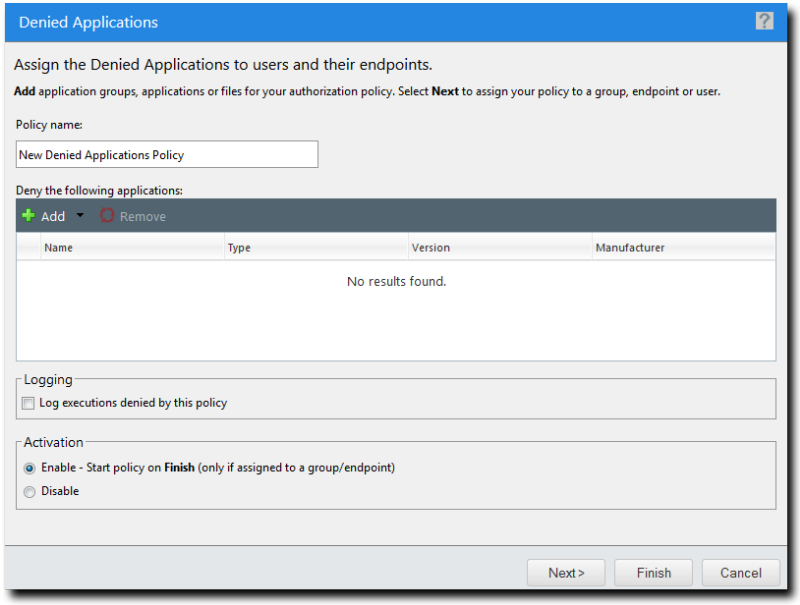


Figure 36: Denied Applications Wizard

3. Type a name for the new Denied Applications policy.

Note: Give the policy a descriptive name. For example, if this Denied Applications policy relates to unauthorized browsers, you could name it `Unauthorized Browsers Policy`.

4. Build a list of denied applications (based on application groups, applications, or individual files):

Method	Steps
To add application groups:	1. Click **Add** > **Application Groups**. 2. Enter an application group name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Application Groups**. 6. Click **OK**.

Method	Steps
To add applications:	1. Click **Add** > **Applications**. 2. Enter an application name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Applications**. 6. Click **OK**.
To add files:	1. Click **Add** > **Files**. 2. Enter a file name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Files**. 6. Click **OK**.

Note: The application groups, applications, and files available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

Step Result: One or more application groups, applications or files are displayed in the **Assigned List**.

5. Select **Log executions denied by this policy** if you want a record of the attempts to run the denied application(s).

Note: Even if this control is not selected, logging may occur when other policy types (such as Easy Auditor or Easy Lockdown) have logging enabled.

6. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to at least one endpoint or group and one user.
Disable	The policy will be disabled once created, even if it is assigned to an endpoint/group and user. You can enable it at a later time.

7. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints or users. You can assign the policy at a later time.

Step Result: The ***Denied Applications Wizard*** opens to the ***Assign the Denied Applications to groups, endpoints, and/or users*** page.

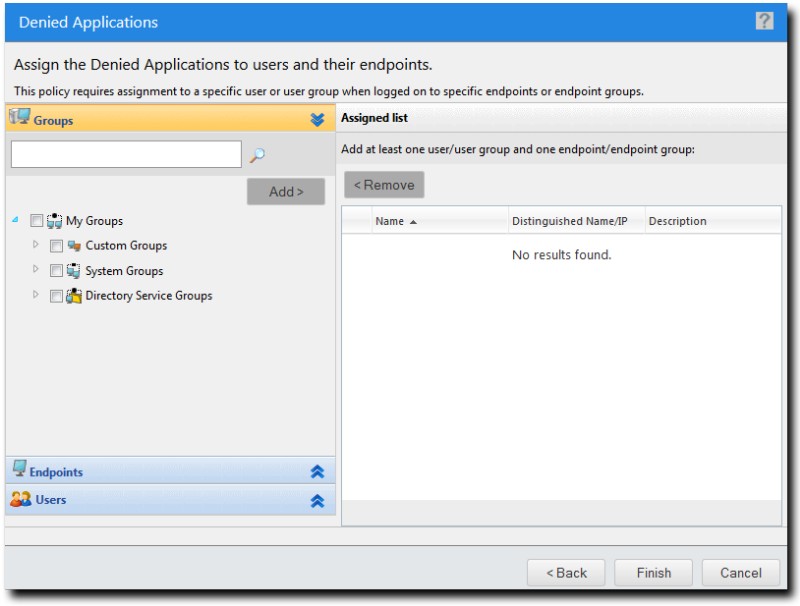


Figure 37: Denied Applications Wizard

8. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

9. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

10. Click **Finish**.

Result: The Denied Applications policy is created and assigned to the selected user(s) and endpoint(s). The new policy is displayed on the ***Managed Policies*** tab.

Tip: When endpoint users get multiple blocked application notifications, they can close them all at once by right-clicking on the task bar icon for the notifications and selecting **Close all windows**.

Adding Application Groups to a Policy

You can add application groups to a Denied Applications policy or a Supplemental Easy Lockdown/ Auditor policy using the ***Add Application Groups*** dialog.

This dialog is accessed by clicking the **Add** button on the ***Denied Applications*** dialog or the **Authorize** button on the ***Supplemental Easy Lockdown/Auditor*** wizard, then selecting **Application Groups** from the dropdown.

Note: The application groups available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

1. Type the name of an application group in the search field.

   Note: Sub-string matching is supported, so you do not have to type the application group's full name. Typing a partial name may result in multiple matches.

2. Click **Search**.
3. Select the required application group(s).
4. Click **Add Application Groups**.

   Step Result: The selected application groups are added to the list.

   Note: You can remove an application group from the list if required by selecting it and clicking **Unassign**.

5. Click **OK**.

Result: Application groups are added to the policy. The dialog closes and you return to the wizard.

Adding Applications to a Policy
You can add applications to a Denied Applications policy or a Supplemental Easy Lockdown/Auditor policy using the ***Add Applications*** dialog.

This dialog is accessed by clicking the **Add** button on the ***Denied Applications*** dialog or the **Authorize** button on the ***Supplemental Easy Lockdown/Auditor*** wizard, then selecting **Applications** from the dropdown.

Note: The applications available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

1. Type the name of an application in the search field.

   Note: Sub-string matching is supported, so you do not have to type the application's full name. Typing a partial name may result in multiple matches.

2. Click **Search**.
3. Select the required application(s).
4. Click **Add Applications**.

   Step Result: The selected applications are added to the list.

   Note: You can remove an application from the list if required by selecting it and clicking **Unassign**.

5. Click **OK**.

Result: Applications are added to the policy. The dialog closes and you return to the wizard.

Adding Files to a Policy

You can add files to a Denied Applications policy or a Supplemental Easy Lockdown/Auditor policy using the ***Add Files*** dialog.

This dialog is accessed by clicking the **Add** button on the ***Denied Applications*** dialog or the **Authorize** button on the ***Supplemental Easy Lockdown/Auditor*** wizard, then selecting **Files** from the dropdown.

Note: The files available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

1. Type the name of a file in the search field.

   Note: Sub-string matching is supported, so you do not have to type the file's full name. Typing a partial name may result in multiple matches.

2. Click **Search**.
3. Select the required file(s).
4. Click **Add Files**.

   Step Result: The selected files are added to the list.

   Note: You can remove a file from the list if required by selecting it and clicking **Unassign**.

5. Click **OK**.

Result: Files are added to the policy. The dialog closes and you return to the wizard.

Removing Applications from a Denied Applications Policy

You can remove applications from a Denied Applications policy.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select a Denied Applications policy.

   Step Result: The selected policy is highlighted.

3. Click **Edit**.

   Step Result: The ***Denied Applications Wizard*** opens.

4. Select the application(s) you want to remove from the Denied Applications policy.

   Note: Applications can be defined at file, application, and application group level in the Application Library.

   Step Result: The **Remove** button is enabled.

5. Click **Remove**.

   Step Result: A confirmation dialog is displayed.

6. Click **Yes**.
7. Click **Finish**.

Result: The specified application groups, applications or files are removed from the Denied Applications policy.

Adding an Individual User to a Policy

You can add one or more individual users to a policy using the ***Add Individual Users*** dialog.

This dialog is accessed by clicking the **Add Individual User** button on a **User** pane. This feature is available on wizards that support user assignment.

1. Search for users using either of the following methods:

Option	Steps
Search for all users	Leave the **Username** field blank and click **Search**. This returns all existing users in the current domain.
Search for one or more selected users	1. Type a user name in the **Username** field. **Note:** Sub-string matching is supported, so you do not have to type the full name. Typing a partial name may result in multiple matches 2. Click **Search**.

   Step Result: One or more users appear in the results list.

   Note: If you cannot find the user(s) you want, try searching other available domains. Select a searchable domain controller from the **Domain** drop-down list.

2. Select one or more users.
3. Click **Add Users**.

   Step Result: The users are added to the selection list.

4. Click **OK**.

   Step Result: The ***Add Individual Users*** dialog closes and you return to the **Users** pane of the policy wizard, with the new user(s) added to the **Users** list.

Assigning a Denied Applications Policy

You can select an existing Denied Applications policy and assign it to endpoints/endpoint groups and users/user groups.

A Denied Applications policy requires both an endpoint/endpoint group *and* a user/user group assignment.

1. Select **Manage** > **Application Control Policies**.

   Step Result: The ***Managed Policies*** tab on the ***Application Control Policies*** page is displayed.

2. Select a Denied Applications policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the required Denied Application policy.

   Step Result: The selected policy is highlighted.

3. Click **Assign**.

   Step Result: The ***Denied Applications*** dialog is displayed.

4. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

5. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

6. Click **OK**.

Result: The Denied Application policy is assigned to selected endpoints/endpoint groups and users/user groups.

Unassigning a Denied Applications Policy

You can unassign a Denied Applications policy, removing the link to the endpoints and users it was assigned to. Policies that are no longer assigned remain in the system as unassigned policies, which you can re-assign to endpoints and users at a later time.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select one or more Denied Applications policies.

Tip: Filter the **Policy Name** and **Policy Type** columns to locate required policies.

Step Result: The selected policies are highlighted.

3. Click **Unassign**.

   Step Result: One of two confirmation dialogs is displayed, depending on whether you selected a single policy or multiple policies.

Figure 38: Unassign Application Control Policy

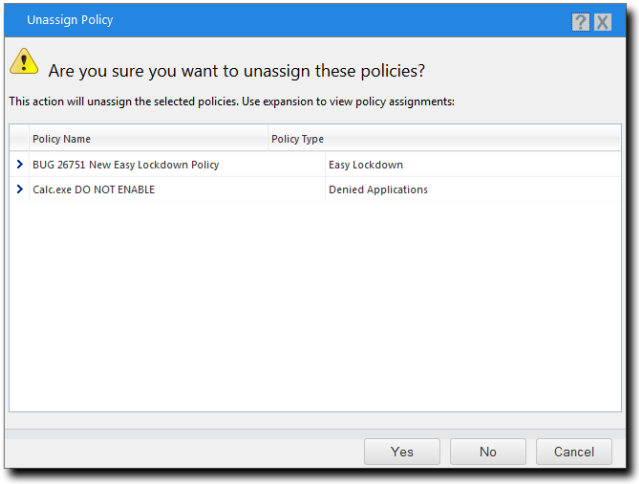


Figure 39: Unassign Multiple Application Control Policies

4. Click **Yes**.

Result: One or more Denied Applications policies are unassigned.

Editing a Denied Applications Policy

You can edit a Denied Application policy and, for example, change the logging option or the endpoints to which it is assigned.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select a Denied Applications policy.

   Note: You can only edit one policy at a time.

   Step Result: The selected policy is highlighted.

3. Click **Edit**.

   Step Result: The ***Denied Applications Wizard*** opens.

4. [Optional] Edit the **Policy Name**.
5. [Optional] Add one or more applications to the blacklist of denied applications (based on application groups, applications, or individual files):

Method	Steps
To add application groups:	1. Click **Add** > **Application Groups**. The ***Add Application Groups*** dialog opens. 2. Enter an application group name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Application Groups**. 6. Click **OK**.
To add applications:	1. Click **Add** > **Applications**. The ***Add Applications*** dialog opens. 2. Enter an application name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Applications**. 6. Click **OK**.
To add files:	1. Click **Add** > **Files**. The ***Add Files*** dialog opens. 2. Enter a file name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Files**. 6. Click **OK**.

Note: The application groups, applications, and files available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

Step Result: One or more application groups, applications or files are added to the blacklist.

6. [Optional] Remove one or more applications from the blacklist of denied applications:
   a) Select one or more applications from the list.
   b) Click **Remove**.

7. [Optional] Change the **Logging** option.

Note: Even if this control is not selected, logging may occur when other policy types (such as Easy Auditor or Easy Lockdown) have logging enabled.

8. [Optional] Change the **Activation** option.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

9. Click **Next**.

Step Result: The ***Denied Application Wizard*** opens to the ***Assign the Denied Applications to groups, endpoints and/or users*** page.

10. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

11. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	**1.** Select one or more users from the **Users** list. **2.** Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	**1.** Select one or more users from the **Assigned list**. **2.** Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

12. Click **Finish**.

Result: The Denied Applications policy is edited.

Disabling a Denied Applications Policy

You can disable a Denied Applications policy without deleting it. The details of the policy are retained and you can enable it again at a later time.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control policies is displayed.

2. Select the enabled policies that you want to disable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

3. Click **Disable**.

Result: The selected Denied Applications policy or policies are disabled.

Enabling a Denied Applications Policy

You can enable a Denied Applications policy that is currently disabled.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control policies is displayed.

2. Select the check box(es) for the disabled Denied Applications policies that you want to enable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

3. Click **Enable**.

Result: The selected Denied Applications policies are enabled.

Deleting a Denied Application Policy

You can delete a Denied Application policy, as long as it is not assigned to any endpoint.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control Policies is displayed.

2. Select the required Denied Applications policy.

   Note: The policy must not be assigned to an endpoint (**Assigned** column value of *Not Assigned*). If it is assigned, you must first unassign it to continue.

   Step Result: The selected policy is highlighted.

3. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned.

4. Click **Yes**.

Result: The Denied Applications policy is deleted.

Exporting Denied Applications Policies

You can export a list of Denied Applications Policies to a `csv` (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a `csv` file with the following columns:

Name	Description
Status	Enabled or Disabled
Policy Name	The name of the policy
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)

Name	Description
Policy Type	The type of policy (Denied Applications, Trusted Updater, and so on)
Blocking	Off, On, Authorized, Non-authorized, or (Authorized, Non-authorized)
Logging	Authorized, Non-authorized, or Off
Last Updated Date	The date the policy was last changed

Working with Supplemental Easy Lockdown/Auditor Policy

Administrators can use a Supplemental Easy Lockdown/Auditor policy to add applications to an endpoint's whitelist, thereby authorizing the applications to run. This is a good way to authorize an application after Easy Lockdown.

This feature is implemented through the ***Supplemental Easy Lockdown/Auditor Policy Wizard***. The administrator can specify what is to be authorized at file, application, and application group level, based on what is configured in Application Library.

Important: A Supplemental Easy Lockdown/Auditor policy can only be applied to an endpoint that already has a whitelist, created when Easy Auditor or Easy Lockdown was applied.

Even though based on endpoint whitelists, the Supplemental Easy Lockdown/Auditor policy provides convenient centralized control for whitelisting applications.

Supplemental Easy Lockdown/Auditor in Practice

A Supplemental Easy Lockdown/Auditor policy is a good method for authorizing a new application after Easy Lockdown has been put in place.

When an Easy Lockdown policy is in place and running smoothly, it is not a good idea to disable it to install a new application. Rescanning the endpoints takes time and authorizes possibly undesirable software that may be present on endpoints. It is better to authorize the new application using a Supplemental Easy Lockdown/Auditor policy. This can be done in the following way:

- Install the application on an endpoint that is not locked down.
- Use Easy Auditor to scan the endpoint and add the application's executables and installer to Application Library.
- Create a Supplemental Easy Lockdown/Auditor policy for the application.
- Assign this policy to the users and locked-down endpoints that need it.

A Supplemental Easy Lockdown/Auditor policy is also useful for authorizing an application or upgrade that is being deployed in stages. For example, when a new version of an application is being rolled out in the enterprise, it is often deployed one department or group at a time. In this scenario the administrator can authorize the new version with a Supplemental Easy Lockdown/Auditor policy, adding it to all endpoint whitelists. Then, as the endpoints in each group get upgraded with the

new version, the application can run without the need to reapply Easy Lockdown or assign a trust mechanism to it.

Creating a Supplemental Easy Lockdown/Auditor Policy

You can create a Supplemental Easy Lockdown/Auditor policy that allows execution of specific applications on endpoints and groups, for specified users.

1. Select **Manage** > **Application Control Policies**.
2. Select **Create** > **Supplemental Easy Lockdown/Auditor Policy**.

   Step Result: The ***Supplemental Easy Lockdown/Auditor Policy Wizard*** opens to the ***Allow execution for the listed applications*** page.

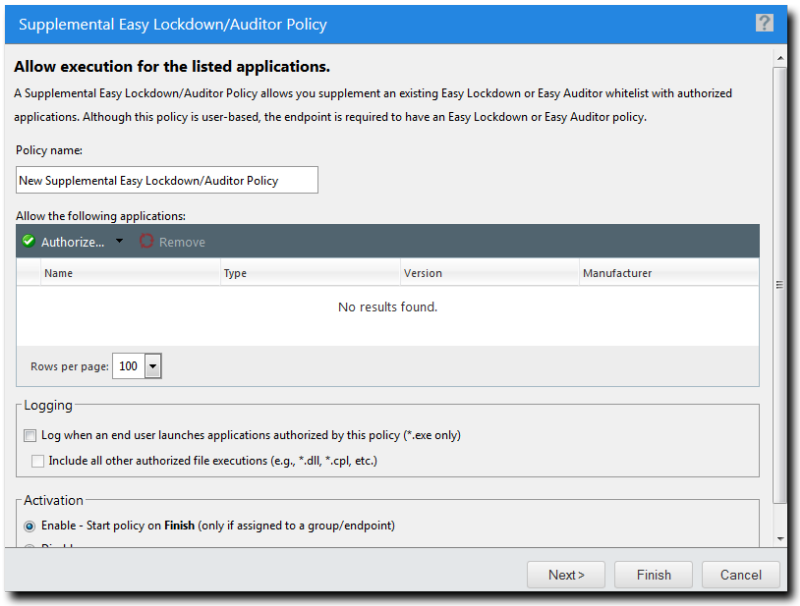


Figure 40: Supplemental Easy Lockdown/Auditor Policy Wizard

3. Type a name for the new Supplemental Easy Lockdown/Auditor policy.

Note: Give the policy a descriptive name. For example, if this policy relates to authorized browsers, you could name it `Authorized Browsers Policy`.

4. Build a list of authorized applications (based on application groups, applications, or individual files):

Method	Steps
To add application groups:	1. Click **Authorize** > **Application Groups**. The ***Add Application Groups*** dialog opens. 2. Enter a full or partial application group name in the search field, or leave it empty to return all values. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Application Groups**. 6. Click **OK**.
To add applications:	1. Click **Authorize** > **Applications**. The ***Add Applications*** dialog opens. 2. Enter a full or partial application name in the search field, or leave it empty to return all values. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Applications**. 6. Click **OK**.
To add files:	1. Click **Authorize** > **Files**. The ***Add Files*** dialog opens. 2. Enter a full or partial file name in the search field, or leave it empty to return all values. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Files**. 6. Click **OK**.

Note: The application groups, applications, and files available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

Step Result: One or more application groups, applications or files are displayed in the **Assigned List**.

5. Select the **Logging** options.

Option	Description
Log when an end user launches applications authorized by this policy (*.exe only)	Track the launches of the application's initial excutable file only.
Include all other authorized file executions (e.g. *.dll, *.cpl, etc.)	Track the launches of all executable files associated with the application.

6. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to at least one endpoint or group and one user.
Disable	The policy will be disabled once created, even if it is assigned to an endpoint/group and user. You can enable it at a later time.

7. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints or users. You can assign the policy at a later time.

Step Result: The ***Supplemental Easy Lockdown/Auditor Policy Wizard*** opens to the ***Assign the Supplemental Easy Lockdown/Auditor Policy to groups, endpoints, and/or users*** page.

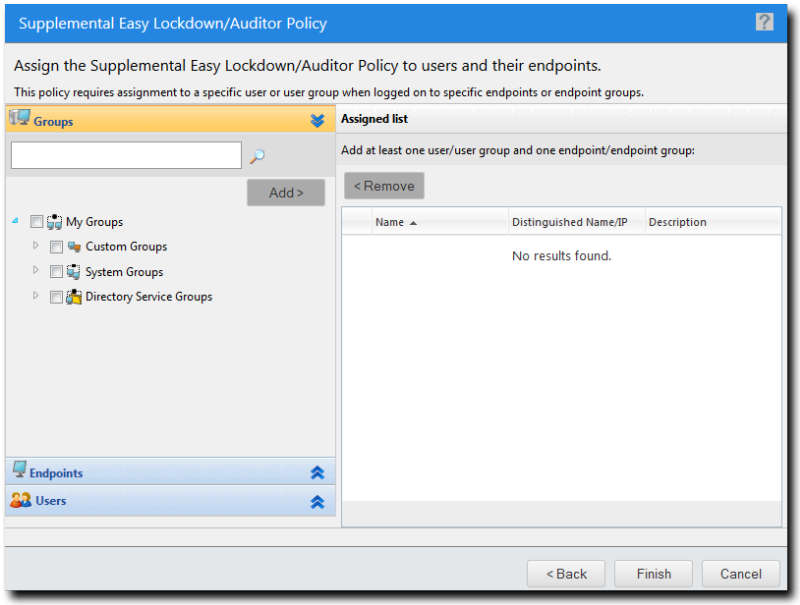


Figure 41: Assign the Supplemental Easy Lockdown/Auditor Policy to groups, endpoints, and/or users page

8. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

9. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the Add Individual User button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

10. Click **Finish**.

Result: The Supplemental Easy Lockdown/Auditor Policy is assigned to endpoints/endpoint groups and users.

Adding Application Groups to a Supplemental Easy Lockdown/AuditorPolicy

You can add application groups to a Supplemental Easy Lockdown/Auditor policy using the ***Add Application Groups*** dialog.

This dialog is accessed by clicking the **Authorize** button on the ***Supplemental Easy Lockdown/ Auditor*** wizard, then selecting **Application Groups** from the dropdown.

Note: The application groups available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

1. Type the name of an application group in the search field.

Note: Sub-string matching is supported, so you do not have to type the application group's full name. Typing a partial name may result in multiple matches.

2. Click **Search**.
3. Select the required application group(s).
4. Click **Add Application Groups**.

   Step Result: The selected application groups are added to the list.

   Note: You can remove an application group from the list if required by selecting it and clicking **Unassign**.

5. Click **OK**.

Result: Application groups are added to the Supplemental Easy Lockdown/Auditor policy, the dialog closes and you return to the wizard.

Adding Applications to a Supplemental Easy Lockdown/Auditor Policy
You can add applications to a Supplemental Easy Lockdown/Auditor policy using the ***Add Applications*** dialog.

This dialog is accessed by clicking the **Authorize** button on the ***Supplemental Easy Lockdown/ Auditor*** wizard, then selecting **Applications** from the dropdown.

Note: The applications available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

1. Type the name of an application in the search field.

   Note: Sub-string matching is supported, so you do not have to type the application's full name. Typing a partial name may result in multiple matches.

2. Click **Search**.
3. Select the required application(s).
4. Click **Add Applications**.

   Step Result: The selected applications are added to the list.

   Note: You can remove an application from the list if required by selecting it and clicking **Unassign**.

5. Click **OK**.

Result: Applications are added to the Supplemental Easy Lockdown/Auditor policy, the dialog closes and you return to the wizard.

Adding Files to a Supplemental Easy Lockdown/Auditor Policy

You can add files to a Supplemental Easy Lockdown/Auditor policy using the ***Add Files*** dialog.

This dialog is accessed by clicking the **Authorize** button on the ***Supplemental Easy Lockdown/ Auditor*** wizard, then selecting **Files** from the dropdown.

Note: The files available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

1. Type the name of a file in the search field.

   Note: Sub-string matching is supported, so you do not have to type the file's full name. Typing a partial name may result in multiple matches.

2. Click **Search**.
3. Select the required file(s).
4. Click **Add Files**.

   Step Result: The selected files are added to the list.

   Note: You can remove a file from the list if required by selecting it and clicking **Unassign**.

5. Click **OK**.

Result: Files are added to the Supplemental Easy Lockdown/Auditor policy, the dialog closes and you return to the wizard.

Removing Applications from a Supplemental Easy Lockdown/Auditor Policy

You can remove applications from a Supplemental Easy Lockdown/Auditor policy.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select a Supplemental Easy Lockdown/Auditor policy.

   Step Result: The selected policy is highlighted.

3. Click **Edit**.

   Step Result: The ***Supplemental Easy Lockdown/Auditor Wizard*** opens.

4. Select the application(s) you want to remove from the Denied Applications policy.

   Note: Applications can be defined at file, application, and application group level in the Application Library.

   Step Result: The **Remove** button is enabled.

5. Click **Remove**.

   Step Result: A confirmation dialog is displayed.

6. Click **Yes**.
7. Click **Finish**.

Result: The specified application groups, applications or files are removed from the Supplemental Easy Lockdown/Auditor policy.

Adding an Individual User to a Policy

You can add one or more individual users to a policy using the ***Add Individual Users*** dialog.

This dialog is accessed by clicking the **Add Individual User** button on a **User** pane. This feature is available on wizards that support user assignment.

1. Search for users using either of the following methods:

Option	Steps
Search for all users	Leave the **Username** field blank and click **Search**. This returns all existing users in the current domain.
Search for one or more selected users	1. Type a user name in the **Username** field. **Note:** Sub-string matching is supported, so you do not have to type the full name. Typing a partial name may result in multiple matches 2. Click **Search**.

   Step Result: One or more users appear in the results list.

   Note: If you cannot find the user(s) you want, try searching other available domains. Select a searchable domain controller from the **Domain** drop-down list.

2. Select one or more users.
3. Click **Add Users**.

   Step Result: The users are added to the selection list.

4. Click **OK**.

   Step Result: The ***Add Individual Users*** dialog closes and you return to the **Users** pane of the policy wizard, with the new user(s) added to the **Users** list.

Assigning a Supplemental Easy Lockdown/Auditor Policy

You can select an existing Supplemental Easy Lockdown/Auditor policy and assign it to endpoints/endpoint groups and users/user groups.

A Supplemental Easy Lockdown/Auditor policy requires both an endpoint/endpoint group *and* a user/user group assignment.

1. Select **Manage** > **Application Control Policies**.

   Step Result: The ***Managed Policies*** tab on the ***Application Control Policies*** page is displayed.

2. Select a Supplemental Easy Lockdown/Auditor policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the required Supplemental Easy Lockdown/Auditor policy.

   Step Result: The selected policy is highlighted.

3. Click **Assign**.

   Step Result: The ***Supplemental Easy Lockdown/Auditor*** dialog is displayed.

4. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

5. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

6. Click **OK**.

Result: The Supplemental Easy Lockdown/Auditor policy is assigned to selected endpoints/endpoint groups and users/user groups.

Assigning a Supplemental Easy Lockdown/Auditor Policy to an Endpoint

You can assign a Supplemental Easy Lockdown/Auditor policy to a selected endpoint.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.

2. In the **Endpoint Name** column, click an endpoint link.

   Step Result: Detailed information for the selected endpoint is displayed.

3. Select the ***Application Control Policies*** tab.

   Step Result: A list of Application Control policies assigned to the endpoint is displayed.

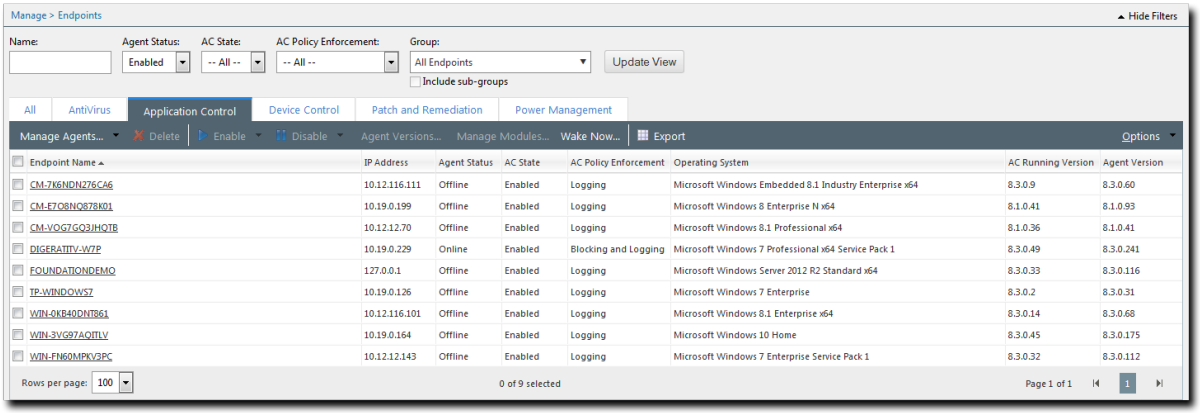


Figure 42: Application Control Policies Tab

4. From the toolbar, select **Assign** > **Supplemental Easy Lockdown/Auditor Policy**.

   Step Result: The ***Assign Policy*** dialog is displayed, listing existing Supplemental Easy Lockdown/Auditor policies.

5. Select one or more Supplemental Easy Lockdown/Auditor policies.

   Note: If multiple Supplemental Easy Lockdown/Auditor policies are assigned to a group, policy settings may conflict. Go to Multiple Policy Resultant Value Rules on page 225 to see how these conflicts are resolved.

6. Click **OK**.

Result: One or more Supplemental Easy Lockdown/Auditor policies are assigned to the group.

Unassigning a Supplemental Easy Lockdown/Auditor Policy

You can unassign a Supplemental Easy Lockdown/Auditor policy, removing the association between it and its endpoints and users. Policies that are no longer assigned remain in the system as unassigned policies, which you can re-assign to endpoints and users at a later time.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select one or more Supplemental Easy Lockdown/Auditor policies.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate required policies.

   Step Result: The selected policies are highlighted.

3. Click **Unassign**.

   Step Result: One of two confirmation dialogs is displayed, depending on whether you selected a single policy or multiple policies.

Figure 43: Unassign Application Control Policy

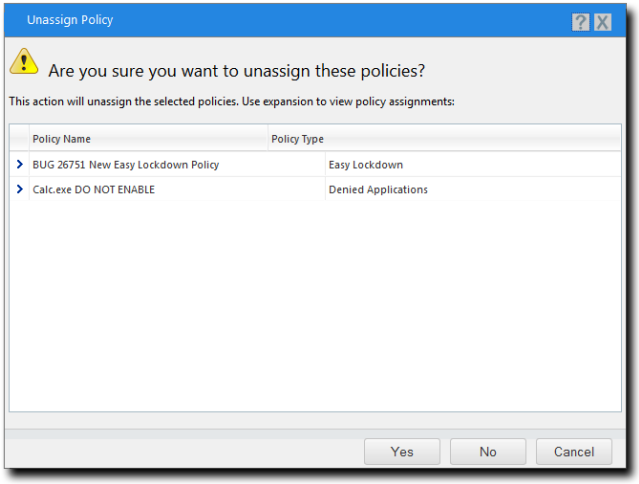


Figure 44: Unassign Multiple Application Control Policies

4. Click **Yes**.

Result: One or more Supplemental Easy Lockdown/Auditor policies are unassigned.

Editing a Supplemental Easy Lockdown/Auditor Policy

You can edit a Supplemental Easy Lockdown/Auditor policy and, for example, change the logging options or the endpoints to which it is assigned.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of policies is displayed.

2. Select a Supplemental Easy Lockdown/Auditor policy.

   Note: You can only edit one policy at a time.

   Step Result: The selected policy is highlighted.

3. Click **Edit**.

   Step Result: The ***Supplemental Easy Lockdown/Auditor Policy Wizard*** opens.

4. [Optional] Edit the **Policy Name**.
5. [Optional] Add more applications to the whitelist (based on application groups, applications, or individual files):

Method	Steps
To add application groups:	1. Click **Add** > **Application Groups**. The ***Add Application Groups*** dialog opens. 2. Enter an application group name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Application Groups**. 6. Click **OK**.
To add applications:	1. Click **Add** > **Applications**. The ***Add Applications*** dialog opens. 2. Enter an application name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Applications**. 6. Click **OK**.
To add files:	1. Click **Add** > **Files**. The ***Add Files*** dialog opens. 2. Enter a file name in the search field. 3. Click **Search**. 4. Select one or more of the results. 5. Click **Add Files**. 6. Click **OK**.

Note: The application groups, applications, and files available through this dialog are based on the contents of the Application Library. See Working with Application Library on page 239 for more information.

Step Result: One or more application groups, applications or files are added to the whitelist.

6. [Optional] Remove one or more applications from the whitelist of authorized applications:
   a) Select one or more applications from the list.
   b) Click **Remove**.

7. [Optional] Change the **Logging** option.

Note: Even if this control is not selected, logging may occur when other policy types (such as Easy Auditor or Easy Lockdown) have logging enabled.

8. [Optional] Change the **Activation** option.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

9. Click **Next**.

Step Result: The ***Supplemental Easy Lockdown/Auditor Wizard*** opens to the ***Assign the Supplemental Easy Lockdown/Auditor Policy to groups, endpoints and/or users*** page.

10. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

11. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

12. Click **Finish**.

Result: The Supplemental Easy Lockdown/Auditor policy is edited.

Disabling a Supplemental Easy Lockdown/Auditor Policy

You can disable a Supplemental Easy Lockdown/Auditor policy without deleting it. The details of the policy are retained and you can enable it again at a later time.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control managed policies is displayed.

2. Select the enabled Supplemental Easy Lockdown/Auditor policy or policies that you want to disable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

3. Click **Disable**.

Result: The selected Supplemental Easy Lockdown/Auditor policy or policies are disabled.

Enabling a Supplemental Easy Lockdown/Auditor Policy

You can enable a Supplemental Easy Lockdown/Auditor policy that is currently disabled.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control managed policies is displayed.

2. Select the check box for the disabled Supplemental Easy Lockdown/Auditor policy that you want to enable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

3. Click **Enable**.

Result: The selected Supplemental Easy Lockdown/Auditor policy is enabled.

Deleting a Supplemental Easy Lockdown/Auditor Policy

You can delete a Supplemental Easy Lockdown/Auditor policy, as long as it is not assigned to any endpoint.

1. Select **Manage** > **Application Control Policies**.

   Step Result: A list of Application Control policies is displayed.

2. Select the required Supplemental Easy Lockdown/Auditor policy.

   Note: The policy must not be assigned to an endpoint (**Assigned** column value of *Not Assigned*). If it is assigned, you must first unassign it to continue.

   Step Result: The selected policy is highlighted.

3. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned.

4. Click **Yes**.

Result: The Supplemental Easy Lockdown/Auditor policy is deleted.

Exporting Supplemental Easy Lockdown/Auditor Policies

You can export a list of Supplemental Easy Lockdown/Auditor Policies to a `csv` (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a `csv` file with the following columns:

Name	Description
Status	Enabled or Disabled
Policy Name	The name of the policy

Name	Description
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)
Policy Type	The type of policy (Denied Applications, Trusted Updater, and so on)
Blocking	Off, On, Authorized, Non-authorized, or (Authorized, Non-authorized)
Logging	Authorized, Non-authorized, or Off
Last Updated Date	The date the policy was last changed

Chapter 6

Using Trusted Change

In this chapter:

Ivanti Application Control uses the concept of *trusted change* to manage applications that are not on endpoint whitelists. This allows administrators to maintain a locked-down system as proposed changes are automatically vetted and approved or denied based on policy.

Even after application control is enforced, there is a need to add and update applications. Administrators can maintain endpoint integrity without a heavy administrative burden using the following Trusted Change policies:

- *Trusted Updater* allows applications to modify files and add them to the whitelist.
- *Trusted Publisher* allows digitally signed applications from a trusted source to run.
- *Trusted Path* allows applications in a specified system path to run.
- *Local Authorization* allows specified users to authorize new applications.

Trusted Change Policies

Ivanti Application Control provides four *Trusted Change* policies which allow non-whitelisted applications to execute. This reduces the administrative burden of maintaining the network after application control is enforced.

Trusted Updater	Trusted Updater allows an application to run and to add or update files on an endpoint. Files added or updated can also run because they are added to the whitelist. This is the only Trusted Change policy that can add files to an endpoint's whitelist. See Working with Trusted Updater on page 144.

Trusted Publisher	Trusted Publisher is a trusted source that digitally signs files and applications through a certificate so that executables are allowed to run on endpoints without each file/application having to be authorized independently. See Working with Trusted Publisher on page 166.
Trusted Path	Trusted Path is a file system path configured so that any executable files it contains can be run by all users/endpoints that have been assigned the Trusted Path policy. See Working with Trusted Path on page 185.
Local Authorization	Local Authorization is a policy that allows a specified user to authorize an application that is not on a whitelist or permitted by another trust mechanism. See Working with Local Authorization on page 206.

Logging Trusted Change Policies

Logging options selected in Easy Auditor and Easy Lockdown policies can determine the logging behavior of trusted change policies.

Trusted Path is the only trusted change policy with its own logging options. But Trusted Updater and Trusted Publisher events can be logged by setting Easy Auditor/Easy Lockdown logging options.

The logging options set on Easy Lockdown and Easy Auditor policies have the following effect on trusted change policies:

Log non-authorized applications option	
Trusted Updater	Logs when applications are added to the whitelist by Trusted Updater.
Trusted Publisher	No effect
Trusted Path	No effect

Log authorized applications option	
Trusted Updater	Logs when applications are added to the whitelist by Trusted Updater. Logs when applications whitelisted by Trusted Updater are allowed to run.
Trusted Publisher	Logs when applications are allowed to run by Trusted Publisher policies.
Trusted Path	Logs when applications are allowed to run by Trusted Path policies. This overrides the setting in the Trusted Path policy.

Include all details on authorized applications option	
Trusted Updater	No effect
Trusted Publisher	No effect
Trusted Path	Detailed information on applications allowed to run by the Trusted Path policy is logged (every executable file and library loaded will be logged). This overrides the setting in the Trusted Path policy.

Unassigning Multiple Policies

You can unassign multiple application control policies at the same time, removing the association between them and their assigned endpoints and users. Policies that are no longer assigned to an endpoint remain in the system as unassigned policies, which you can re-assign at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click either the **Managed Policies** tab or the **Trusted Change** tab.
3. Select all the policies you want to unassign on that page.

   Note: You can select any combination of the policy types available on the page.

   Step Result: The selected policies are highlighted.

4. Click **Unassign**.

   Step Result: The Unassign Policy confirmation dialog is displayed.

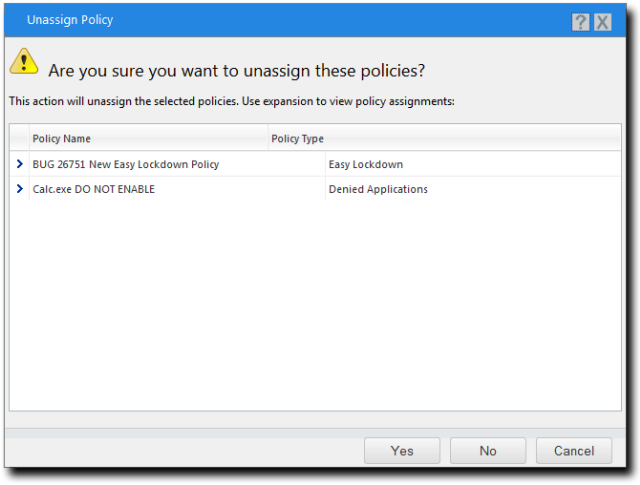


Figure 45: Unassign Multiple Application Control Policies

5. Review the policies to be unassigned. If necessary, click a chevron (**>**) to expand the display of the endpoints and users that a policy is assigned to.

6. Click **Yes**.

Result: The application control policies are unassigned.

Working with Trusted Updater

A Trusted Updater policy allows an administrator to designate an *application updater*, which can add, modify or replace files on an endpoint. The files it adds or updates are added to the endpoint's whitelist and are therefore allowed to execute.

Note: Trusted Updater is the only trusted change policy that can add files to an endpoint's whitelist.

When administrators create a Trusted Updater policy, they have the option to create updaters from a known source or to define their own. A Trusted Updater policy may contain one or more application updaters.

Tip: You can add application updaters for multiple versions of the same executable. This allows the same generalized policy to be applied to large numbers of endpoints without having to know which version of that application updater is running on a given endpoint.

Trusted Updaters are displayed on the ***Trusted Change*** tab of the ***Application Control Policies*** page. You can filter the **Policy Type** column to display only Trusted Updater policies.

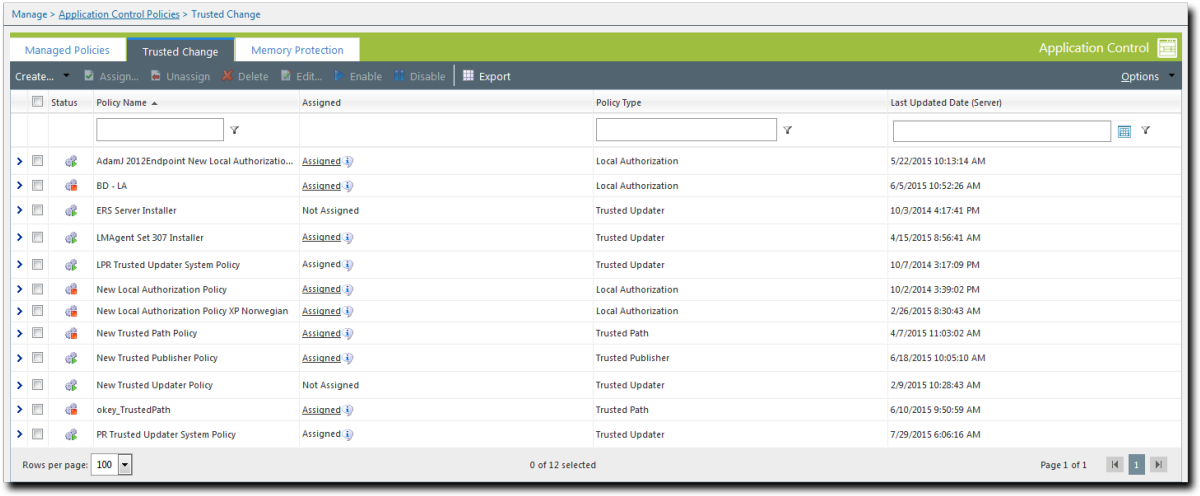


Figure 46: Application Control Policies - Trusted Change Tab

Note: When both Patch and Remediation and Application Control modules are installed, the Patch and Remediation module is treated as a Trusted Updater. It is displayed on the ***Trusted Change*** page as **PR Trusted Updater System Policy**, and is assigned to all endpoints that have Application Control installed.

The Patch and Remediation Trusted Updater differs from other Trusted Updater policies in that it cannot be edited.

Trusted Updater in Practice

A Trusted Updater policy designates a file as an *updater*, a file that can run and that can add other executable files to the endpoint's whitelist.

The primary purpose of Trusted Updater is to enable administrators to automatically install and authorize software patches to update applications that are already installed on the endpoint.

Trusted Updater is the preferred trust mechanism for the following scenarios:

- Ivanti Patch and Remediation installing patches or software from content feeds or customer packages
- Third-party package managers installing patches or software
- An antivirus product updating its engine
- Adobe Updater installing updates to Adobe applications
- Apple Updater installing updates to QuickTime, iTunes, and Safari

Trusted Updater is not intended for installing and authorizing individual software installation packages, such as the `setup.exe` file for a software installer.

There are some situations where Trusted Updater *cannot* be used to install an application. The most common is where an ActiveX component is loaded in a browser as part of the installation. The solution here is to use Trusted Publisher to run the application.

Note: The popular online collaboration program WebEx is an example of the type of program that needs Trusted Publisher to run. See Trusted Publisher in Practice on page 167 for more information.

Identifying the Updater File(s) to Add to a Policy

Many applications include a built-in component that periodically checks for updates, then downloads and installs them automatically.

If an application is installed on an endpoint that is then locked down via Easy Lockdown, it is important that its updater component is defined as a Trusted Updater.

- In some cases the updater's name and location is documented by the application vendor
- The updater component is usually located in the install directory hierarchy of the application e.g. C:\Program Files*manufacturer**application name*
- It may be necessary to add more than one file to the Trusted Updater policy in order for the update to be successful

Identifying the Correct Version of Updater File

It is vital to identify the correct version of the updater file for the Trusted Updater policy, or it will not update the system correctly.

If an updater file in the policy does not exactly match the updater file on the endpoint, it will not update the system correctly. For any given application updater, there is likely to be more than one version on the customer's network. This can happen for a number of reasons:

- Different operating system versions
- 32- and 64-bit versions of the same operating system
- Older, out-of-date machines

The Ivanti Endpoint Security administrator must ensure that the Trusted Updater policy for a given application contains all versions of the application updater files that are present on the endpoints to which the policy is applied.

Trusted Updater and Windows Update

Even after being whitelisted, Windows Update files are not allowed to execute unless they are also Trusted Updaters. This ensures that any new system files they add or modify are automatically whitelisted. You must add the Windows Updates files to a Trusted Updater policy to enable Windows Update to run.

Windows Update is a service that updates Microsoft Windows operating systems and components, using multiple executables. When Easy Lockdown is applied to an endpoint, these executables are added to the whitelist. However, any files that they subsequently add or modify during an update are not automatically added to the whitelist. This would cause endpoint stability issues, so as a precaution Ivanti Application Control does not allow these executables to run unless they are also Trusted Updaters.

If you try to run Windows Update when its files have not been added as Trusted Updaters you get a message saying that Windows Update cannot currently check for updates, or it may check for updates but then fail to install them (the exact message/action depends on the operating system). The attempt is recorded in the All Denied Application Events log.

To allow Windows Update to run, you must add the Windows Update executables as Trusted Updaters. This ensures that any files they add or modify are added to the whitelist and so can execute on locked-down systems.

The following Windows Update files should be added to a Trusted Updater policy:

- WgaTray.exe
- wuapp.exe
- wuauclt.exe
- wuaueng.dll
- wups2.dll
- wusa.exe
- WuSetupV.exe

Note:

- Different versions of these files exist on different endpoints. You must add all versions of each file to the Trusted Updater policy.
- Each Windows system uses a combination of the listed files, but not all of them.
- Files can be added to a Trusted Updater policy directly from the All Denied Application Events log.

Trusted Updater Security Risks

When you add a file to a Trusted Updater policy, every executable file it creates or modifies is added to the whitelist and trusted. This can present a security risk for certain types of files.

There are certain types of executables you should never assign as Trusted Updaters.

Antivirus Scan Engines	Antivirus products often have an updater mechanism that is separate from the virus scanning mechanism. It is important to only trust the updater and not the virus scanner. If you trust the scanner, any time it detects new malware and writes that malware to a quarantine area, that malware would get whitelisted. You would then be relying solely on the antivirus engine to contain that malware.
Web Browsers	Web browser often have an updater mechanism separate from the browser itself. You should only trust the update mechanism, not the browser. If you trust the browser and a user navigates to a site with malicious content, that content could be downloaded and then whitelisted.
Email/Instant Messaging Clients	Only trust the email/IM client's update mechanism, if it has one. If you trust the client itself, mail-borne malware could end up whitelisted on the endpoint.
Media Applications	Media applications frequently download various types of file from the Internet. Such files could contain malware and should not be whitelisted. Trusting the updater rather than the application itself is the correct procedure.
File Sharing Applications	Downloaded files could contain malware so only the application updater mechanism should be trusted, rather than the application itself.

Important: In general, any application that has the capability to add files to the endpoint from the network or Internet is a bad candidate for adding as a Trusted Updater.

Creating a Trusted Updater Policy

A Trusted Updater policy specifies an executable file that is allowed to run on an endpoint. Any executable files added through the trusted executable will also be allowed to run on the endpoint.

Important: Defining an executable file as a Trusted Updater gives a significant capability to that file. Before creating a Trusted Updater policy, make sure you understand the information in Trusted Updater in Practice on page 145 and its related topics, especially Trusted Updater Security Risks on page 147.

Tip: You can also create a new Trusted Updater Policy from the Application Libary. See Trusting Files from the Application Library on page 204.

1. Select **Manage** > **Application Control Policies**.

2. Click the ***Trusted Change*** tab.
3. Select **Create** > **Trusted Updater**.

   Step Result: The ***Trusted Updater Wizard*** opens to the ***Add Application Updaters*** page.

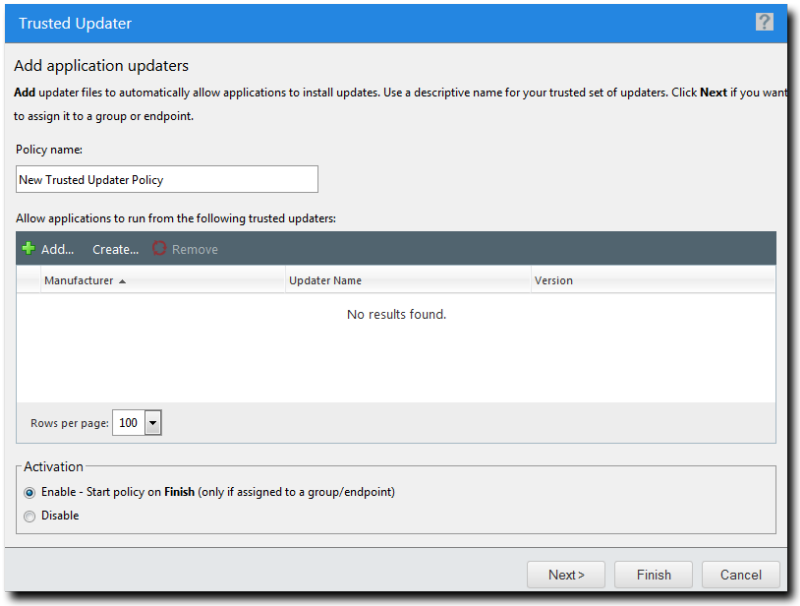


Figure 47: Trusted Updater Wizard - Add Application Updaters Page

4. Type a **Policy Name** for the new Trusted Updater.

Note: Give the policy a descriptive name. For example, if this Trusted Updater policy relates to particular applications used by the graphics department you could name it `Graphics Applications`.

5. Click **Add**.

   Step Result: The ***Add Updaters*** dialog is displayed.

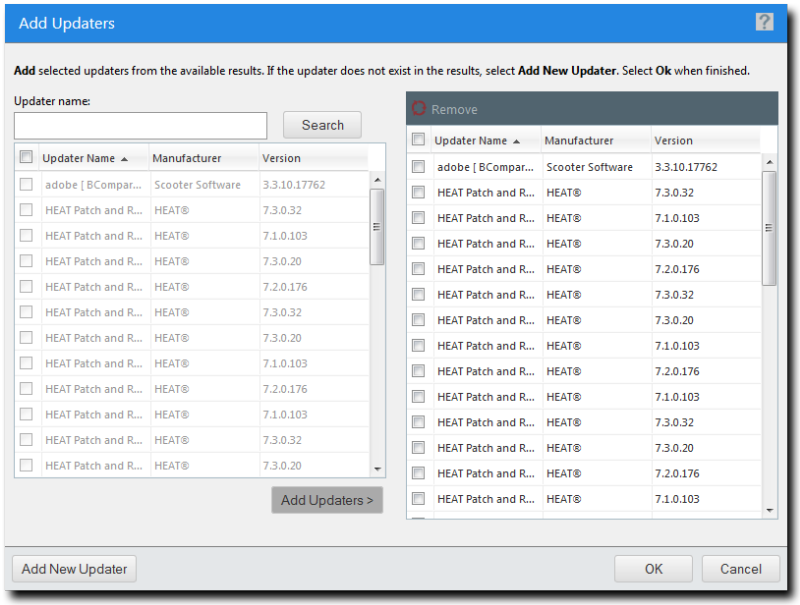


Figure 48: Add Updaters

6. Search for existing Trusted Updaters using either of the following methods:

Option	Steps
Search for all Trusted Updaters	Leave the **Updater name** field blank and click **Search**. This returns all existing Trusted Updaters.
Search for one or more selected Trusted Updaters	**1.** Type a Trusted Updater name in the **Updater name** field. **Note:** Sub-string matching is supported, so you do not have to type the full name. Typing a partial name may result in multiple matches **2.** Click **Search**.

Step Result: One or more Trusted Updaters appears in the results list.

Note: If the list is empty, or you cannot see the updater you want, you will have to add the updater yourself. See Adding a New Trusted Updater on page 152 for more information.

7. Select one or more Trusted Updaters.

8. Click **Add Updaters**.

   Step Result: The Trusted Updaters are added to the policy.

   Note: If you accidentally add an updater, select it and click **Remove**.

9. Click **OK**.

   Step Result: The ***Add Updaters*** dialog closes.

10. [Optional] Edit the **Activation** options.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

11. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time.

Step Result: The ***Trusted Updater Wizard*** opens to the ***Assign Groups and Endpoints*** page.

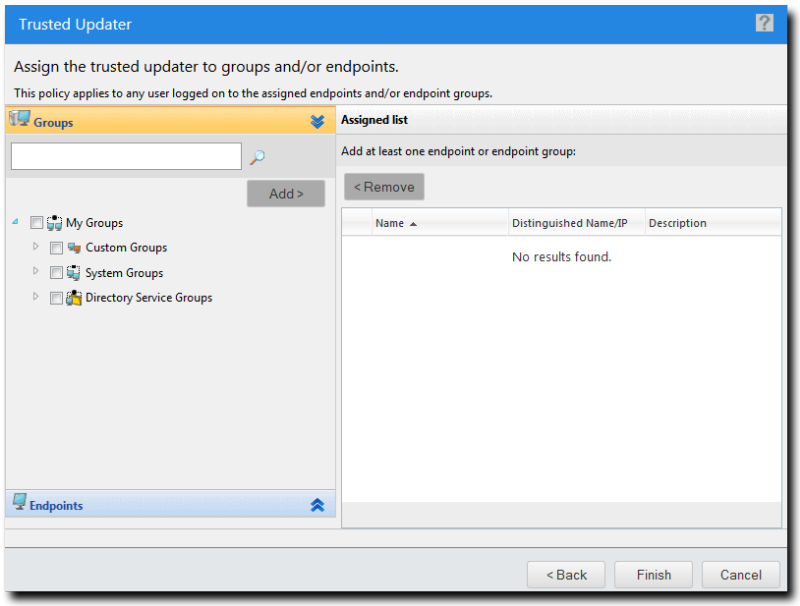


Figure 49: Trusted Updater Wizard - Assign Groups and Endpoints Page

12.[Optional] Edit the list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	**1.** Select a group or groups from the **Groups** list. **2.** Click **Add >**.
To add individual endpoints:	**1.** Select an endpoint or endpoints from the **Endpoints** list. **2.** Click **Add >**.
To remove groups of endpoints:	**1.** Select a group or groups from the **Assigned List**. **2.** Click **< Remove**.
To remove individual endpoints:	**1.** Select an endpoint or endpoints from the **Assigned List**. **2.** Click **< Remove**.

Note: Use the double-arrows () to switch between groups and endpoints.

13. Click **Finish**.

Result: The Trusted Updater policy is created and assigned to selected groups or endpoints.

Adding an Existing Trusted Updater
An existing Trusted Updater is added to a policy using the ***Add Updaters*** dialog.

This dialog is accessed by clicking the **Add** button on the ***Trusted Updater Wizard***.

1. Search for existing Trusted Updaters using either of the following methods:

Option	Steps
Search for all Trusted Updaters	Leave the **Updater name** field blank and click **Search**. This returns all existing Trusted Updaters.

Option	Steps
Search for one or more selected Trusted Updaters	1. Type a Trusted Updater name in the **Updater name** field. **Note:** Sub-string matching is supported, so you do not have to type the full name. Typing a partial name may result in multiple matches 2. Click **Search**.

Step Result: One or more Trusted Updaters appears in the results list.

Note: If the list is empty, or you cannot see the updater you want, you will have to add the updater yourself. See Adding a New Trusted Updater on page 152 for more information.

2. Select one or more Trusted Updaters.
3. Click **Add Updaters**.

   Step Result: The Trusted Updaters are added to the policy.

4. Click **OK**.

   Step Result: The ***Add Updaters*** dialog closes and you are returned to the ***Trusted Updater Wizard***.

Adding a New Trusted Updater

A new Trusted Updater is added by identifying an executable file and adding it to the list of known updaters. This is done using the ***Add New Updater*** dialog.

This dialog can be accessed from different locations.

- If you know that the application file has not yet been defined as a Trusted Updater you can access it directly from the ***Trusted Updater Wizard***.
- If you are on the **Add Updaters** dialog and you find that the application file has not yet been defined as a Trusted Updater, you can access it from there as well.

1. Open the ***Add New Updater*** dialog.

Context	Steps
From the *Trusted Updater Wizard*:	Click **Create**.

Context	Steps
From the *Add Updaters* dialog:	Click **Add New Updater**.

Step Result: The ***Add New Trusted Updater*** dialog opens.

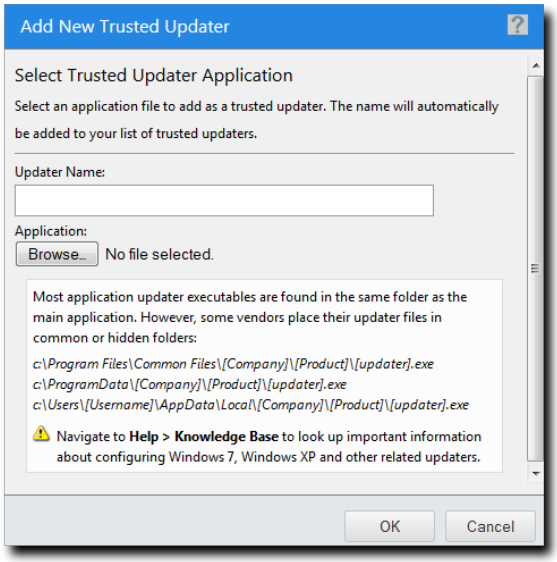


Figure 50: Add New Trusted Updater

2. Add a new updater by identifying the appropriate application file. Use one of the following methods:

Method	Steps
Enter the file path and name	Type the filename and path in the **Application** field.
Browse for the file	1. Click **Browse**. **Note:** Browsing occurs on the local file system, but you may also browse network devices if you have valid credentials. The text below the **Browse** button provides useful information for locating updater files. 2. In the file upload dialog that opens, select the desired file as a Trusted Updater. 3. Click **Open**. The filename and path appear in the **Application** field.

3. Type an appropriate name for the application in the **Updater Name** field.

4. Click **OK**.

   Step Result: The application file is added to the list of Trusted Updaters.

   Note: When you add a new Trusted Updater, the application file is *hashed*, which means that a unique value is created from it and stored on the server.

   Important: You can define very large files (up to 1 GB) as Trusted Updaters. When you add a very large file, however, it may take an appreciable time to upload the file and create its hash.

Result: The application file has been added to the list of Trusted Updaters. The next time you create or edit a Trusted Updater policy, this application will be available from the **Add Updaters** dialog.

Self-Updating Trusted Updaters

A trusted updater file that updates itself is automatically added to the endpoint's whitelist. The administrator can then manually update the Trusted Updater policy on the server by adding the updated file.

A trusted updater can add new files or update existing files on an endpoint. It also adds them to the endpoint's whitelist so that they can run when the endpoint is locked down. The trusted updater itself is on the whitelist.

Many trusted updaters can update themselves by downloading update information from their manufacturer. These are called *self-updating* trusted updaters. When a trusted updater updates itself, the file itself changes and its corresponding hash value changes too. But when this happens it no longer matches the value stored on the endpoint's whitelist.

Ivanti Application Control can handle this scenario, however. The updated file is added to the endpoint's whitelist. It is also added to the endpoint's version of the Trusted Updater policy that listed the original version of the file.

Note: Although the policy on the endpoint is updated automatically, the administrator must update the Trusted Updater policy on the server manually. For more information on how to do this, see Identifying Self-Updated Trusted Updaters on page 154 and Adding a Self-Updated Trusted Updater on page 156.

Identifying Self-Updated Trusted Updaters

You can identify the trusted updaters that updated themselves on the endpoint and use the information to update the Trusted Updater policy on the server.

You have run an application event log query to determine if any trusted updaters have updated themselves. For information on how to do this, see Creating an Application Control Log Query on page 277.

1. Select **Review** > **Application Control Log Queries**.

2. Click the **Completed** tab.

   Step Result: The **Application Control Log Queries** page displays a list of completed queries.

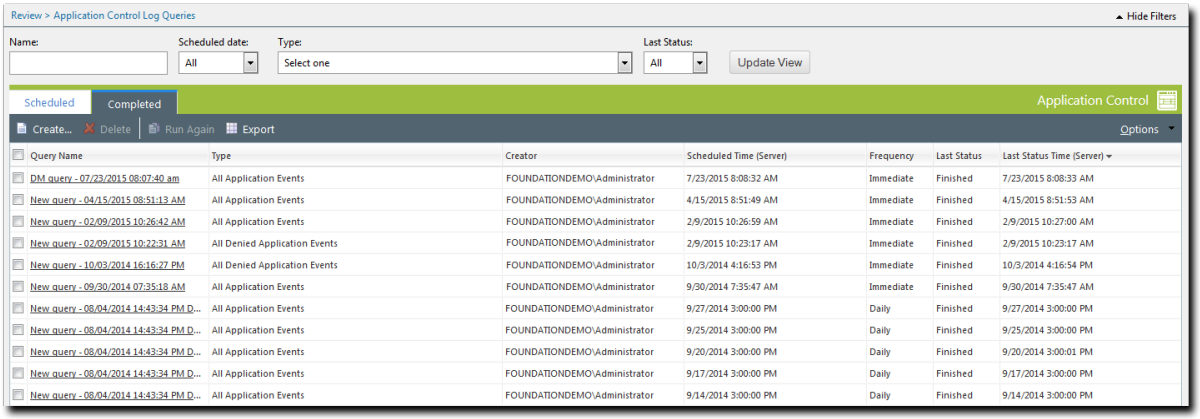


Figure 51: Application Control Log Queries

3. If necessary, sort the list to find the query you want to view (it will be of type **All Updaters Added by Trusted Updater**.
4. In the **Query Name** column, click the name of the query.

   Step Result: The ***Query Results*** page opens, displaying the detailed results.

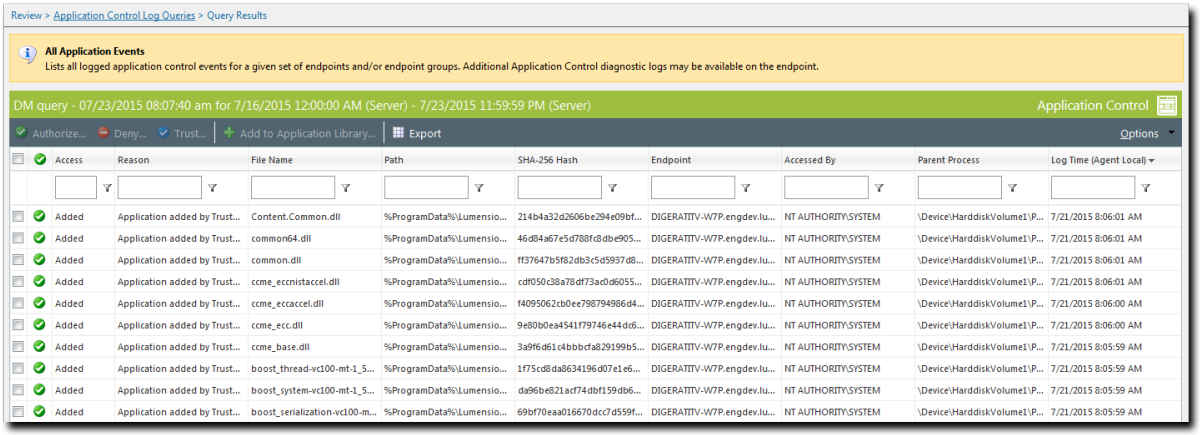


Figure 52: Application Event Logs - Query Results

5. Record the information on the updated trusted updaters (file name, path, endpoint and so on).

Result: You can use the trusted updater information to find the Trusted Updater policies on the server that apply to these updated files.

Adding a Self-Updated Trusted Updater

A self-updated trusted updater is added to server policy by identifying the correct executable file and adding it to the list of known updaters. This is done using the ***Add New Updater*** dialog.

You have identified one or more trusted updaters that have updated themselves on the endpoint.

1. Select **Manage** > **Application Control Policies**.
2. Click **Trusted Change**.

   Step Result: A list of Trusted Change policies is displayed.

3. Select the Trusted Updater policy to be edited (the policy that contains the original trusted updater that has updated itself).

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy. You can only edit one policy at a time.

   Step Result: The selected policy is highlighted.

4. Click **Edit**.

   Step Result: The ***Trusted Updater Wizard*** opens to the ***Add Application Updaters*** page.

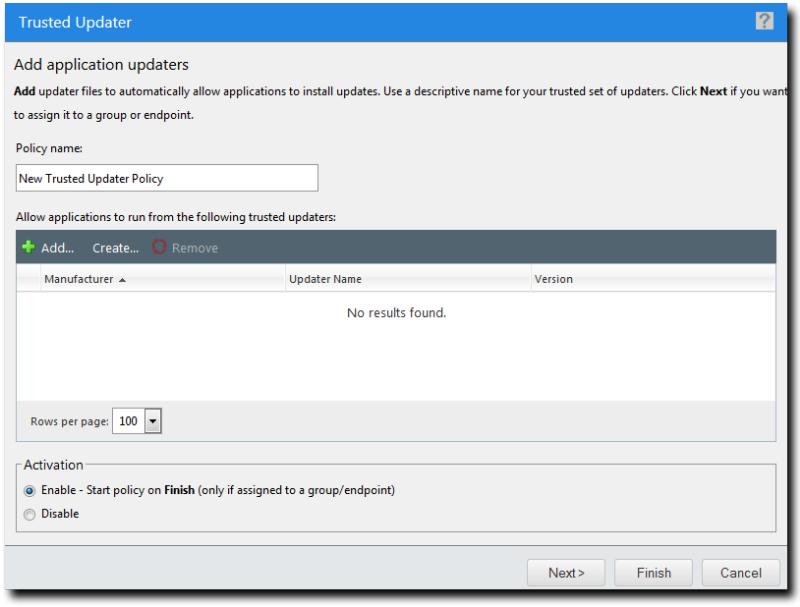


Figure 53: Trusted Updater Wizard - Add Application Updaters Page

5. Click **Create**.

   Step Result: The ***Add New Trusted Updater*** dialog opens.

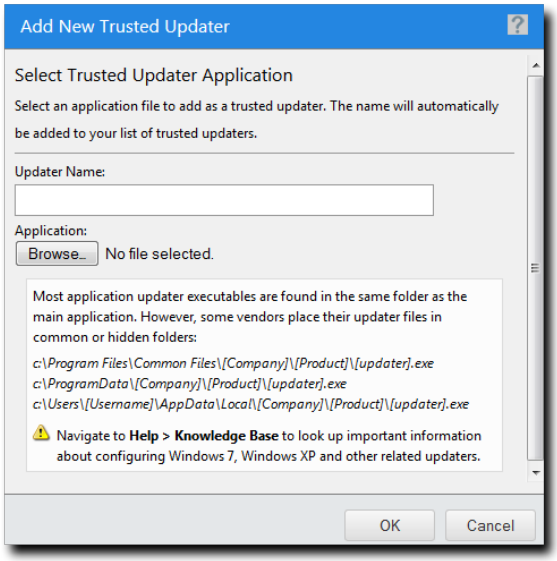


Figure 54: Add New Trusted Updater

6. Add the updated trusted updater by identifying the appropriate application file:
   a) Click **Browse**. Browsing occurs on the local file system, but you may also browse network devices if you have valid credentials. The text below the **Browse** button provides useful information for locating updater files.
   b) In the file upload dialog that opens, select the desired file as a Trusted Updater.
   c) Click **Open**. The filename and path appear in the **Application** field.
7. Type an appropriate name for the updated file in the **Updater Name** field.
8. Click **OK**.

   Step Result: The updated file is added to the list of trusted updaters.

   Note: If the file is very large, it may take an appreciable time to upload it and create its hash.

Result: The self-updated trusted updater file has been added to the list of Trusted Updaters.

Assigning a Trusted Updater Policy

You can select a Trusted Updater policy and assign it to endpoints and/or groups of endpoints.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.

3. Select a Trusted Updater policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

4. Click **Assign**.

   Step Result: The ***Trusted Updater*** dialog is displayed.

5. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

   Note: Use the double-arrows ( ) to switch between groups and endpoints.

   Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

6. Click **OK**.

Result: The Trusted Updater policy is assigned to endpoints and/or groups of endpoints.

Assigning a Trusted Updater Policy to a Group

You can assign a Trusted Updater policy to a selected group of endpoints using the ***Assign Policy*** dialog.

Note: The ***Assign Policy*** dialog is also used to assign a Trusted Updater policy to a selected endpoint. See Assigning a Trusted Updater Policy to an Endpoint on page 159 if you are assigning the policy to an endpoint.

1. Select **Manage** > **Groups**.

   Step Result: The ***Groups*** page is displayed.

2. Select a group from the **Browser** tree.

3. From the **View** list, select **Application Control Policies**.

   Step Result: The Application Control policies for the selected group are displayed.

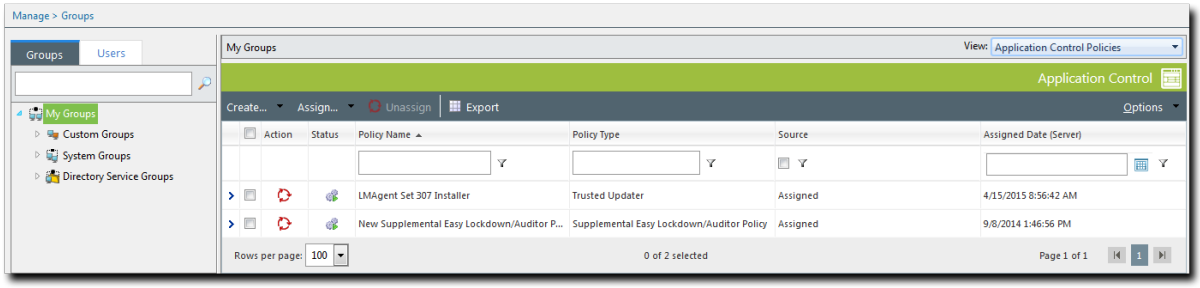


Figure 55: Groups - Application Control Policies View

> **Note:** Inherited policies can not be selected. In addition, the **Source** column reads *Inherited*.

4. From the toolbar, select **Assign** > **Trusted Updater**.

   Step Result: The ***Assign Policy*** dialog is displayed, listing existing Trusted Updater policies.

5. Select one or more Trusted Updater policies.
6. Click **OK**.

Result: The Trusted Updater policy is assigned to the group.

Assigning a Trusted Updater Policy to an Endpoint

You can assign a Trusted Updater policy to a selected endpoint.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.

2. In the **Endpoint Name** column, click an endpoint link.

   Step Result: Detailed information for the selected endpoint is displayed.

3. Select the ***Application Control Policies*** tab.

   Step Result: A list of Application Control policies assigned to the endpoint is displayed.

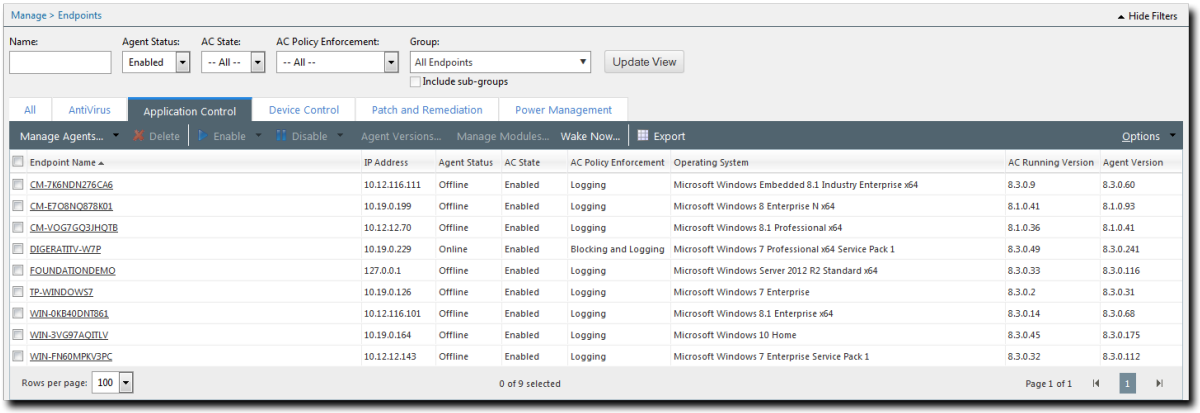


Figure 56: Application Control Policies Tab

4. From the toolbar, select **Assign** > **Trusted Updater**.

   Step Result: The ***Assign Policy*** dialog is displayed, listing existing Trusted Updater policies.

5. Select one or more Trusted Updater policies.
6. Click **OK**.

Result: The Trusted Updater policy is assigned to the endpoint.

Unassigning a Trusted Updater Policy

You can unassign a Trusted Updater policy, removing the association between it and any endpoints. Policies that are no longer assigned to an endpoint remain in the system as unassigned policies, which you can re-assign to endpoints at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select one or more Trusted Updater policies.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

4. Click **Unassign**.

   Step Result: One of two confirmation dialogs is displayed, depending on whether you selected a single policy or multiple policies.

Figure 57: Unassign Application Control Policy

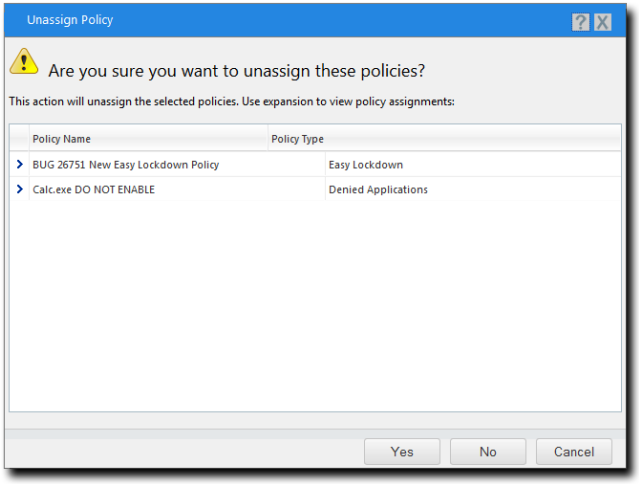


Figure 58: Unassign Multiple Application Control Policies

5. Click **Yes**.

Result: One or more Trusted Updater policies are unassigned.

> **Note:** When a Trusted Updater policy is unassigned, the application can no longer run as a trusted updater. However, it may still be able to run as an application, depending on when the Trusted Updater policy was created:
>
> - If the policy was created *before* an Easy Lockdown, the application will still be able to run as an application (though not as a trusted updater). In this case, if you want to block the application from running, you must apply a Denied Applications policy to it.
> - If the policy was created *after* an Easy Lockdown, the application will no longer be able to run in any capacity.

Editing a Trusted Updater Policy

You can edit a Trusted Updater policy and, for example, add or remove trusted updaters or change the endpoints to which the policy is assigned.

Note: If both Patch and Remediation and Application Control modules are installed, an PR Trusted Updater System Policy is automatically created. Although you can select this policy and click **Edit**, you cannot change any of the policy's options or settings. See Working with Trusted Updater on page 144 for more information.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the Trusted Updater policy to be edited.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy. You can only edit one policy at a time.

   Step Result: The selected policy is highlighted.
4. Click **Edit**.

   Step Result: The ***Trusted Updater Wizard*** opens to the ***Add Application Updaters*** page.
5. [Optional] Edit the **Policy Name**.
6. [Optional] Add a Trusted Updater to the policy using one of the following options:

Option	Steps
Add an existing Trusted Updater	1. Click **Add** to open the ***Add Trusted Updater*** dialog. 2. Select a Trusted Updater from the **Trusted Updaters** drop-down list. 3. Click **OK**.

Option	Steps
Add a new Trusted Updater	1. Click **Add** to open the ***Add Trusted Updater*** dialog. 2. Click **Add New Trusted Updater** to open the **Add New Trusted Updater** dialog. 3. In the **Add New Trusted Updater** dialog, type a name in the **Updater Name** field. 4. Click **Browse**. 5. Locate the updater `.exe` and click **Open**. 6. Click **OK**. 7. Click **OK**.

Note: When you add a new Trusted Updater, the application file is *hashed*, which means that a unique value is created from it and stored on the server.

Important: You can define very large files (up to 1 GB) as Trusted Updaters. When you add a very large file, however, it may take an appreciable time to upload the file and create its hash.

Step Result: One or more Trusted Updaters appears in the results list.

Note: If the list is empty, or you cannot see the updater you want, you will have to add the updater yourself. See Adding a New Trusted Updater on page 152 for more information.

7. [Optional] Remove a Trusted Updater from the policy:
   a) Select a Trusted Updater.
   b) Click **Remove**.

      Step Result: The ***Remove Trusted Updater*** dialog is displayed.

   c) Click **Yes**.

      Note: When a Trusted Updater is removed from the policy, any running processes associated with that updater lose their trusted status when the policy is applied.

      Step Result: The ***Remove Trusted Updater*** dialog is closed.

8. [Optional] Edit the **Activation** options.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

9. Click **Next**.

   Step Result: The ***Trusted Updater Wizard*** opens to the ***Assign Groups and Endpoints*** page.

10. [Optional] Edit the list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

11. Click **Finish**.

Result: The Trusted Updater policy is edited.

Disabling a Trusted Updater Policy

You can disable policies without deleting them. The details of the policies are retained and you can enable the policies at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the enabled Trusted Updater policies that you want to disable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy/policies.

   Step Result: The selected policies are highlighted.

4. Click **Disable**.

Result: The selected Trusted Updater policies are disabled.

Enabling a Trusted Updater Policy

You can enable policies that are currently disabled.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the disabled Trusted Updater policy or policies that you want to enable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.
4. Click **Enable**.

Result: The selected Trusted Updater policies are enabled.

Deleting a Trusted Updater Policy

You can delete a Trusted Updater policy, as long as it is not assigned to an endpoint.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the Trusted Updater policy you want to delete, ensuring it is not assigned to an endpoint (**Assigned** column value of *Not Assigned*).

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.
4. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned.
5. Click **Yes**.

Result: The Trusted Updater policy is deleted.

Exporting Trusted Updater Policies

You can export a list of policies to a `csv` (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a `csv` file with the following columns:

Name	Description
Status	Enabled or Disabled

Name	Description
Policy Name	The name of the policy
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)
Policy Type	The type of policy (Easy Lockdown, Trusted Updater, and so on)
Last Updated Date (Server)	The date and time (on the server) that the policy was last changed

Working with Trusted Publisher

A Trusted Publisher policy allows an application that has been signed with a digital certificate from a trusted source to run on an endpoint.

When administrators create a Trusted Publisher policy, they have the option to search for executables that contain a signature that is marked as having originated from a specific manufacturer or other trusted source.

Note: MSIs that are not Trusted Updaters are blocked automatically.

Later, when applications signed with that same certificate are executed, Ivanti Application Control compares the digital signature of the certificate being executed to the list of Trusted Publishers. If the signatures match then the executable is allowed to run.

Note: Some applications require more than one certificate to execute and have all application features work correctly. Each Trusted Publisher policy may have multiple certificates associated with it.

Trusted Publishers are displayed on the ***Trusted Change*** tab of the ***Application Control Policies*** page. You can filter the **Policy Type** column to display only Trusted Publisher policies.

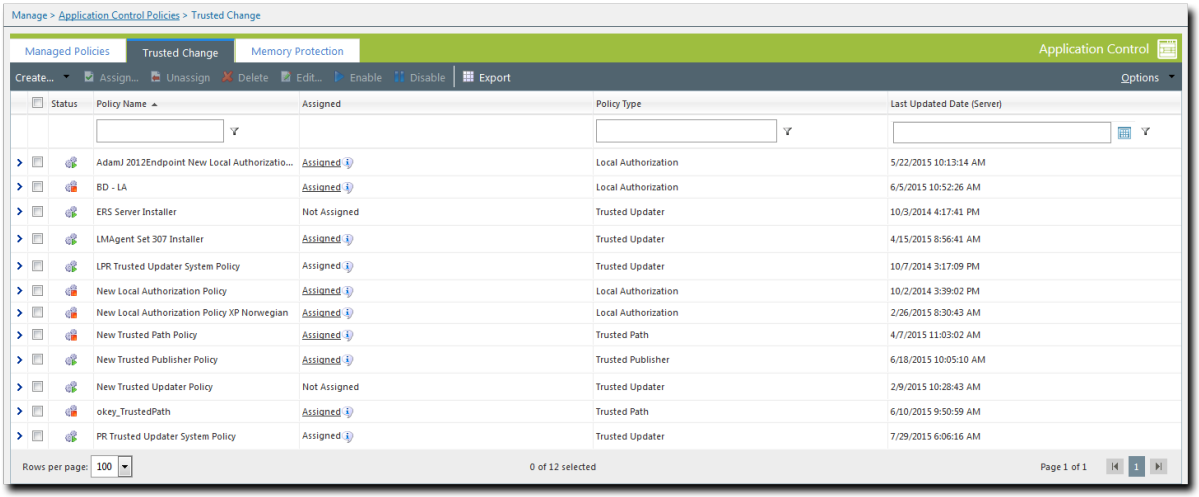


Figure 59: Application Control Policies - Trusted Change Tab

Trusted Publisher in Practice

A Trusted Publisher policy permits the running of executable files that have a signed certificate from a trusted source.

Trusted Publishers may be software manufacturers such as Microsoft, Adobe, WebEx, McAfee, and so on. But proprietary software may also be authorized with a Trusted Publisher policy if it has an internal corporate certificate.

Note:

- Some Windows Store (formerly Metro) apps do not have signed executables. It is not possible to apply a Trusted Publisher policy to these applications.
- >MSIs that are not Trusted Updaters are blocked automatically.

An important role for Trusted Publisher is to allow applications that depend on signed ActiveX controls being downloaded into a browser. The online collaboration program WebEx is an example of such a program, which cannot be installed with Trusted Updater.

Another role for Trusted Publisher is allowing signed lightweight applications that do not require an installation process. (These are the type of applications that you typically drop on the desktop and click to run.)

Caution: In theory you can apply Trusted Publisher to a signed installer program but this is NOT recommended. Even if it installs, there is no guarantee the application will run. Also, Trusted Publisher could overwrite shared files (.exes or .dlls) on the whitelist and this could stop other programs from running, or even cause the endpoint to fail.

Important: Because Trusted Publisher is certificate based, all applications signed by a specific certificate are allowed to run once one of the applications has been added to a Trusted Publisher policy. If there is a need to block applications that have been authorized in this way, they can be added to a Denied Applications policy.

Creating a Trusted Publisher Policy

A Trusted Publisher policy specifies one or more publishers that are allowed to run executable files on an endpoint/endpoint group.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Click **Create** > **Trusted Publisher**.

   Step Result: The ***Trusted Publisher Wizard*** opens to the ***Name Policy and Add Trusted Publishers*** page.

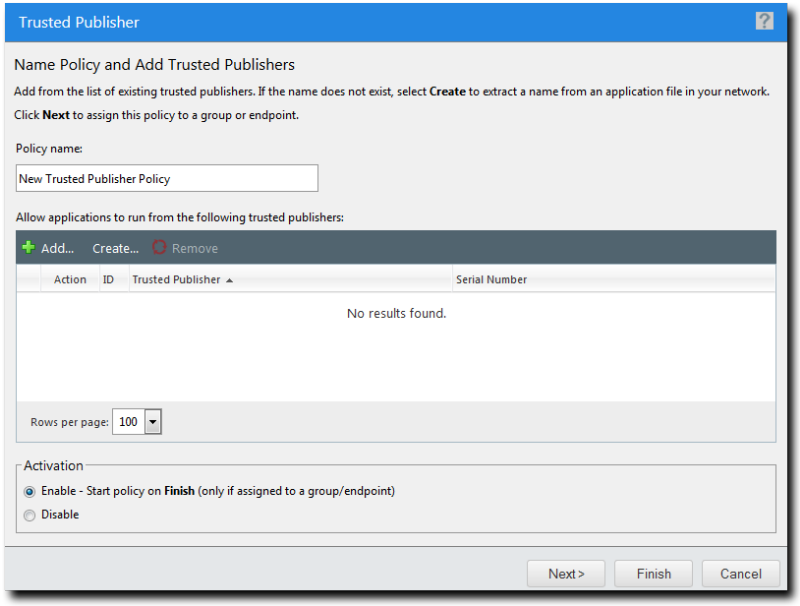


Figure 60: Trusted Publisher Wizard

4. Type a **Policy Name** for the new Trusted Publisher policy.

Note: Give the policy a descriptive name. For example, if this Trusted Publisher policy relates to particular applications published by Adobe you could name it `Adobe Applications`.

5. Click **Add**.

Step Result: The ***Add Publishers*** dialog is displayed. Initially, it does not display any publishers.

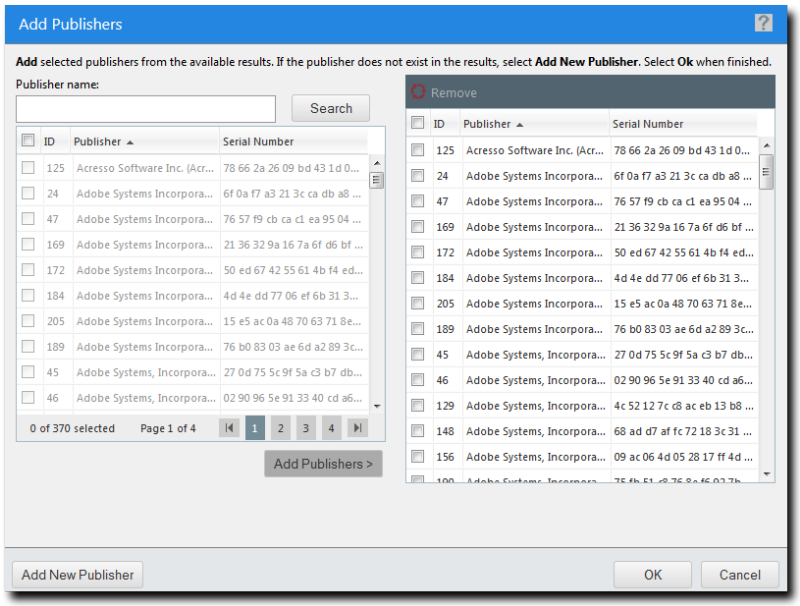


Figure 61: Add Publishers

6. Search for existing publishers using either of the following methods:

Method	Steps
Search for all publishers	Leave the **Publisher name** field blank and click **Search**. This returns all existing publishers.

Method	Steps
Search for selected publishers	1. Type a publisher name in the **Publisher name** field. **Note:** Sub-string matching is supported, so you do not have to type the full name. A partial name may return multiple results. 2. Click **Search**.

Step Result: One or more publishers appears in the results list.

Note: If the list is empty, or you cannot see the publisher you want, you will have to add the publisher yourself. See Adding a New Publisher on page 173 for more information.

7. Select one or more publishers.

Note: Several publishers may share the same name, but the serial number is unique and is associated with the digital signature of the file from which the metadata was taken.

8. Click **Add Publishers**.

   Step Result: The publishers are added to the policy.

9. Click **OK**.

   Step Result: The ***Add Publishers*** dialog closes.

10. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

11. Click **Next** to assign the policy to endpoints.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time.

Step Result: The ***Trusted Publisher Wizard*** opens to the ***Assign Groups and Endpoints*** page.

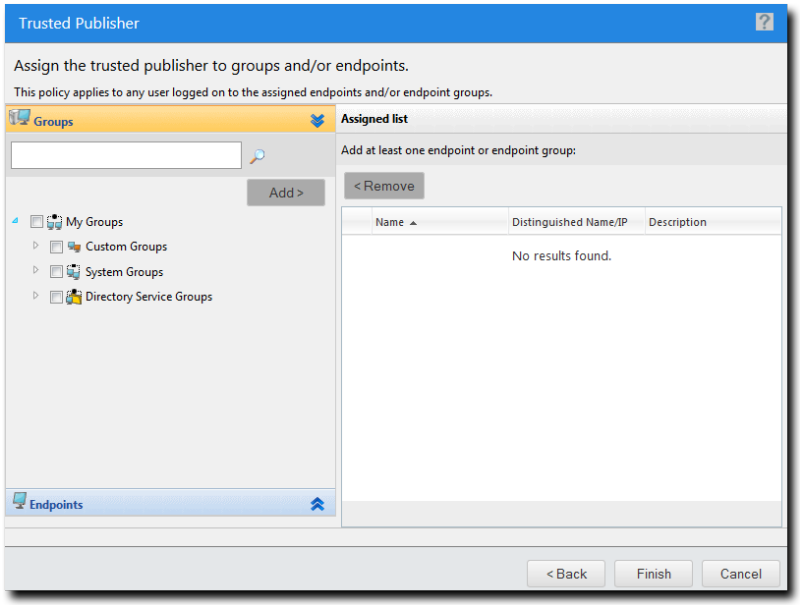


Figure 62: Trusted Publisher Wizard - Assign Groups and Endpoints Page

12. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

13. Click **Finish**.

Result: The Trusted Publisher policy is created and assigned to groups or endpoints.

Important: When a Trusted Publisher policy is assigned to an endpoint, it allows signed applications resident on that endpoint's drive(s) to execute. However, it does not allow the execution (on that endpoint) of signed applications that are resident on a network share that the endpoint can access.

Adding an Existing Publisher

An existing publisher is added to a Trusted Publisher policy using the ***Add Publishers*** dialog.

This dialog is accessed by clicking the **Add** button on the ***Trusted Publisher Wizard***.

1. Search for existing publishers using either of the following methods:

Method	Steps
Search for all publishers	Leave the **Publisher name** field blank and click **Search**. This returns all existing publishers.
Search for selected publishers	1. Type a publisher name in the **Publisher name** field. **Note:** Sub-string matching is supported, so you do not have to type the full name. A partial name may return multiple results. 2. Click **Search**.

Step Result: One or more publishers appears in the results list.

Note: If the list is empty, or you cannot see the publisher you want, you will have to add the publisher yourself. See Adding a New Publisher on page 173 for more information.

2. Select one or more publishers.

Note: Several publishers may share the same name, but the serial number is unique and is associated with the digital signature of the file from which the metadata was taken.

3. Click **Add Publishers**.

Step Result: The publisher is added to the Trusted Publisher policy.

4. Click **OK**.

Step Result: The ***Add Publishers*** dialog closes and you are returned to the ***Trusted Publisher Wizard***.

Adding a New Publisher

A publisher is added by identifying an executable or certificate file, extracting the vendor information, and adding it to the list of known publishers. This is done using the ***Add New Publisher*** dialog.

This dialog can be accessed from different locations.

- If you know that the application file has not yet been defined as trusted, you can access it directly from the ***Trusted Publisher Wizard***.
- If you are on the **Add Publishers** dialog and you find that the application file has not yet been defined as trusted, you can access it from there as well.

1. Open the ***Add New Publisher*** dialog.

Context	Steps
From the *Trusted Publisher Wizard*:	Click **Create**.

Context	Steps
From the *Add Publishers* dialog:	Click **Add New Publisher**.

Step Result: The ***Add New Publisher*** dialog opens.

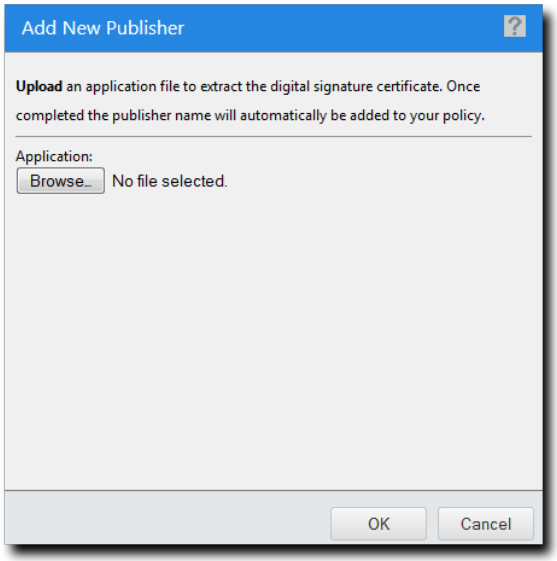


Figure 63: Add New Publisher

2. Add a new publisher by identifying the appropriate file, which can be an `.exe`, a `.dll`, or a `.cer` (certificate) file. Use one of the following methods:

Method	Steps
Name the file explicitly	Type the filename and path in the **Application** field.
Browse for the file	1. Click **Browse**. 2. In the file upload dialog that opens, select an appropriate file to identify its vendor as a publisher you wish to use for Trusted Publisher policies. The filename and path appear in the **Application** field. **Note:** Browsing occurs on the local file system. Network devices may also be browsed to if the logged-on user has valid credentials.

3. Click **OK**.

   Step Result: The certificate metadata is extracted from the file and uploaded. While this is happening, a progress indicator is displayed.

Assigning a Trusted Publisher Policy

You can select a Trusted Publisher policy and assign it to endpoints and/or groups of endpoints.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Trusted Publisher policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

4. Click **Assign**.

   Step Result: The ***Trusted Publisher*** dialog is displayed.

5. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

6. Click **OK**.

Result: The Trusted Publisher policy is assigned to endpoints and/or groups of endpoints.

> **Important:** When a Trusted Publisher policy is assigned to an endpoint, it allows signed applications resident on that endpoint's drive(s) to execute. However, it does not allow the execution (on that endpoint) of signed applications that are resident on a network share that the endpoint can access.

Assigning a Trusted Publisher Policy to a Group

You can assign a Trusted Publisher policy to a group of endpoints using the ***Assign Policy*** dialog.

> **Note:** The ***Assign Policy*** dialog is also used to assign a Trusted Publisher policy to a selected endpoint. See Assigning a Trusted Publisher Policy to an Endpoint on page 177 if you are assigning the policy to an endpoint.

1. Select **Manage** > **Groups**.

   Step Result: The ***Groups*** page is displayed.

2. Select a group from the **Browser** tree.
3. From the **View** list, select **Application Control Policies**.

   Step Result: The Application Control policies for the selected group are displayed.

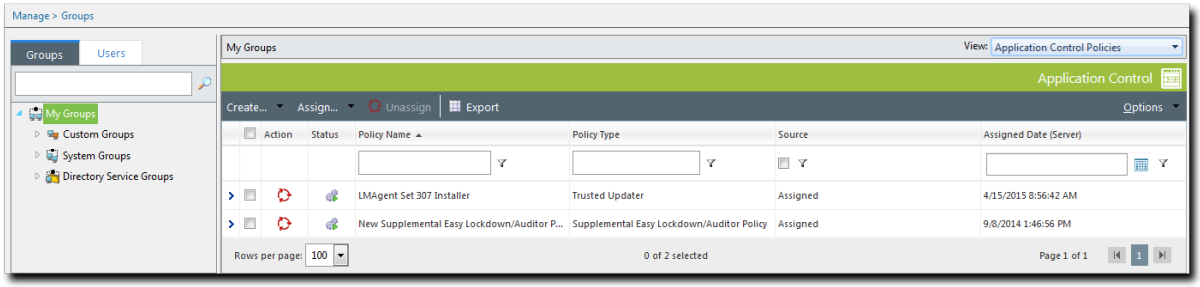


Figure 64: Groups - Application Control Policies View

> **Note:** Inherited policies can not be selected. In addition, the **Source** column reads *Inherited*.

4. From the toolbar, select **Assign** > **Trusted Publisher**.

   Step Result: The ***Assign Policy*** dialog is displayed.

5. Select one or more Trusted Publisher policies.

6. Click **OK**.

Result: The Trusted Publisher policy is assigned to the group of endpoints.

> **Important:** When a Trusted Publisher policy is assigned to an endpoint, it allows signed applications resident on that endpoint's drive(s) to execute. However, it does not allow the execution (on that endpoint) of signed applications that are resident on a network share that the endpoint can access.

Assigning a Trusted Publisher Policy to an Endpoint

You can assign a Trusted Publisher policy to an endpoint.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.

2. In the **Endpoint Name** column, click an endpoint link.

   Step Result: Detailed information for the selected endpoint is displayed.

3. Select the ***Application Control Policies*** tab.

   Step Result: A list of Application Control policies assigned to the endpoint is displayed.

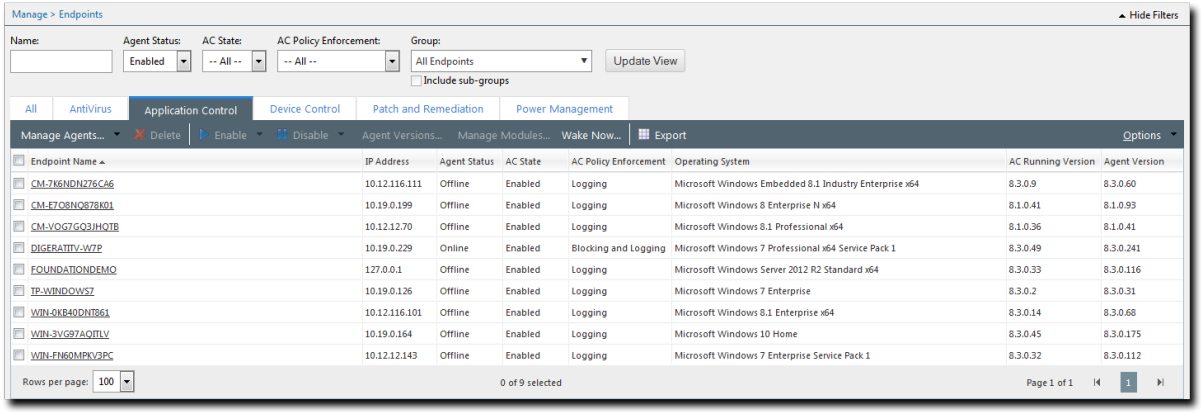


Figure 65: Application Control Policies Tab

4. From the toolbar, select **Assign** > **Trusted Publisher**.

   Step Result: The ***Assign Policy*** dialog is displayed.

5. Select one or more Trusted Publisher policies.

6. Click **OK**.

Result: One or more Trusted Publisher policies are assigned to the endpoint.

> **Important:** When a Trusted Publisher policy is assigned to an endpoint, it allows signed applications resident on that endpoint's drive(s) to execute. However, it does not allow the execution (on that endpoint) of signed applications that are resident on a network share that the endpoint can access.

Unassigning a Trusted Publisher Policy

You can unassign a Trusted Publisher policy, removing the association between it and any endpoints. Policies that are no longer assigned remain in the system as unassigned policies, which you can re-assign to endpoints at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select one or more Trusted Publisher policies.

> **Tip:** Filter the **Policy Name** and **Policy Type** columns to locate the policy.

4. Click **Unassign**.

   Step Result: One of two confirmation dialogs is displayed, depending on whether you selected a single policy or multiple policies.

Figure 66: Unassign Application Control Policy

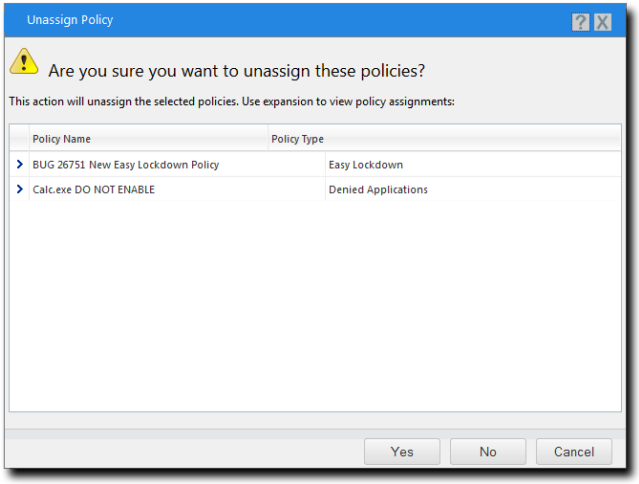


Figure 67: Unassign Multiple Application Control Policies

5. Click **Yes**.

Result: One or more Trusted Publisher policies are unassigned.

Editing a Trusted Publisher Policy

You can edit a Trusted Publisher policy with the ***Trusted Publisher Wizard***. For example, you might want to add a new Trusted Publisher to the policy, or assign it to different endpoints or groups.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Trusted Publisher policy.

Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

Step Result: The selected policy is highlighted.

4. Click **Edit**.

   Step Result: The ***Trusted Publisher Wizard*** opens to the ***Name Policy and Add Trusted Publishers*** page.

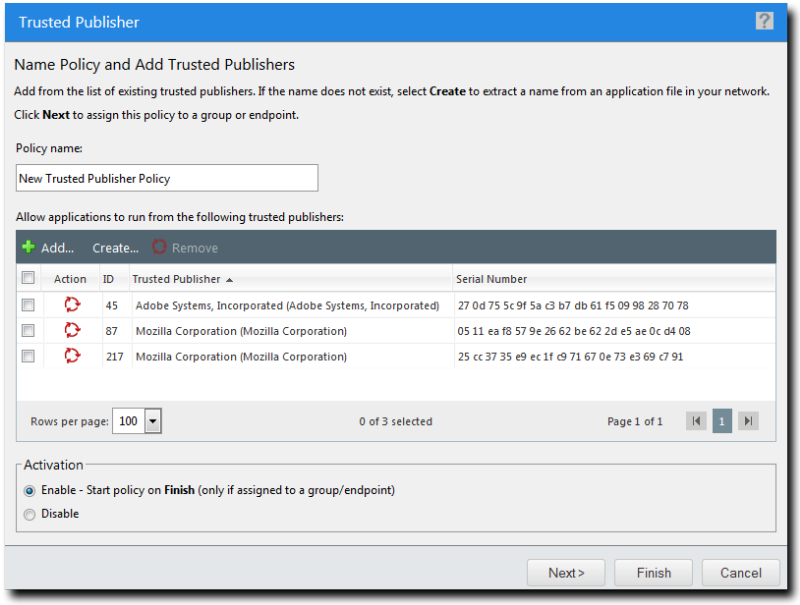


Figure 68: Trusted Publisher Wizard - Name Policy and Add Trusted Publishers Page

5. [Optional] Edit the **Policy Name**.

Note: Give the policy a descriptive name. For example, if this Trusted Publisher policy relates to applications published by Microsoft you could name it `Microsoft Applications`.

6. [Optional] Add a Publisher to the policy using one of the following options:

Option	Steps
Add an existing Publisher	1. Click **Add** to open the ***Add Trusted Publisher*** dialog. 2. Select a Trusted Updater from the **Trusted Publishers** drop-down list. 3. Click **OK**.

Option	Steps
Add a new Publisher	1. Click **Add** to open the ***Add Trusted Publisher*** dialog. 2. Click **Add New Trusted Publisher** to open the **Add New Trusted Publisher** dialog. 3. In the **Add New Trusted Publisher** dialog, click **Browse**. 4. Locate the application file and click **Open**. 5. Click **OK**. 6. Click **OK**.

Step Result: One or more publishers appears in the results list.

> **Note:** If the list is empty, or you cannot see the publisher you want, you will have to add the publisher yourself. See Adding a New Publisher on page 173 for more information.

7. [Optional] Remove a Trusted Publisher from the policy:
   a) Select a Trusted Publisher.
   b) Click **Remove**.

      Step Result: The ***Remove Trusted Publisher*** dialog is displayed.

   c) Click **Yes**.

      Step Result: The ***Remove Trusted Publisher*** dialog is closed.

8. [Optional] Edit the **Activation** options.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

9. Click **Next**.

   Step Result: The ***Trusted Publisher Wizard*** opens to the ***Assign Groups and Endpoints*** page.

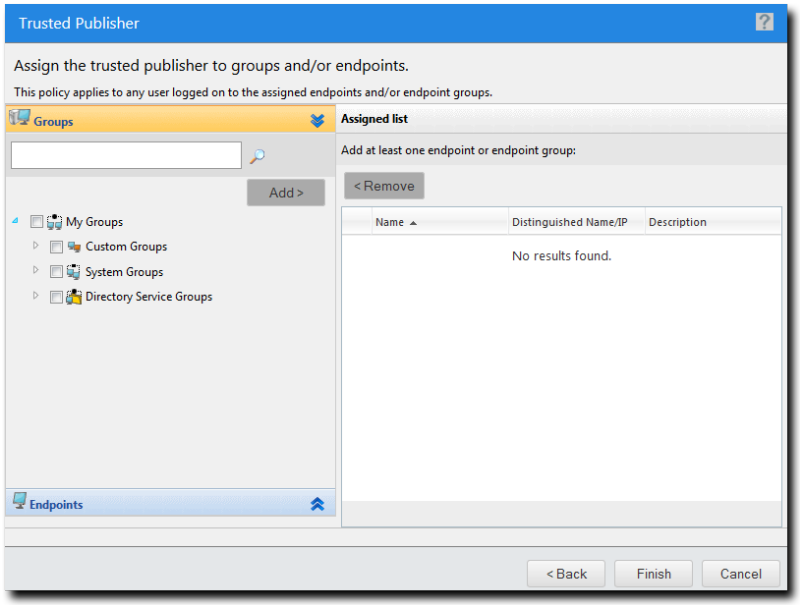


Figure 69: Trusted Publisher Wizard - Assign Groups and Endpoints Page

10. [Optional] Edit the list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

11. Click **Finish**.

Result: The Trusted Publisher policy has been edited.

Disabling a Trusted Publisher Policy

You can disable Trusted Publisher policies without deleting them. The details of the policies are retained and you can enable the policies at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the enabled Trusted Publisher policies that you want to disable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

4. Click **Disable**.

Result: One or more Trusted Publisher policies are disabled.

Enabling a Trusted Publisher Policy

You can enable a Trusted Publisher policy that is currently disabled.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the disabled Trusted Publisher policy or policies that you want to enable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

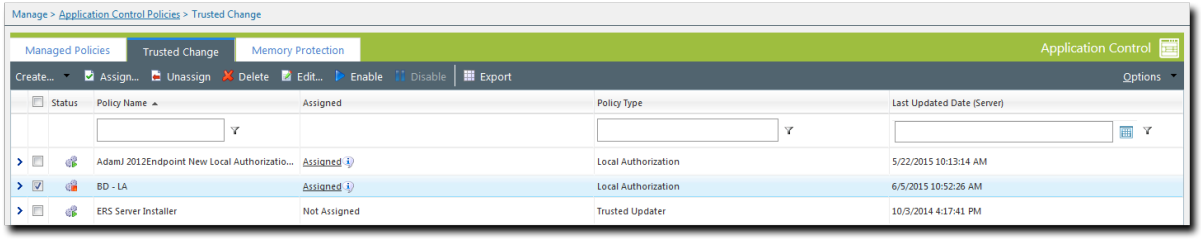


Figure 70: Select Disabled Policy

4. Click **Enable**.

Result: One or more Trusted Publisher policies are enabled.

Deleting a Trusted Publisher Policy

You can delete a Trusted Publisher policy, as long as it is not assigned to an endpoint.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Trusted Publisher policy that is not assigned to an endpoint (**Assigned** column value of *Not Assigned*).

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.
4. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned.
5. Click **Yes**.

Result: The Trusted Publisher policy is deleted.

Exporting Trusted Publisher Policies

You can export a list of policies to a `csv` (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a `csv` file with the following columns:

Name	Description
Status	Enabled or Disabled
Policy Name	The name of the policy
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)
Policy Type	The type of policy (Easy Lockdown, Trusted Updater, and so on)
Last Updated Date (Server)	The date and time (on the server) that the policy was last changed

Working with Trusted Path

A Trusted Path policy allows an administrator to designate a file system path so that any executable files residing at this path are allowed to run on all endpoints that are assigned the Trusted Path policy.

The Trusted Path may be a shared resource such as a network drive/share that is protected by file system security. Optionally, trusted paths may be created such that all executables in a parent folder and all child folders are allowed to run. Trusted Paths may be helpful to users as a temporary trusted change activity involving frequently-changing executables (for example, development or testing of new applications or IT services).

Adding Trusted Paths allows executable files that are found within specified folders to run. You may optionally limit execution to files containing a specific owner attribute.

Trusted Path policies are displayed on the ***Trusted Change*** tab of the ***Application Control Policies*** page. You can filter the **Policy Type** column to display only Trusted Path policies.

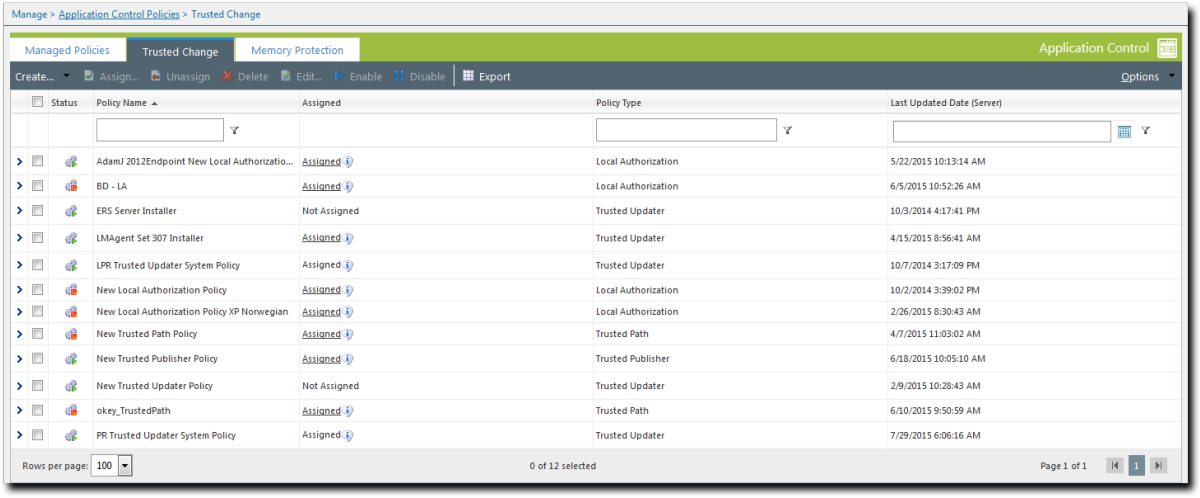


Figure 71: Application Control Policies - Trusted Change Tab

Trusted Path in Practice

A Trusted Path policy allows executable files resident in a specified file system path to run.

Trusted Path is the preferred trust mechanism for the following scenarios:

- Build output locations for in-house software development
- Unsigned executables which change frequently
- Applications that cannot be authorized through other trust policies

This trust mechanism is ideal for handling large numbers of executable files that don't have certificates and that are likely to change.

Caution: In theory you can run an installer program in a Trusted Path but this is NOT recommended. It could overwrite shared files (.exes or .dlls) on the whitelist and this could stop other programs from running, or even cause the endpoint to fail.

Trusted Path can also be used when the other trust mechanisms are not suitable. For example, some applications dynamically create temporary executable files, and these files will be blocked on a locked-down endpoint. In this scenario, Trusted Publisher will not enable the application to run (as the temporary executable will still be blocked), and Trusted Updater is not recommended (as the original file is not an installer or an updater). Trusted Path is the best trust mechanism to use in this situation.

Trusted Path has an Authorized Owner feature which allows administrators to limit execution of the files in the path to specific users (the file's owner). This can be used as a security feature to restrict use of Trusted Path.

Trusted Path and ASP.NET Applications

An IIS web server on a locked-down endpoint can run ASP.NET applications only if an appropriate Trusted Path policy is applied.

Internet Information Services (IIS) is a web server that can use various technologies to produce dynamic web pages and applications. ASP.NET is one such technology, but if you try to run an ASP.NET application on a locked-down endpoint, the website throws errors.

This happens because the ASP.NET process creates and tries to run temporary executable files. Because these files are not on the endpoint's whitelist, Ivanti Application Control prevents them from executing and generates a Denied Application Event log.

You can enable ASP.NET applications to run on a locked-down endpoint by creating trusted paths where the temporary ASP.NET executables can run. To do this, create a Trusted Path policy with the following characteristics:

Trusted Paths	• `%SystemRoot%\WINDOWS\Microsoft.Net\Framework\v4.0.30319\Temporary ASP.NET Files\root` • `%SystemRoot%\WINDOWS\Microsoft.Net\Framework64\v4.0.30319\Temporary ASP.NET Files\root` • `%SystemRoot%\WINDOWS\Microsoft.Net\Framework\v2.0.50727\Temporary ASP.NET Files\root` • `%SystemRoot%\WINDOWS\Microsoft.Net\Framework64\v2.0.50727\Temporary ASP.NET Files\root` **Important:** Be sure to create all four paths and select the **Include sub-folders** checkbox in each case.
Authorized Owner	Set the Authorized Owner for each path to **Network Service** (this can be found in the **Built-in Users and Groups** list).
User	Set the User to **Network Service**.

See Creating a Trusted Path Policy on page 187 for details of creating a Trusted Path policy.

Creating a Trusted Path Policy

A Trusted Path policy specifies one or more paths that are allowed to run executable files on an endpoint.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Click **Create** > **Trusted Path**.

   Step Result: The ***Trusted Path Wizard*** opens to the ***Name your policy and add one or more paths*** page.

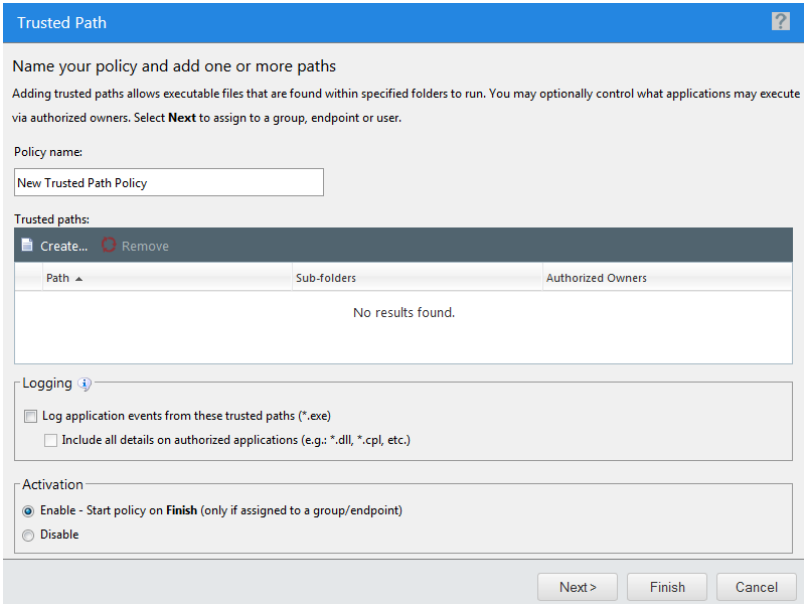


Figure 72: Trusted Path Wizard

4. Type a name for the new policy in the **Policy name** field.

Note: Give the policy a descriptive name. For example, if this Trusted Path policy relates to a path that contains applications used by the accounting department you could name it `Accounting Applications`.

5. Click **Create**.

   Step Result: The ***New Trusted Path*** dialog is displayed.

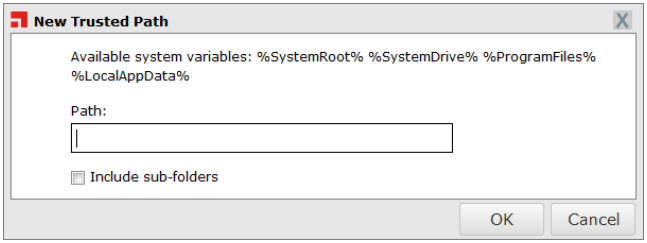


Figure 73: New Trusted Path

6. Type the name of the trusted path.

Note:

- You must enter a valid *path* (a unique directory in the file system).

  Important: Do not enter a *file path* (that is, a path ending in a file name). If you do, the complete string entered will be treated as a path name, with unpredictable results.

- Alternatively, you can use the system variables `%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%`, or `%LocalAppData%`.

7. [Optional] Select the **Include sub-folders** check box to include any sub-folders in the trusted path.
8. Click **OK**.

   Step Result: The ***New Trusted Path*** dialog is closed, and the new trusted path appears in the **Trusted paths** list.

9. [Optional] Add one or more *Authorized Owners* to this trusted path.

   If an Authorized Owner is specified, an executable file in the trusted path can only run if the file's owner matches an Authorized Owner on the list. The user running the file must also be assigned the Trusted Path policy.

   If no Authorized Owner is specified, any user that the policy is assigned to can run the executable files in the path.

Note: Specifying an Authorized Owner is optional, but the policy must be assigned to at least one user, which is done on the next page of the Trusted Path Wizard.

a) Click the **Authorized Owners** ellipses [...] button for the path.

   Step Result: The ***Add Users*** dialog opens.

b) Type a full or partial user name in the **User name** field.

Note: You can optionally define in which domain to search for users by clicking the ellipses [...] button beside the **Domain** field.

c) Click **Search**.
d) Select the required user(s) from the results list.
e) Click **Add Users**.
f) Click **OK**.

Step Result: The ***Add Users*** dialog closes and the specified users are displayed in the **Authorized Owners** column for that trusted path.

10. [Optional] Repeat the previous steps to add more trusted paths to the list. A Trusted Path policy can have multiple trusted paths.

11. If you want to log the activity of applications that reside in the policy's trusted path(s), select the **Logging** options:

Option	Description
Log application events from these trusted paths (*.exe).	Log the activity of applications that reside in the trusted path.
Include all details on authorized applications (e.g. *.dll, *.cpl, etc.)	Log the activity of applications that reside in the trusted path. In addition, log the activity of all the executable files (such as DLLs) associated with those applications.

Note: Even if not selected here, logging may occur when other policy types (such as Easy Auditor) have logging enabled.

12. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

13. Click **Next** to assign the policy to endpoints.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time.

Step Result: The ***Trusted Path Wizard*** opens to the ***Assign the trusted path to groups, endpoints and/or users*** page.

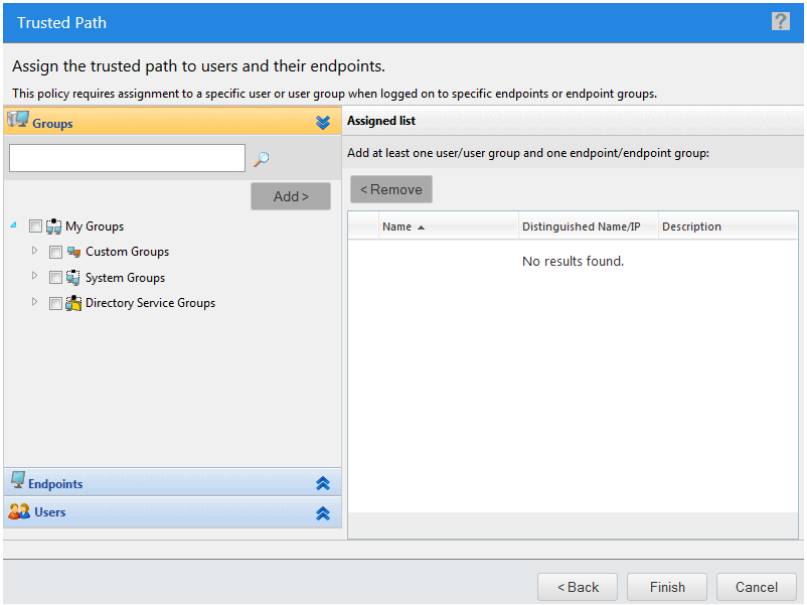


Figure 74: Trusted Path Wizard - Assign Groups and Endpoints Page

14. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

15. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

16. Click **Finish**.

Result: The Trusted Path policy is created and assigned to groups, endpoints, or users.

Trusted Path Precedence

When multiple Trusted Path policies and paths are assigned you can determine which one allowed application execution by examining their *precedence*.

If there are multiple Trusted Path policies, the first policy whose path\pattern matches that of the file execution request is the one that allows that request to succeed. If logging is enabled, the event is logged and reported when a relevant query is run. However, the query result does not show which policy permitted the application to run.

You can determine the policy that allowed the application to run by examining the Trusted Path policy precedence:

- The Trusted Path policy that was created first is evaluated first.
  - Other policies are evaluated in the order in which they were created.
- If a Trusted Path policy has more than one trusted path, the path that was created first is evaluated first.
  - Other paths are evaluated in the order in which they were created.
- If a Trusted Path policy is assigned to multiple users and groups (such as Administrators or Power Users) these assignments are *not* necessarily evaluated in the order in which they were created.

Adding an Authorized Owner to a Trusted Path

You can add one or more *Authorized Owners* to a trusted path using the ***Add Users*** dialog.

If an Authorized Owner is specified, an executable file in the trusted path can only run if the file's owner matches an Authorized Owner on the list. The user running the file must also be assigned the Trusted Path policy.

The ***Add Users*** dialog is accessed by clicking an **Authorized Owners** ellipses (...) button on the **Trusted paths** list.

1. Search for users using either of the following methods:

Option	Steps
Search for all users	Leave the **Username** field blank and click **Search**. This returns all existing users in the current domain.
Search for one or more selected users	1. Type a user name in the **Username** field. **Note:** Sub-string matching is supported, so you do not have to type the full name. Typing a partial name may result in multiple matches 2. Click **Search**.

Step Result: One or more users appear in the results list.

Note: If you cannot find the user(s) you want, try searching other available domains. Select a searchable domain controller from the **Domain** drop-down list.

2. Select one or more users.
3. Click **Add Users**.

Step Result: The users are added to the selection list.

4. Click **OK**.

   Step Result: The ***Add Users*** dialog closes and you return to the ***Trusted Path Wizard***. The trusted path is now restricted to authorized owner(s) that you specified.

Assigning a Trusted Path Policy

You can select a Trusted Path policy and assign it to endpoints/endpoint groups and users/user groups.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Trusted Path policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

4. Click **Assign**.

   Step Result: The ***Trusted Path*** dialog is displayed.

5. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

6. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

7. Click **OK**.

Result: The Trusted Path policy is assigned to endpoints, groups of endpoints, or users.

Assigning a Trusted Path Policy to a Group

You can assign a Trusted Path policy to group of selected endpoints using the ***Assign Policy*** dialog.

Note: The ***Assign Policy*** dialog is also used to assign a Trusted Path policy to a selected endpoint. See Assigning a Trusted Path Policy to an Endpoint on page 196 if you are assigning the policy to an endpoint.

1. Select **Manage** > **Groups**.

   Step Result: The ***Groups*** page is displayed.

2. Select a group from the **Browser** tree.

3. From the **View** list, select **Application Control Policies**.

   Step Result: The Application Control policies for the selected group are displayed.

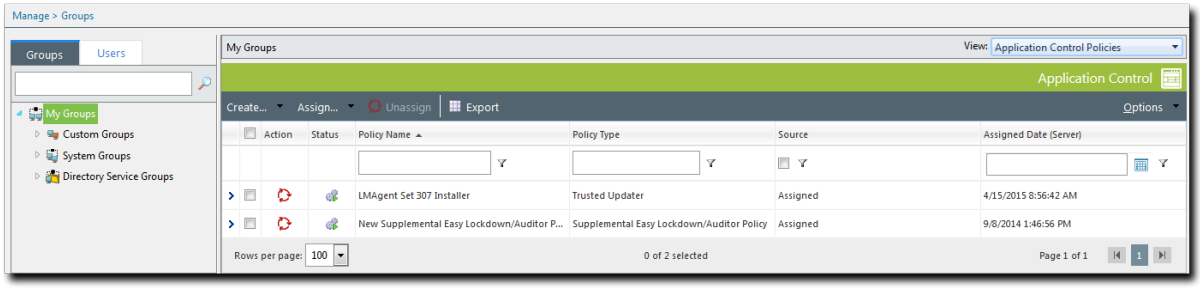


Figure 75: Groups - Application Control Policies View

> **Note:** Inherited policies can not be selected. In addition, the **Source** column reads *Inherited*.

4. From the toolbar, select **Assign** > **Trusted Path**.

   Step Result: The ***Assign Policy*** dialog is displayed.

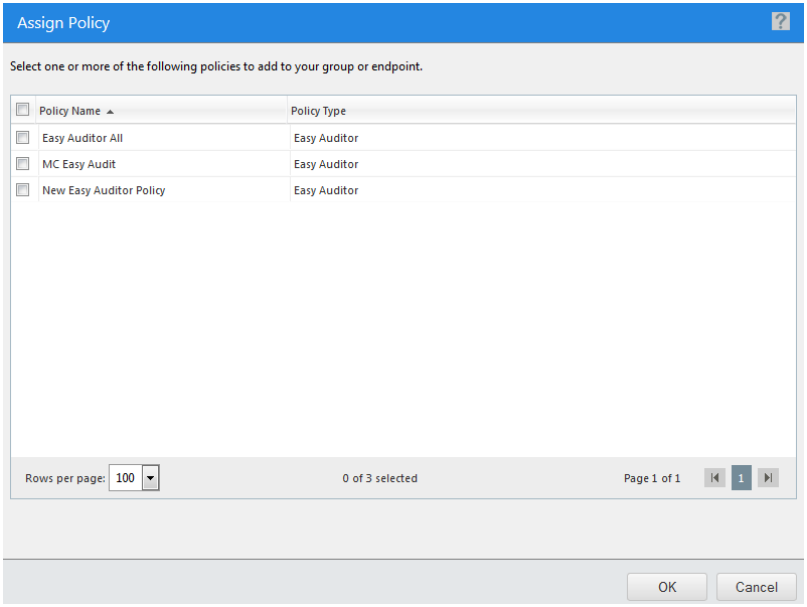


Figure 76: Assign Policy Dialog

5. Select one or more Trusted Path policies.
6. **Note:** The purpose of a Trusted Path policy is to enable one or more specified users to run executables in a designated file system path on a locked-down endpoint. You should ensure that the policy you are assigning to the group is already assigned to the relevant user(s).

   Click **OK**.

Result: One or more Trusted Path policies are assigned to the group.

Assigning a Trusted Path Policy to an Endpoint

You can assign a Trusted Path policy to a selected endpoint.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.
2. In the **Endpoint Name** column, click an endpoint link.

   Step Result: Detailed information for the selected endpoint is displayed.
3. Select the ***Application Control Policies*** tab.

   Step Result: A list of Application Control policies assigned to the endpoint is displayed.

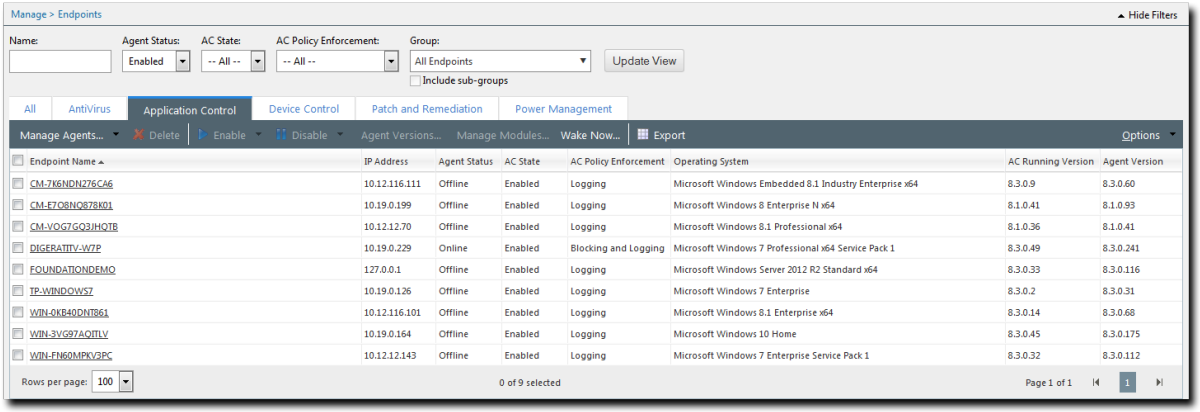


Figure 77: Application Control Policies Tab

4. From the toolbar, select **Assign** > **Trusted Path**.

   Step Result: The ***Assign Policy*** dialog is displayed.

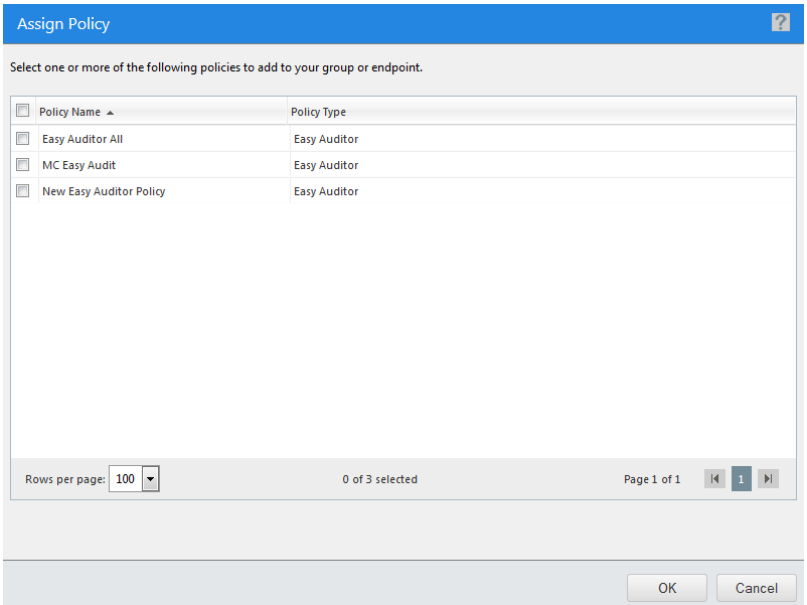


Figure 78: Assign Policy Dialog

5. Select one or more Trusted Path policies.
6. **Note:** The purpose of a Trusted Path policy is to enable one or more specified users to run executables in a designated file system path on a locked-down endpoint. You should ensure that the policy you are assigning to the endpoint is already assigned to the relevant user(s).

   Click **OK**.

Result: One or more Trusted Path policies are assigned to the endpoint.

Unassigning a Trusted Path Policy

You can unassign a Trusted Path policy, removing the association between it and its endpoints and users. Policies that are no longer assigned remain in the system as unassigned policies, which you can re-assign to endpoints and users at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select one or more Trusted Path policies.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.

4. Click **Unassign**.

   Step Result: One of two confirmation dialogs is displayed, depending on whether you selected a single policy or multiple policies.

Figure 79: Unassign Application Control Policy

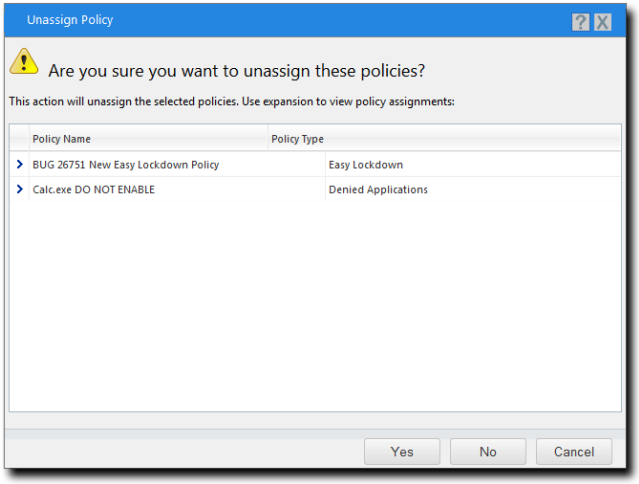


Figure 80: Unassign Multiple Application Control Policies

5. Click **Yes**.

Result: One or more Trusted Path policies are unassigned.

Editing a Trusted Path Policy

You can edit a Trusted Path policy. For example, you may want to add or remove trusted paths, or change its assignment.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Trusted Path policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

4. Click **Edit**.

   Step Result: The ***Trusted Path Wizard*** opens to the ***Name Policy and Add Trusted Paths*** page.

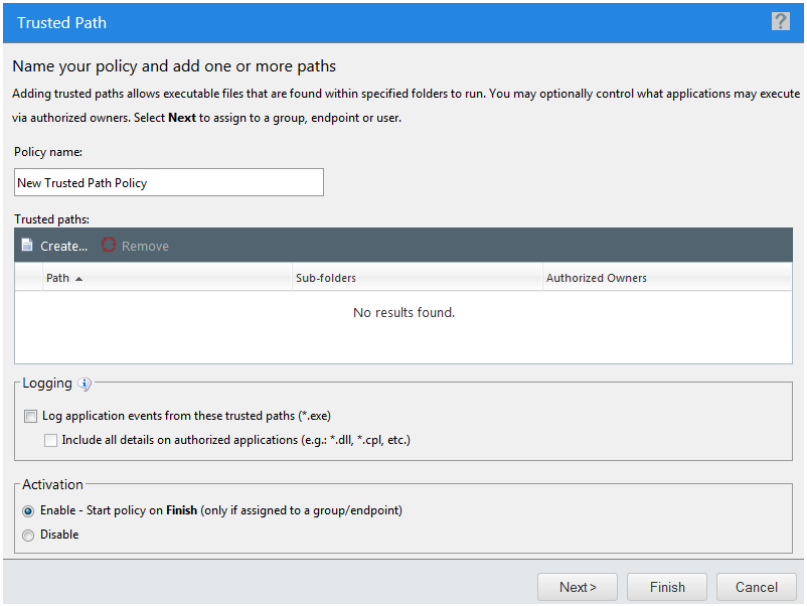


Figure 81: Trusted Updater Wizard - Add Application Updaters Page

5. [Optional] Edit the **Policy Name**.
6. To add a new trusted path:
   a) Click **Create**.

      Step Result: The ***New Trusted Path*** dialog is displayed.

   b) Type the name of the trusted path.

   Note:

   - Wild card (*) is supported.
   - System variables `%SystemRoot%`, `%SystemDrive%`, `%ProgramFiles%`, and `%LocalAppData%` are supported.
   - The path is validated before the dialog closes.

   c) Click **OK**.

      Step Result: The ***New Trusted Path*** dialog is closed and the trusted path is added to the list.

7. To remove an existing trusted path:
   a) Select the trusted path.

b) Click **Remove**.

Step Result: The ***Remove Trusted Path*** dialog is displayed.

c) Click **Yes**.

Step Result: The ***Remove Trusted Path*** dialog is closed and the trusted path is removed from the list.

8. [Optional] Add or remove *Authorized Owners* for this trusted path.

a) Click the **Authorized Owners** ellipses [...] button for the path.

Step Result: The ***Add Users*** dialog opens.

b) To add an Authorized Owner, search for the required user(s) in the **User name** field.
c) Select the required user(s) and click **Add Users**.
d) To remove an Authorized Owner, select it on the right-hand list and click **Remove**.
e) Click **OK**.

Step Result: The ***Add Users*** dialog closes and the list of **Authorized Owners** for that trusted path is updated.

9. [Optional] Change the **Logging** options.

10.[Optional] Edit the **Activation** options.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

11. Click **Next**.

Step Result: The ***Trusted Path Wizard*** opens to the ***Assign the trusted path to groups, endpoints and/or users*** page.

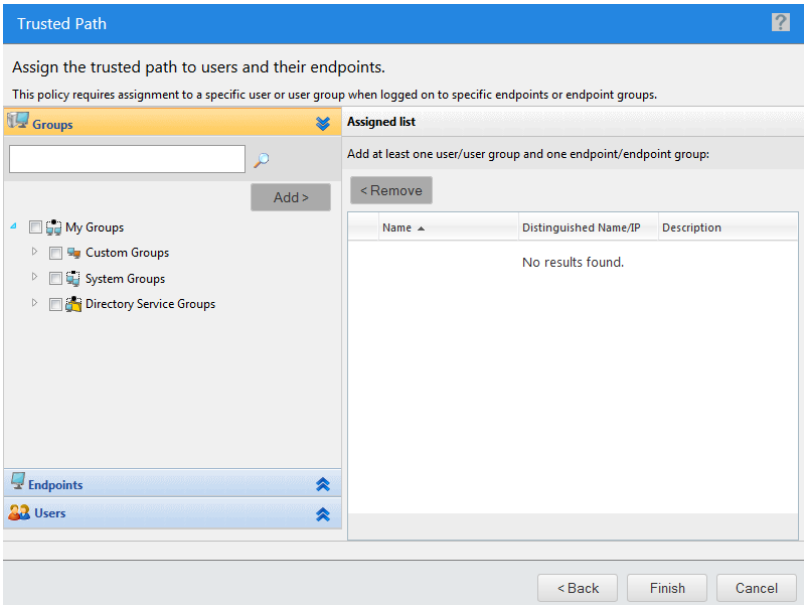


Figure 82: Trusted Path Wizard - Assign Groups and Endpoints Page

12. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

13. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

14. Click **Finish**.

Result: The Trusted Path policy has been edited.

Disabling a Trusted Path Policy

You can disable policies without deleting them. The details of the policies are retained and you can enable the policies at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the enabled Trusted Path policy or policies that you want to disable.

Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

Step Result: The selected policies are highlighted.

4. Click **Disable**.

Result: One or more Trusted Path policies are disabled.

Enabling a Trusted Path Policy

You can enable a Trusted Path policy that is currently disabled.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the disabled Trusted Path policy or policies that you want to enable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.
4. Click **Enable**.

Result: One or more Trusted Path policies are enabled.

Deleting a Trusted Path Policy

You can delete a Trusted Path policy, as long as it is not assigned to an endpoint or a user.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Trusted Path policy that is not assigned to an endpoint or user (**Assigned** column value of *Not Assigned*).

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.
4. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned.
5. Click **Yes**.

Result: The Trusted Path policy is deleted.

Exporting Trusted Path Policies

You can export a list of policies to a `csv` (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a `csv` file with the following columns:

Name	Description
Status	Enabled or Disabled

Name	Description
Policy Name	The name of the policy
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)
Policy Type	The type of policy (Easy Lockdown, Trusted Updater, and so on)
Last Updated Date (Server)	The date and time (on the server) that the policy was last changed

Trusting Files from the Application Library

You can trust an files directly from the Applicaion Library and add them to existing Trusted Updater Policy.

Prerequisites:

You have grouped or ungrouped installer files in your Application Library that you need to be treated as a Trusted Updater.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, expand the the containers until you reach the one containing the files you want to add.
3. In the ***Application Library*** list, select the files you want to trust.

   Tip: Sort the files by folder/path to help identify the files for a particular application.

   Step Result: The **Trust** button is enabled.

4. Click **Trust**.

   Step Result: The ***Trust Selected Files*** dialog opens.

5. Add the files to a new or existing policy:

Option	Description
Create a new Trusted Updater or Trusted Installer policy:	1. Select **Add to one or more existing policies** option, then click **OK**. 2. Type a **Policy Name** for the new Trusted Updater. Give the policy a descriptive name. For example, if this Trusted Updater policy relates to particular applications used by the graphics department you could name it `Graphics Applications`. 3. Add more files as trusted updaters to the new policy: a. Click **Add**. b. Select **Files from application library** or **Files from other policies**. c. Search for and select one or more files. d. Click **Add Updaters**. e. Click **OK**. 4. Select an **Activation** option. **Note:** If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time. 5. Click **Next**. The ***Assign the trusted updater to groups and/or endpoints*** panel displays. 6. Edit the list of targets (groups or endpoints) for the policy. 7. Click **Finish**.
Add the file to one or more existing policies:	1. Select the **Add to one or more existing policies** option. 2. Select one or more of the existing policies. You can click **View details** to review the policies first, paying particular attention to the users or endpoints that are affected. 3. Click **OK**.

Result: One or more files you selected from the Application Library are added as Trusted Updaters.

Working with Local Authorization

Local Authorization is a trust mechanism that allows a specified user to temporarily or permanently authorize an application that is not currently on a whitelist or permitted by another trust mechanism.

In Ivanti Application Control, an *authorized* application is either on a whitelist or is permitted by a trust mechanism, while a *denied* application is on the blacklist. A *non-authorized* application is one that is neither authorized nor denied.

Note:

An application that is neither authorized or denied (by being put on the blacklist) is sometimes said to be on the *graylist*.

An end user may need to run a non-authorized application. If the Ivanti Endpoint Security administrator trusts the end user's abilities, the administrator can assign a Local Authorization policy to that user. This enables the user to run non-authorized applications when needed. This can greatly reduce the administrative workload.

Local Authorization in Practice

Local Authorization is different from other Application Control policies in that it delegates the responsibility to run non-authorized files to selected end users.

With other Application Control policies, the Ivanti Endpoint Security administrator decides which applications are authorized and which are blocked. When an end user is assigned a Local Authorization policy, however, that user has the option of temporarily or permanently authorizing a non-authorized application.

The administrator should be careful when assigning a Local Authorization policy to an end user because of the power being delegated. But an experienced end-user may have a better knowledge of the applications that are available for use. Responsible use of Local Authorization provides benefits for both the end user and the administrator.

Local Authorization for the End User

An end user assigned a Local Authorization policy can interact with the system to authorize or deny non-authorized applications.

When the end-user user attempts to execute a non-authorized application, Ivanti Application Control displays a dialog which indicates that the application is non-authorized and presents several options to the user.

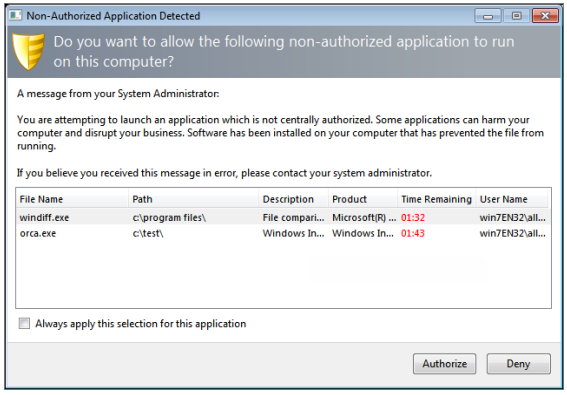


Figure 83: Non-authorized Application Detected Dialog

The ***Non-Authorized Application Detected*** dialog displays the details of the non-authorized file, including its name, path, description, and the product it is a part of. These details help the end user decide whether to authorize the application file or to deny it.

The user is allowed two minutes to decide whether to authorize or deny the file. The time counts down in the **Time Remaining** column. If the time runs out, the application file is denied permission to run.

The user can apply the authorize/deny decision permanently by selecting the **Always apply this selection for this application** checkbox. Leaving the checkbox deselected means that a decision has to be made each time the non-authorized file attempts to execute.

More than one executable file can be displayed in the dialog simultaneously. For example, an application's initial executable could be followed by associated DLLs. The end user can make a decision on each file.

Note: In Windows 8, applications can be launched from the Modern interface or from the Desktop. The Local Authorization dialog can only be displayed on the Desktop, however. If a user who is assigned a Local Authorization policy tries to launch an unauthorized application from the Modern interface, that user will not see the Local Authorization dialog unless he or she switches to the Desktop.

Local Authorization and Easy Auditor

Easy Auditor normally allows non-authorized applications to run on an endpoint. If Local Authorization is also applied, however, the user has to explicitly authorize such applications to run.

When Easy Auditor is applied to an endpoint, a user can launch and run an application that is not authorized. This happens transparently to the user (although the event will be logged if logging is enabled).

If a Local Authorization policy is then applied to that endpoint, however, the behavior changes. When the user tries to launch a non-authorized application, Ivanti Application Control displays the ***Non-Authorized Application Detected*** dialog. The user must click **Authorize** to run the application.

If the application file is not authorized within two minutes it times out and is denied permission to run. But if the user launches the application again, the dialog will reopen and it can be authorized at that point.

Creating a Local Authorization Policy

A Local Authorization policy can specify one or more users that are allowed to run non-authorized applications on specific endpoints or endpoint groups.

This type of policy links specific users with specific endpoints. This means that a specified user can only run non-authorized applications when logged in to a specified endpoint.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Click **Create** > **Local Authorization**.

   Step Result: The ***Local Authorization Policy Wizard*** opens.

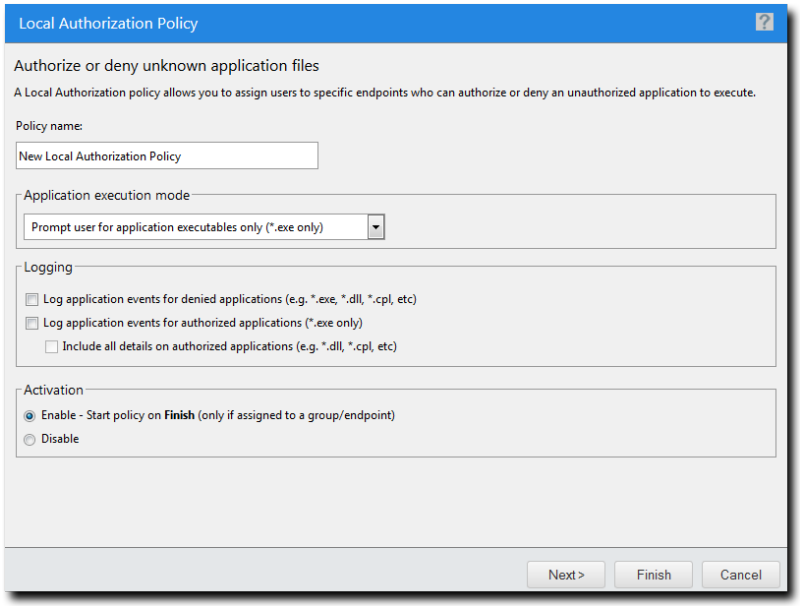


Figure 84: Local Authorization Policy Wizard

4. Type a name for the new policy in the **Policy Name** field.

Note: Give the policy a descriptive name. For example, if this Local Authorization policy relates to the IT Support group, you could name it `IT Support`.

5. Select the **Application execution mode**.

Option	Description
Prompt user for application executables only (*.exe only)	The user is only asked to authorize the application's initial executable.
Prompt user for all application file types (*.exe, *.dlls, *.cpls, etc)	The user is asked to authorize all the application's executable file types. **Important:** Selecting this option may cause a large number of prompts to be presented to the user when installing certain applications. Due to this impact, you should use this setting with caution.

6. Select the **Logging** options.

Note: An *authorized* application is one that is authorized by the end user and a *denied* application is one that is denied by the end-user, when prompted.

Log application events for denied applications (e.g. *.exe, *.dll, *.cpl, etc.)	Log attempts to run the application denied by the end user. This includes details of all the application's executable file types, not just the original executable (*.exe).
Log application events for authorized applications (*.exe only)	Log running of the application authorized by the end user. Only the initial executable (*.exe) is logged. **Note:** Use the **Include all details** option below to log subsequent executable files or dependent libraries loaded by the initial executable.
Include all details on applications (e.g. *.dll, *.cpl, etc.)	Detailed information on the granted application is logged (including every executable file and library loaded). This option is only available if the **Log application events for authorized applications** option is selected.

To create a log query and view the log results refer to Using Application Control Log Queries on page 277.

Note: These logging options can affect other Application Control policies. See Logging Managed Policies on page 73 for more information.

7. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

8. Click **Next** to assign the policy to users and endpoints.

Note: If you click **Finish** at this point, the policy will be created but will not have any assignment.

Step Result: The ***Local Authorization Policy Wizard*** opens to the ***Assign Local Authorization policy to groups, endpoints and/or users*** page.

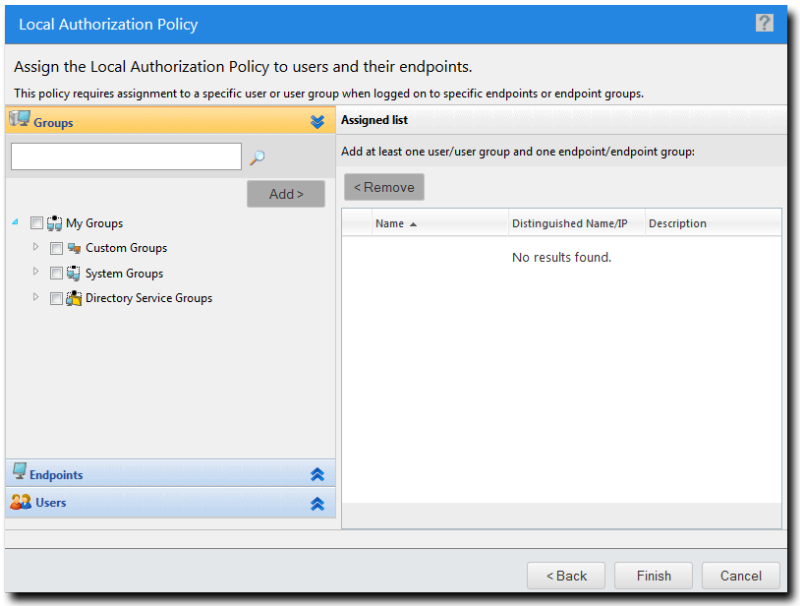


Figure 85: Local Authorization Policy Wizard - Assign Local Authorization policy to groups, endpoints and/or users Page

9. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.

Method	Steps
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

10. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

Tip: Some applications will not install or run unless they are assigned to the Local System and Network Service accounts, in addition to the required user or user group.

11. Click **Finish**.

Result: The Local Authorization policy is created and assigned to a combination of user(s) and endpoint(s).

Assigning a Local Authorization Policy

You can select a Local Authorization policy and assign it to endpoints/endpoint groups and users/user groups.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Local Authorization policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

4. Click **Assign**.

   Step Result: The ***Local Authorization*** dialog is displayed.

5. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows () to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

6. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

7. Click **OK**.

Result: The Local Authorization policy is assigned to endpoints/endpoint groups and users/user groups.

Assigning a Local Authorization Policy to a Group

You can assign a Local Authorization policy to a group of endpoints using the ***Assign Policy*** dialog.

Note: The ***Assign Policy*** dialog is also used to assign a Local Authorization policy to a selected endpoint. See Assigning a Local Authorization Policy to an Endpoint on page 215 if you are assigning the policy to an endpoint.

1. Select **Manage** > **Groups**.

   Step Result: The ***Groups*** page is displayed.

2. Select a group from the **Browser** tree.

3. From the **View** list, select **Application Control Policies**.

   Step Result: The Application Control policies for the selected group are displayed.

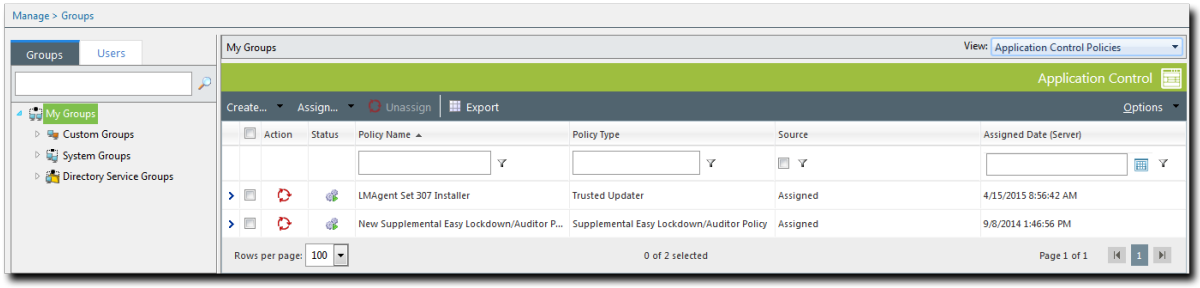


Figure 86: Groups - Application Control Policies View

> **Note:** Inherited policies can not be selected. In addition, the **Source** column reads *Inherited*.

4. From the toolbar, select **Assign** > **Local Authorization**.

   Step Result: The ***Assign Policy*** dialog is displayed.

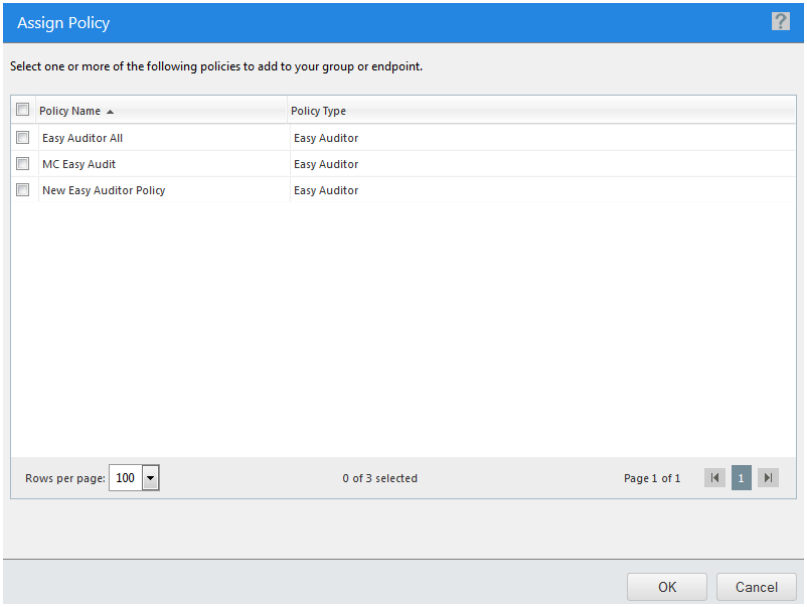


Figure 87: Assign Policy Dialog

5. Select one or more Local Authorization policies.
6. **Note:** The purpose of a Local Authorization policy is to enable one or more specified users to temporarily authorize files and applications on a locked-down endpoint. You should ensure that the policy you are assigning to the group is already assigned to the relevant user(s).

   Click **OK**.

Result: One or more Local Authorization policies are assigned to the group.

Assigning a Local Authorization Policy to an Endpoint

You can assign a Local Authorization policy to a selected endpoint.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.
2. In the **Endpoint Name** column, click an endpoint link.

   Step Result: Detailed information for the selected endpoint is displayed.
3. Select the ***Application Control Policies*** tab.

   Step Result: A list of Application Control policies assigned to the endpoint is displayed.

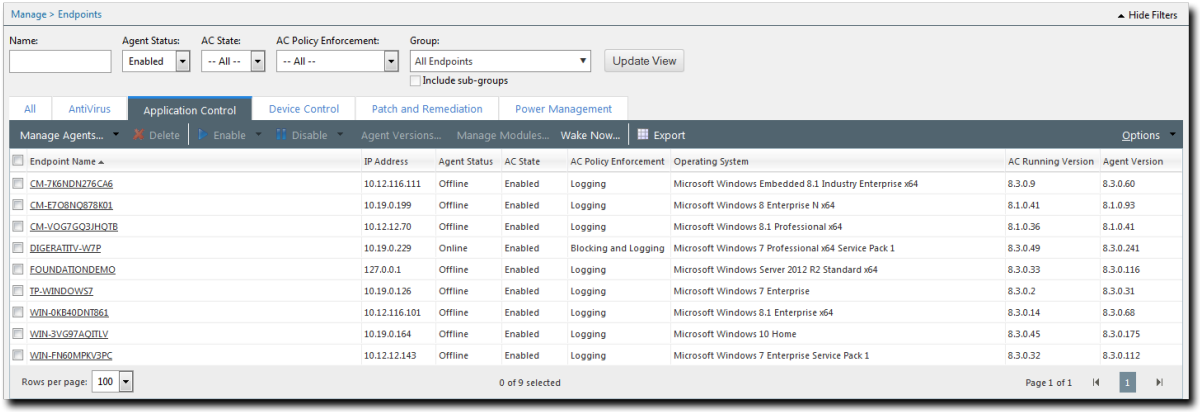


Figure 88: Application Control Policies Tab

4. From the toolbar, select **Assign** > **Local Authorization**.

   Step Result: The ***Assign Policy*** dialog is displayed.

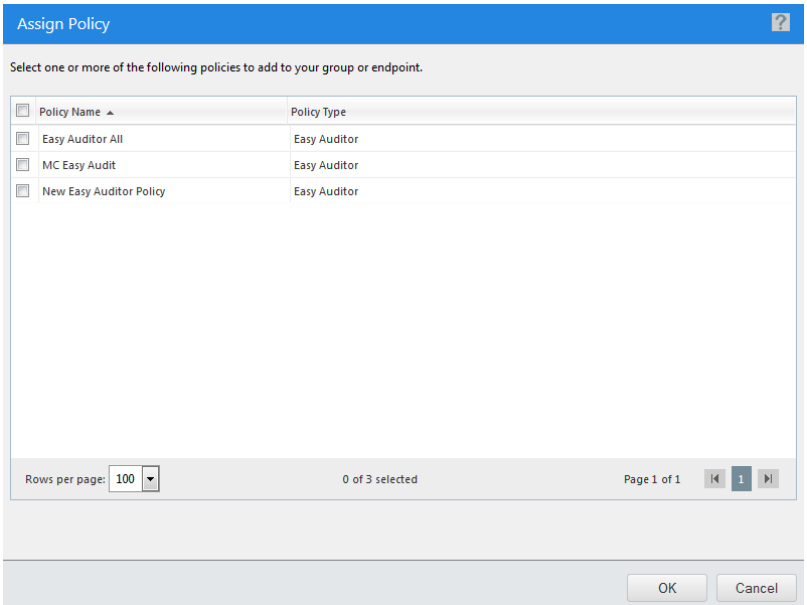


Figure 89: Assign Policy Dialog

5. Select one or more Local Authorization policies.
6. **Note:** The purpose of a Local Authorization policy is to enable one or more specified users to temporarily authorize files and applications on a locked-down endpoint. You should ensure that the policy you are assigning to the endpoint is already assigned to the relevant user(s).

   Click **OK**.

Result: One or more Local Authorization policies are assigned to the endpoint.

Editing a Local Authorization Policy

You can edit a Local Authorization policy. For example, you may want to add or remove users, or change the endpoints it is assigned to.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Local Authorization policy.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.

4. Click **Edit**.

   Step Result: The ***Local Authorization Policy Wizard*** opens.

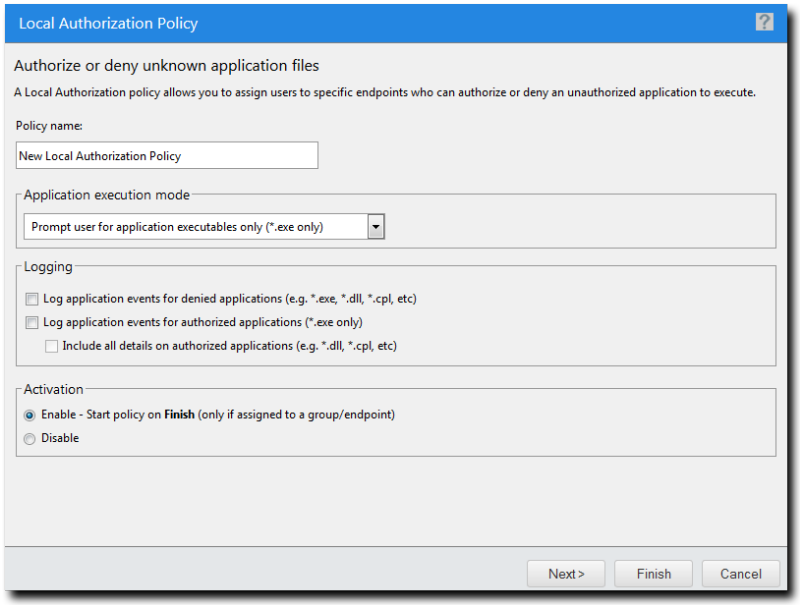


Figure 90: Local Authorization Policy Wizard

5. [Optional] Edit the **Policy Name**
6. [Optional] Change the **Application execution mode**.

Option	Description
Prompt user for application executables only (*.exe only)	The user is only asked to authorize the application's initial executable.
Prompt user for all application file types (*.exe, *.dlls, *.cpls, etc)	The user is asked to authorize all the application's executable file types. **Important:** Selecting this option may cause a large number of prompts to be presented to the user when installing certain applications. Due to this impact, you should use this setting with caution.

7. [Optional] Change the **Logging** options.

Note: An *authorized* application is one that is authorized by the end-user and a *denied* application is one that is denied by the end-user, when prompted.

Log application events for denied applications (*.exe)	Log the denial of an application by the user. This includes details of all the application's executable file types, not just the original executable (*.exe). **Note:** Only the initial executable file will be logged.
Log application events for granted applications (*.exe)	Log the authorization of an application by the user. Only the initial executable (*.exe) is logged. **Note:** Use the **Include all details** option below to log subsequent executable files or dependent libraries loaded by the initial executable.
Include all details on applications (e.g. *.dll, *.cpl, etc.)	Detailed information on the granted application is logged (including every executable file and library loaded). This option is only available if the **Log application events for authorized applications** option is selected.

To create a log query and view the log results refer to Using Application Control Log Queries on page 277.

Note: These logging options can affect other Application Control policies. See Logging Managed Policies on page 73 for more information.

8. [Optional] Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

9. [Optional] Click **Next** to change the user and endpoint assignment.

   Step Result: The ***Local Authorization Policy Wizard*** opens to the ***Assign Local Authorization policy to groups, endpoints and/or users*** page.

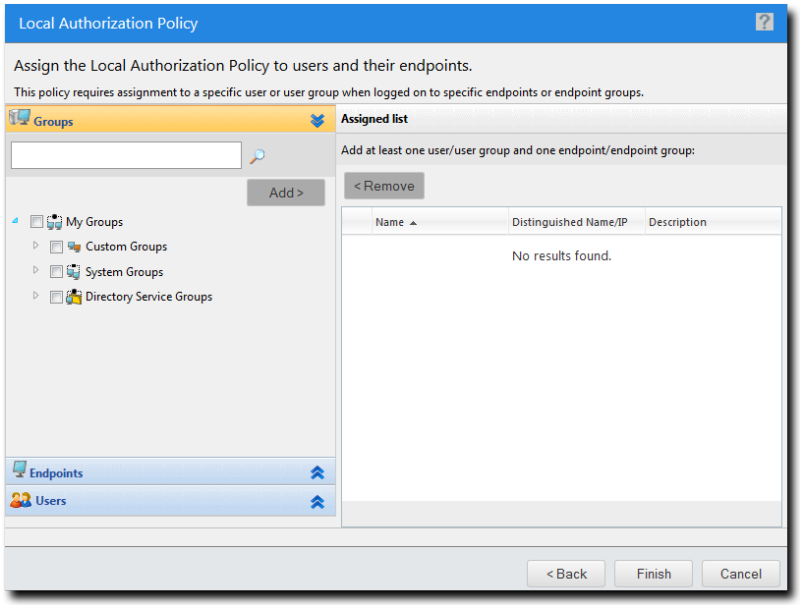


Figure 91: Local Authorization Policy Wizard - Assign Local Authorization policy to groups, endpoints and/or users Page

10. The policy must be assigned to at least one endpoint or endpoint group. Assign the policy to endpoints:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned list**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned list**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between Groups and Endpoints panes.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned list**.

11. The policy must be assigned to at least one user or user group. Assign the policy to users:

Method	Steps
To add users:	1. Select one or more users from the **Users** list. 2. Click **Add >**. **Note:** If you cannot locate a specific user, click the **Add Individual User** button. See Adding an Individual User to a Policy on page 115 for more information.
To remove users:	1. Select one or more users from the **Assigned list**. 2. Click **< Remove**.

Important: Both a user/user group AND an endpoint/endpoint group must be assigned.

Step Result: The selected users are displayed in the **Assigned list**.

12. Click **Finish**.

Result: The Local Authorization policy has been edited.

Disabling a Local Authorization Policy

You can disable a Local Authorization policy without deleting it. The policy details are retained and you can enable it again at a later time.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the enabled Local Authorization policy or policies that you want to disable.

Tip: Filter the **Policy Name** and **Policy Type** columns to locate policies.

Step Result: The selected policies are highlighted.

4. Click **Disable**.

Result: One or more Local Authorization policies are disabled.

Enabling a Local Authorization Policy

You can enable a Local Authorization policy that is currently disabled.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select the disabled Local Authorization policy or policies that you want to enable.

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policies are highlighted.
4. Click **Enable**.

Result: One or more Local Authorization policies are enabled.

Deleting a Local Authorization Policy

You can delete a Local Authorization policy, as long as it is not assigned to an endpoint or a user.

1. Select **Manage** > **Application Control Policies**.
2. Click the ***Trusted Change*** tab.
3. Select a Local Authorization policy that is not assigned to an endpoint or user (**Assigned** column value of *Not Assigned*).

   Tip: Filter the **Policy Name** and **Policy Type** columns to locate the policy.

   Step Result: The selected policy is highlighted.
4. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned.
5. Click **Yes**.

Result: The Local Authorization policy is deleted.

Exporting Local Authorization Policies

You can export a list of Local Authorization policies to a `csv` (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a `csv` file with the following columns:

Name	Description
Status	Enabled or Disabled

Name	Description
Policy Name	The name of the policy
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)
Policy Type	The type of policy (Easy Lockdown, Trusted Updater, and so on)
Last Updated Date (Server)	The date and time (on the server) that the policy was last changed

Chapter 7

Using Memory Protection

In this chapter:

Ivanti Application Control provides a memory protection feature which stops unauthorized code from outside the local file system from being executed within an authorized process running in memory.

This protection is implemented with *Memory Injection* policies, which can be assigned to endpoints and groups just like other Application Control policies.

Memory Injection Policies

Memory injection happens when external code executes within an authorized process. You can create a Memory Injection policy to protect against such an attack.

Reflective memory injection occurs when code that did not originate from an executable file or library on the local file system is executed within an authorized process running in memory. This is sometimes (though not always) the result of a malware attack. Because the code originates from outside the local file system, it bypasses the protection afforded by the endpoint's whitelist and application control policies.

Ivanti Application Control provides a Memory Injection policy to handle this type of violation. The policy can operate in two modes:

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

A Memory Injection policy operating in Enforcement mode provides ongoing protection against reflective memory injection attacks. But not every memory injection event is caused by malware. You can switch to Audit mode to investigate such events and to determine if the relevant file is safe or not.

Note:

Reflective memory injection is not the same as DLL injection. Both techniques involve external code executing within the memory space of a running process. In reflective memory injection, the external code originates outside the local file system. In DLL injection, the external code is in a DLL on the local file system.

Ivanti Application Control's Easy Lockdown and Supplementary Easy Lockdown/Auditor policies protect against unauthorized DLLs being loaded into a running process.

Memory Injection Scanning

Ivanti Application Control can scan running processes for reflective memory injection.

There are two mechanisms for running the scan.

System Calls	A scan is carried out whenever a process makes one of the following system calls: • Creating a process • Creating a thread (either in the process itself or in another process) • Loading a library
Polling	If a scan has not been initiated by any of the three system calls for five minutes, it is carried out automatically.

The combination of these mechanisms provides continuous protection against reflective memory injection without affecting performance.

Excluding Files from Memory Injection Policies

Some files use memory injection as part of their normal operation. You can exclude these files from Memory Injection policies.

Ivanti Application Control can detect memory injection, but this is not always the result of a malicious attack. For example, dynamic languages such as Python and .NET may execute code in memory that did not originate from the file system. Application Control will correctly identify this as a reflective memory injection, but in this case it is not desirable to shut down the process.

You can avoid this by configuring the Memory Injection policy to exclude files/applications that use memory injection in their normal operation. You can identify these files/applications by initially running the policy in Audit mode.

Multiple Policy Resultant Value Rules

If an endpoint is assigned or inherits more than one Memory Injection Policy, some settings may conflict. Resultant value rules determine which settings prevail on the endpoint.

When multiple Memory Injection Policies are assigned to groups, an endpoint may inherit different and possibly conflicting, policy settings. Standard inheritance rules mean that the policy assigned closest to the endpoint will prevail. However, if two policies are at the same parent level, or if two policies are assigned directly to the endpoint, the following rules determine which setting prevails.

Enforcement Settings	The *Enforce* setting overrides the *Audit only* setting.
Logging Settings	Logging turned on overrides logging turned off.
Exception Settings	Exception settings are cumulative, so all files listed as exceptions in the different policies are treated as if in a single list. If the exception option is different for the same file name, the *Log memory injection events* option will override the *Exclude from policy* option.

Working with Memory Injection Policies

Memory Injection Policies protect against external code executing within an authorized process. These policies can be used in the same way as other Application Control policies.

With Memory Injection Policies, it is important to remember that some files may legitimately execute external code within an authorized process. If such files generate a *false positive* you can disable or unassign the relevant policy, edit it to change the Enforcement option or create a policy exception for the file, then enable or reassign the policy to maintain protection against memory injection attacks.

Creating a Memory Injection Policy

A Memory Injection policy protects an endpoint's running processes from malicious attack. It is created using the ***Memory Injection Policy*** wizard.

1. Select **Manage** > **Memory Protection Policies**.

   Step Result: The ***Application Control Policies*** page opens at the ***Memory Protection*** tab.

   > **Note:** Even though **Memory Protection Policies** is a separate menu item from **Application Control Policies**, the feature is part of Application Control.

2. Click **Create**.

   Step Result: The ***Memory Injection Policy*** wizard opens

3. Type a **Policy Name** for the new Memory Injection policy.

   Note: Give the policy a descriptive name. For example, if this policy relates to a group of endpoints used by Product Managers you could name it `Product Management - Memory Policy`.

4. Select an Enforcement option.

Enforce - Stop a process when memory injection is detected	This will stop any process on any assigned endpoint when memory injection is detected, unless the relevant file or application is specified as an exception.
Audit only - Do not stop a process when memory injection is discovered	This will not stop a process when memory injection is discovered, but it will log the event. You can analyze the logs to determine what files or applications legitimately use memory injection, and you can then specify them as exceptions.

5. Select a **Logging** option. The logging option available depends on the Enforcement option selected in the previous step.

Enforce option selected	The **Logging** checkbox is selected by default but can be deselected if logging is not required.
Audit only option selected	The **Logging** checkbox is selected and disabled, which means that logging is mandatory.

6. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

7. Click **Next**.

   Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time.

   Step Result: The ***Memory Injection Policy Wizard*** opens to the ***Policy Exceptions*** page.

8. [Optional] Create one or more policy exceptions to prevent file processes from being stopped.
   a) Enter the path or filename.
      - Ensure paths end with a backslash (\), otherwise they will be interpreted as filenames.
      - A path's files and folders are excluded recursively.
      - Paths and filenames are not case-sensitive.
      - To exclude a specific file, use the fully qualified path e.g. C:\folder\subfolder\file.exe.
   b) Select the exception option.

Log memory injection events, but do not stop process from running	If a memory injection event occurs, it will be logged but the process will not be stopped. Note that logging must be turned on.
Exclude from policy	The file is not monitored for memory injection.

   c) Click **Add**.

      Step Result: The file name is displayed in the exception list.

   d) [Optional] Repeat the previous steps to add all required paths or files.
9. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time.

Step Result: The ***Memory Injection Policy Wizard*** opens to the ***Assign the Memory Injection Policy to groups and/or endpoints*** page.

10. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.

Method	Steps
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

11. Click **Finish**.

Result: The Memory Injection policy is created and assigned to the selected groups or endpoints. The new policy is displayed on the ***Memory Protection*** tab.

Assigning a Memory Injection Policy

You can select a Memory Injection policy and assign it to endpoints and/or groups of endpoints.

1. Select **Manage** > **Memory Protection Policies**.
2. Select a Memory Injection policy.

   Step Result: The selected policy is highlighted.
3. Click **Assign**.

   Step Result: The ***Memory Injection Policy*** dialog is displayed.
4. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

5. Click **OK**.

Result: The Memory Injection policy is assigned to endpoints and/or groups of endpoints.

Assigning a Memory Injection Policy to a Group

You can assign a Memory Injection policy to a selected group of endpoints using the ***Assign Policy*** dialog.

Note: The ***Assign Policy*** dialog is also used to assign a Memory Injection policy to a selected endpoint. See Assigning a Memory Injection Policy to an Endpoint on page 230 if you are assigning the policy to an endpoint.

1. Select **Manage** > **Groups**.

   Step Result: The ***Groups*** page is displayed.

2. Select a group from the **Browser** tree.
3. From the **View** list, select **Application Control Policies**.

   Step Result: The Application Control policies for the selected group are displayed.

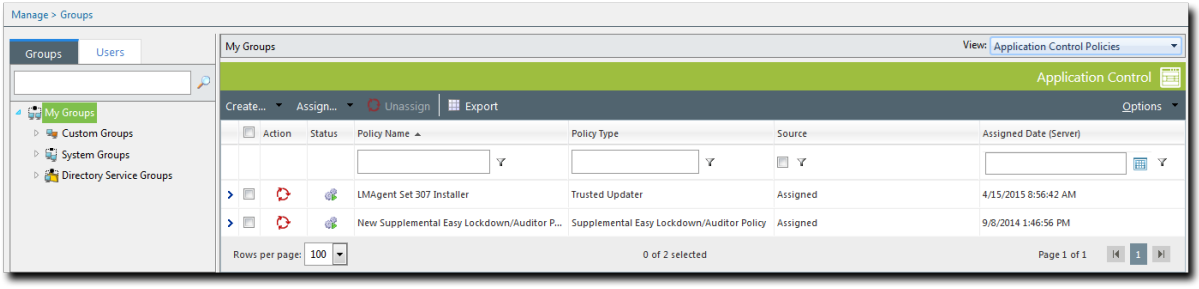


Figure 92: Groups - Application Control Policies View

Note: Inherited policies can not be selected. In addition, the **Source** column reads *Inherited*.

4. From the toolbar, select **Assign** > **Memory Injection Policies**.

   Step Result: The ***Assign Policy*** dialog is displayed, listing existing Memory Injection policies.

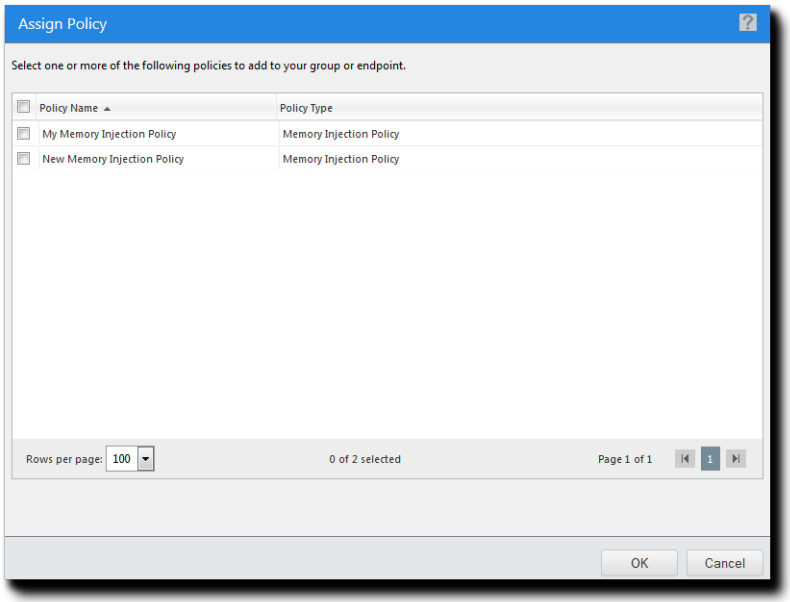


Figure 93: Assign Policy Dialog

5. Select one or more Memory Injection policies.

   Note: If multiple Memory Injection polices are assigned to a group, policy settings may conflict. Go to Multiple Policy Resultant Value Rules on page 225 to see how these conflicts are resolved.

6. Click **OK**.

Result: One or more Memory Injection policies are assigned to the group.

Assigning a Memory Injection Policy to an Endpoint

You can assign a Memory Injection policy to a selected endpoint.

1. Select **Manage** > **Endpoints**.

   Step Result: The ***Endpoints*** page opens to the **All** tab.

2. In the **Endpoint Name** column, click an endpoint link.

   Step Result: Detailed information for the selected endpoint is displayed.

3. Select the ***Application Control Policies*** tab.

   Step Result: A list of Application Control policies assigned to the endpoint is displayed.

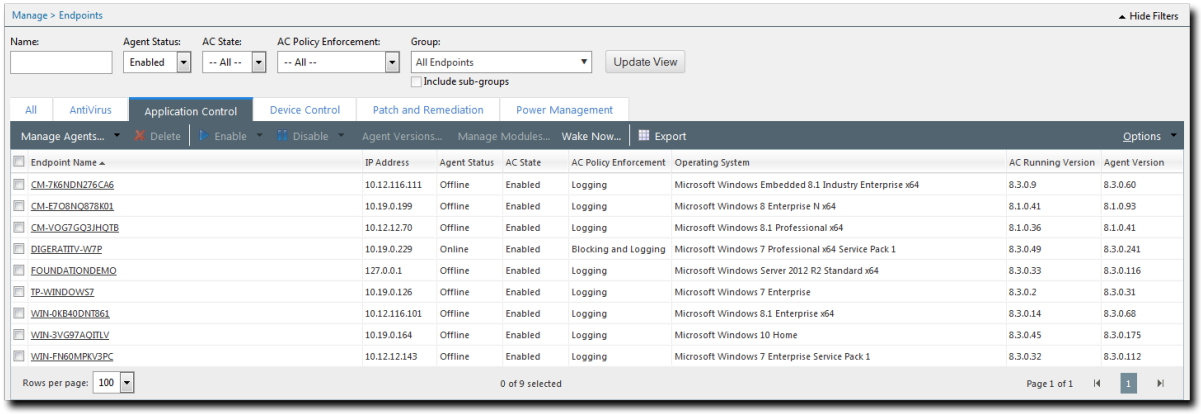


Figure 94: Application Control Policies Tab

4. From the toolbar, select **Assign** > **Memory Injection Policies**.

   Step Result: The ***Assign Policy*** dialog is displayed, listing existing Memory Injection policies.

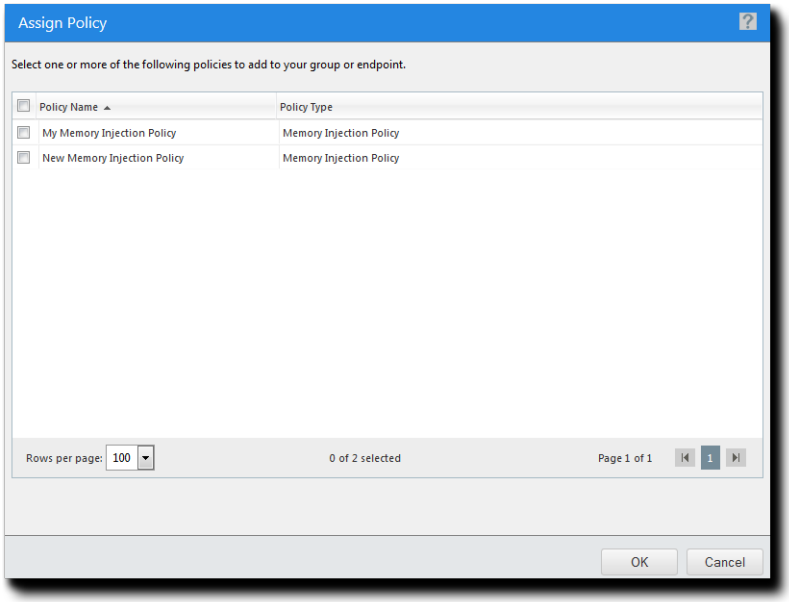


Figure 95: Assign Policy Dialog

5. Select one or more Memory Injection policies.

   Note: If multiple Memory Injection polices are assigned to an endpoint, policy settings may conflict. Go to Multiple Policy Resultant Value Rules on page 225 to see how these conflicts are resolved.

6. Click **OK**.

Result: One or more Memory Injection policies are assigned to the endpoint.

Unassigning a Memory Injection Policy

You can unassign a Memory Injection policy, removing the association between it and any endpoints. Policies that are no longer assigned to an endpoint remain in the system as unassigned policies, which you can re-assign to endpoints at a later time.

1. Select **Manage** > **Memory Protection Policies**.
2. Select one or more Memory Injection policies.

   Step Result: The selected policies are highlighted.

3. Click **Unassign**.

   Step Result: One of two confirmation dialogs is displayed, depending on whether you selected a single policy or multiple policies.

Figure 96: Unassign Application Control Policy

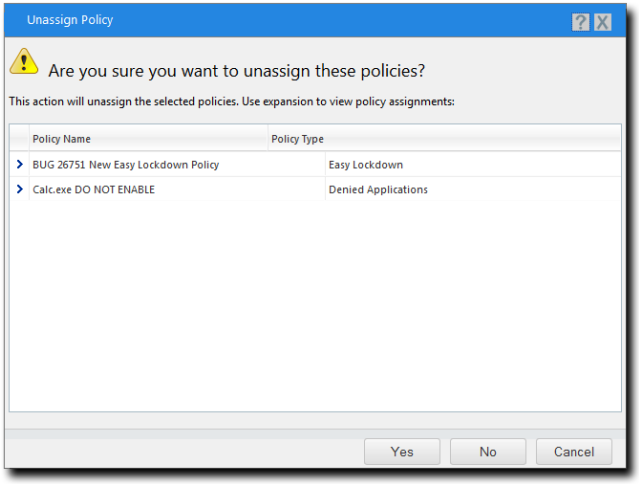


Figure 97: Unassign Multiple Application Control Policies

4. Click **Yes**.

Result: One or more Memory Injection policies are unassigned.

Editing a Memory Injection Policy

You can edit a Memory Injection policy and, for example, change its Enforcement option or the endpoints to which the policy is assigned.

1. Select **Manage** > **Memory Protection Policies**.
2. Select the Memory Injection policy to be edited.

   Note: You can only edit one policy at a time.

   Step Result: The selected policy is highlighted.

3. Click **Edit**.

   Step Result: The ***Memory Injection Policy Wizard*** opens.

4. [Optional] Edit the **Policy Name**.
5. [Optional] Select an Enforcement option.

Enforce - Stop a process when memory injection is detected	This will stop any process on any assigned endpoint when memory injection is detected, unless the relevant file or application is specified as an exception.
Audit only - Do not stop a process when memory injection is discovered	This will not stop a process when memory injection is discovered, but it will log the event. You can analyze the logs to determine what files or applications legitimately use memory injection, and you can then specify them as exceptions.

6. [Optional] Select a **Logging** option. The logging option available depends on the Enforcement option selected in the previous step.

Enforce option selected	The **Logging** checkbox is selected by default but can be deselected if logging is not required.
Audit only option selected	The **Logging** checkbox is selected and disabled, which means that logging is mandatory.

7. Select an option under **Activation**.

Option	Description
Enable	The policy will be enabled once it is created, as long as you assign it to a group or endpoint.
Disable	The policy will be disabled once created, even if it is assigned to a group or endpoint. You can enable it at a later time.

8. Click **Next**.

Note: If you click **Finish** at this point, the policy will be created but not assigned to any endpoints. You can assign the policy to endpoints at a later time.

Step Result: The ***Memory Injection Policy Wizard*** opens to the ***Policy Exceptions*** page.

9. [Optional] Add a policy exception.
   a) Enter the path or file name.
   b) Select the exception option.

Log memory injection events, but do not stop process from running	If a memory injection event occurs, it will be logged but the process will not be stopped. Note that logging must be turned on.
Exclude from policy	The file is not monitored for memory injection.

c) Click **Add**.

Step Result: The file name is displayed in the exception list.

d) [Optional] Repeat the previous steps to add all required paths or files.

10. [Optional] Remove a policy exception.

a) Select a policy exception from the exception list.
b) Click **Remove**.

11. [Optional] Edit a policy exception.

a) Select a policy exception from the exception list.
b) Click **Edit**.

Step Result: The form is loaded with the path/file name and the Exception option of the selected policy exception.

c) Change the path/file name or the Exception option.

12. Click **Next**.

Step Result: The ***Memory Injection Policy Wizard*** opens to the ***Assign the Memory Injection Policy to groups and/or endpoints*** page.

13. Build a list of targets (groups or endpoints) for the policy, using any of the following methods:

Method	Steps
To add groups of endpoints:	**1.** Select a group or groups from the **Groups** list. **2.** Click **Add >**.
To add individual endpoints:	**1.** Select an endpoint or endpoints from the **Endpoints** list. **2.** Click **Add >**.
To remove groups of endpoints:	**1.** Select a group or groups from the **Assigned List**. **2.** Click **< Remove**.
To remove individual endpoints:	**1.** Select an endpoint or endpoints from the **Assigned List**. **2.** Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and endpoints are displayed in the **Assigned List**.

14. Click **Finish**.

Result: The Memory Injection policy is edited.

Disabling a Memory Injection Policy

You can disable Memory Injection policies without deleting them. The details of the policies are retained and you can enable the policies at a later time.

1. Select **Manage** > **Memory Protection Policies**.
2. Select the enabled Memory Injection policies that you want to disable.

   Step Result: The selected policies are highlighted.
3. Click **Disable**.

Result: The selected Memory Injection policies are disabled.

Enabling a Memory Injection Policy

You can enable Memory Injection policies that are currently disabled.

1. Select **Manage** > **Memory Protection Policies**.
2. Select the disabled Memory Injection policy or policies that you want to enable.

   Step Result: The selected policies are highlighted.
3. Click **Enable**.

Result: The selected Memory Injection policies are enabled.

Deleting a Memory Injection Policy

You can delete a Memory Injection policy, as long as it is not assigned to any endpoint.

1. Select **Manage** > **Memory Protection Policies**.
2. Select the Memory Injection policy you want to delete, ensuring it is not assigned to an endpoint (**Assigned** column value of *Not Assigned*).

   Step Result: The selected policy is highlighted.
3. Click **Delete**.

   Step Result: A confirmation dialog is displayed.

   Note: If the policy is currently in use, a message is displayed telling you that the policy can not be deleted until it has been unassigned.
4. Click **Yes**.

Result: The Memory Injection policy is deleted.

Exporting Memory Injection Policies

You can export a list of policies to a csv (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

The list of policies is saved as a csv file with the following columns:

Name	Description
Status	Enabled or Disabled
Policy Name	The name of the policy
Assigned	Assigned/Not Assigned (if assigned, export includes the groups and endpoints that the policy is assigned to)
Policy Type	The type of policy (Memory Injection, Trusted Updater, and so on)
Last Updated Date (Server)	The date and time (on the server) that the policy was last changed

Chapter 8

Using Application Library

In this chapter:

- Working with Application Library
- The Application Library Page
- Organizing Application Library by Application
- Organizing Application Library by Application Group
- Assigning Policies in Application Library
- Maintaining the Application Library

The Application Library is the central area for managing all applications and files that are in Application Control.

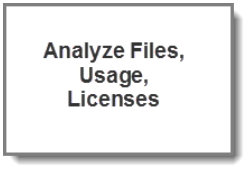
Administrators need to be able to manage the applications being used across the enterprise. They use an application scan (run during both Easy Auditor and Easy Lockdown) to locate the executable files on the network.

The results are placed into a local *Application Library* that is maintained at each server. Administrators can then associate files with applications, organize them into application and application group containers, and assign policies to authorize or block applications for selected groups.

Working with Application Library

This flow chart guides you through the process of using Application Library.

Populate Application Library with the executable files that are in use across the enterprise. You can do this by applying Easy Auditor and Easy Lockdown policies.



Analyze all files detected, check for valid software licenses and users.

Organize files into applications by creating application containers. An application container holds the multiple files that comprise a single application.

Organize applications into application groups to reflect the usage of software within departments and groups across the enterprise.

Assign application control policies, granting or denying access to specific applications for individuals or groups.

Maintain Application Library over time to reflect changing software deployments and usage throughout the enterprise.

The Application Library Page

The ***Application Library*** page is the main way to view and manage the files in Application Library. It has two main elements, the *Application Browser* and the *Application Library list*.

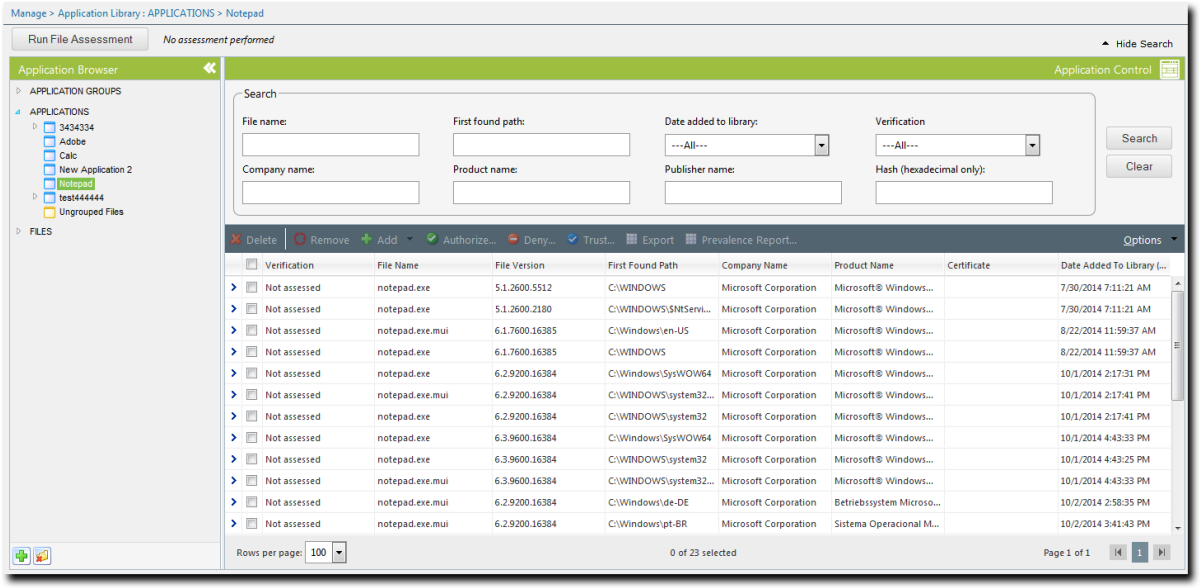


Figure 98: Application Library

The Application Browser is a collapsible navigation feature on the left of the page, which provides both predefined and user-defined views of the contents of the Application Library.

The Application Library list on the right displays a list of files, determined by the container selected in the Application Browser. You can view a file's details by clicking the arrow (>) beside the file name. The list also has an associated search feature normally displayed at the top of the page. It provides advanced search functionality and can be hidden when not in use.

Viewing the Application Library Page

The ***Application Library*** page displays the files, applications, and application groups that can be managed in Application Control.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

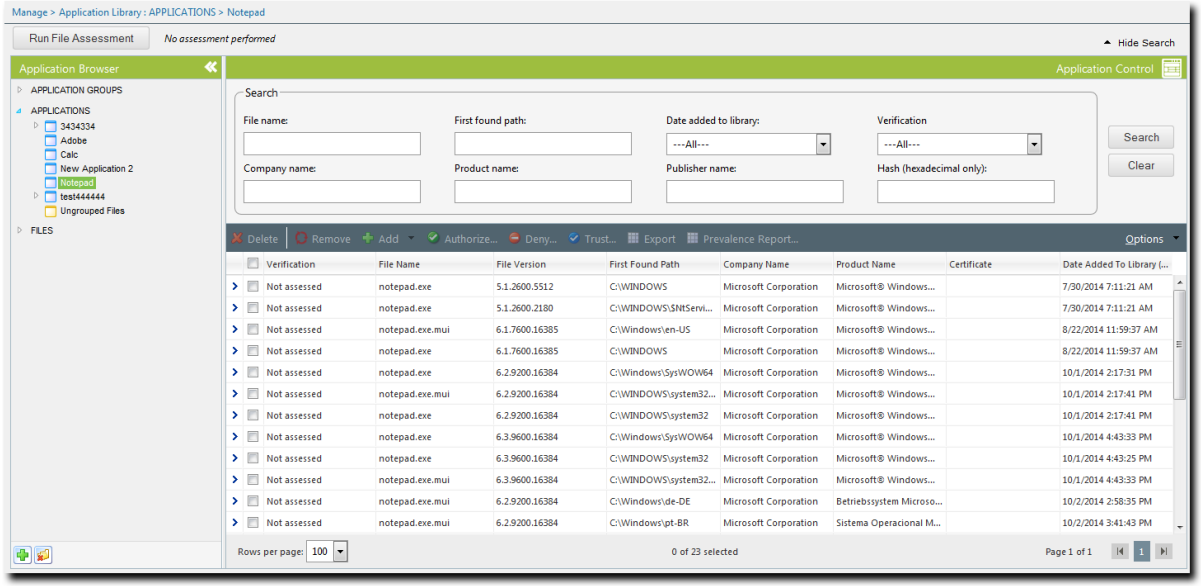


Figure 99: Application Library

2. Select the required view in the **Application Browser**.

   Step Result: The Application Library list displays the files or applications associated with the selected view.

3. If you have trouble finding specific files or applications, use the Search feature. See Application Library Search on page 249 for more information.

The Application Browser

The ***Application Browser*** is a navigation tool that allows you to view and manage the applications and files in the Application Library.

The browser is located on the left side of the ***Application Library*** page. It allows you to select predefined and user-defined containers to view and manage the applications and files that are in the Application Library. The contents of the selected container are displayed in a list on the right side of the ***Application Library*** page.

The ***Application Browser*** has the following elements:

Table 42: Application Browser Elements

Root Folders	Predefined Containers	User-defined Containers
APPLICATION GROUPS	**Ungrouped Applications**	Up to three levels of application group containers
APPLICATIONS	**Ungrouped Files**	Up to three levels of application containers
FILES	• **By Path** • **By Company** • **By Product** • **Unknown Files**	No user-defined containers

You can not rename or delete the root folders or predefined containers. You can create, rename, and delete as many user-defined containers as you need, and nest them up to three levels deep.

Tip: The ***Application Browser*** can be collapsed into a narrow vertical strip by clicking the arrow in its top right corner, providing more screen area. Clicking the arrow again expands the browser to its original size.

User-defined Containers

The ***Application Browser*** allows the user to create application and application group containers.

You can create and structure these containers to manage the many files that are normally contained in the Application Library. There are two types of user-defined containers, *application groups* and *applications*. You can create as many of these containers as you need and nest them up to three levels deep.

Application Groups	You create and structure application groups to represent software use in the organization. For example, you could have • **Department Applications** > **Design** > **Web Design** • **Finance** > **Accounts** **Note:** The **APPLICATION GROUPS** root folder contains a predefined container called **Ungrouped Applications** that displays applications that have not been assigned to any application group. You can not rename or delete this container.

Applications	Applications are defined by the user and each can contain one or more files. Multiple applications can contain the same file, but each application name must be unique. They can be nested up to three levels deep. You create and nest applications to organize them in a meaningful way. For example, you could have **Graphic Design Software** > **Adobe Programs** > **Adobe Photoshop 12**. **Note:** The **APPLICATIONS** root folder contains a predefined container called **Ungrouped Files** that displays files that have not been assigned to any application. You can not rename or delete this container.

Note: The **FILES** root folder view provides a general display of all files in the library. It has predefined categories (**By Path**, **By Company**, **By Product**) that are based on file metadata. It also has a predefined container called **Unknown Files**, for files that lack metadata. You can not create user-defined containers in this root folder.

Application Browser Actions

The ***Application Browser*** allows the user to perform actions on its root folders, predefined containers, and user-defined containers.

You can interact with the ***Application Browser*** in several ways:

Right-clicking a root folder	Opens a contextual menu with a **New** option that creates a new child container. **Note:** You can not add a child container to the ***FILES*** root folder.
Right-clicking a user-defined container	Opens a contextual menu with the following options: • **New** - Creates a new child container. Only three levels of user-defined containers are allowed, so this option is not available on a third-level container. • **Rename** - Renames the container. • **Delete** - Deletes the container. • **Authorize** - Opens the ***Authorize*** dialog to authorize the application or application group. • **Deny** - Opens the ***Deny*** dialog to deny the application or application group. **Note:** You can not perform any of these actions on a predefined container.
Selecting a container	Displays the container's files or applications.
Expanding a root folder or user-defined container	Clicking the small triangle beside a root folder or user-created container expands it to reveal the containers inside.

Using the buttons at the bottom of Application Browser	Adds or deletes containers at the selected level: • Add - Adds a child container to a first- or second-level user-defined container. • Delete - Deletes the selected container. The Add and Delete functionality depends on the container selected. You can not delete a predefined container, for example, or add more than three levels of user-defined containers.

Tip: The ***Application Browser*** can be collapsed into a narrow vertical strip by clicking the arrow in its top right corner. This provides more screen area to view the **Application Control** list. Clicking the arrow again expands the browser to its original size.

The Application Library List

The Application Library list displays the content of the container selected in the Application Browser.

The toolbar controls displayed above the list depend on what is selected in the Application Browser.

When an *application group* container is selected, the following controls are displayed:

Table 43: Application Group Container Selected

Control	Function
Delete	Delete the selected application(s) from Application Library. **Note:** No application files are deleted from the computer's file system.
Remove	Remove the selected application(s) from the application group.
Copy	Copy the selected application(s) to a new application group. **Note:** You *copy* an application when it is used by more than one application group; otherwise, you *move* it.
Move	Move the selected application(s) to a new application group.
Authorize	Open the ***Authorized*** dialog for the selected application(s).
Deny	Open the ***Denied*** dialog for the selected application(s).
Export	Export the list of applications as a comma-separated value file (`.csv`).

When an *application* container is selected, the following controls are displayed:

Table 44: Application Container Selected

Control	Function
Delete	Delete the selected file(s) from Application Library. **Note:** The file is only deleted from the Application Library database, not from the computer's file system.
Remove	Remove the selected file(s) from the application. **Note:** The file is not deleted from the Application Library database.
Copy	Copy the selected file(s) to a new application. **Note:** You *copy* a file when it is used by more than one application; otherwise, you *move* it.
Move	Move the selected file(s) to a different application.
Authorize	Open the ***Authorized*** dialog for the selected file(s).
Deny	Open the ***Denied*** dialog for the selected file(s).
Import	Import an XML list of applications to the Application Library. The file can be generated in the Agent Control Panel (Application Scan) or manually created using the appropriate schema.
Export	Export the list of applications as a comma-separated value file (`.csv`).
Prevalence Report	Generate a report of the displayed files' prevalence among endpoints; send a link to download the report, which is in a comma-separated value (`.csv`) format.

When a *files* container is selected, the following controls are displayed:

Table 45: Files Container Selected

Control	Function
Delete	Delete the selected file(s) from Application Library. **Note:** The file is only deleted from the Application Library database, not from the computer's file system.
Remove	This button cannot be used for file containers.
Add	Add the selected file(s) to an application or application group.
Authorize	Open the ***Authorized*** dialog for the selected file(s).

Control	Function
Deny	Open the ***Denied*** dialog for the selected file(s).
Export	Export the list of files as a comma-separated value file (`.csv`).
Trust	Open the ***Trust Selected Files*** dialog for the selected file(s).
Prevalence Report	Generate a report of the displayed files' prevalence among endpoints; send a link to download the report, which is in a comma-separated value (`.csv`) format.

When displaying files, the Application Library list has the following columns:

Table 46: Files List Columns

Column	Description
File Name	The file name, including extension.
File Version	File version number.
First Found Path	The path where the file was first discovered by Application Control.
Company Name	The company that created the file.
Product Name	The product that the file is part of.
Certificate	The status of the file's certificate (if it has one): • None - there is no certificate. • Present - there is a certificate but it is not yet verified. • Valid - certificate is verified and not expired. • Expired - certificate was verified but is now expired.
Date Added To Library (Server)	The date and time that the file was added to Application Library, shown as server time (UTC).

When displaying applications, the Application Library list has the following columns:

Table 47: Applications List Columns

Column	Description
Application Name	The name assigned to the application by the user.
Date Added To Library (Server)	The date and time that the application was added to Application Library, shown as server time (UTC).

Select All Behavior

The Application Library list's Select All control provides useful functionality for managing large numbers of files or applications.

When you select a container in Application Browser the resulting list is initially displayed with none of the items selected.

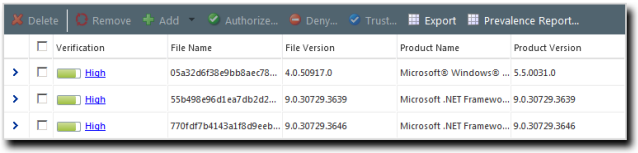


Figure 100: No Items Selected

If you select the **Select All** check box at the top of the column of check boxes, all the items on the page are selected. The number of selected items is shown in a pale yellow row displayed across the top of the list.

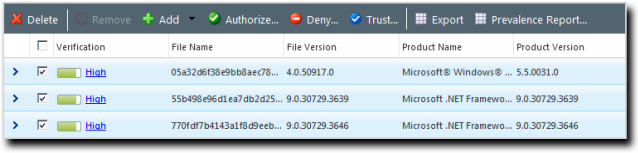


Figure 101: Page Items Selected

But if there are a large number of list items they will run across multiple pages. Clicking the **Select all** link selects all these items.

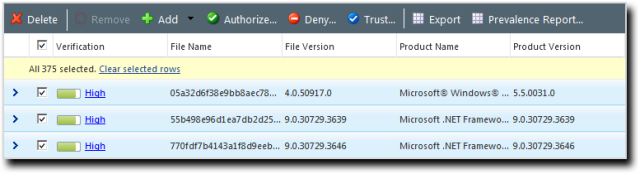


Figure 102: All Items Selected

Clicking **Clear selected rows** deselects all items and the pale yellow row disappears.

The Select All feature is especially useful when very large numbers of files are listed.

Application Library Search

The Application Library list has an advanced search feature, which allows you to search for files using a wide range of criteria.

The search feature is normally displayed above the Application Library list but can be hidden if required. You can search using the following criteria:

Table 48: Application Control Search

Field	Description
File name	All or part of the name of the file(s) you are searching for.
First found path	The path where the file was first discovered by Application Control.
Date added to library	When the file was added to the library; the drop-down provides the following options: • All • Last 5 days • Last 30 days • Last 60 days • Last 90 days • Older than 90 days
Company name	The company that created the file.
Product name	The product that the file is part of.
Publisher name	The publisher of the digital certificate associated with the file.

Field	Description
Hash (hexadecimal only)	A hash value which uniquely identifies a file. Several formats are supported, including SHA-256, SHA-1, and MD5. When searching on a hash value, ensure that you enter a valid value: • 128-bit MD5 hashes need 32 hexadecimal digits - for example, cd2eed36037845eef016323fd0f1ea0e • 160-bit SHA-1 hashes need 40 hexadecimal digits - for example, 011860ff7431b60ac59a606884c264acafe952ee • 256-bit SHA-256 hashes need 64 hexadecimal digits - for example, a5fa1120247ac52bcf8a9c0d679d9649bea71f345bb17a003ced5c52d8aaa9b5 **Note:** Hash values are not case sensitive. You can use upper or lower case.

Important: When you click **Search**, Application Library will return one or more files that meet the specified criteria, up to a limit of 20,000. If results are greater than 20,000 files, you will have to refine the search parameters to limit the results to a lower number.

Note: When an application group container is selected in Application Browser, the search feature has only one field, **Application Name**.

Generating an Application Prevalence Report

Application Library allows you to generate an *application prevalence report* which returns a list of specified files and the number of endpoints that each file was detected on.

Note: To generate an application prevalence report, the Application Library list must be displaying one or more *files* (not applications). If the list is not displaying files, the **Prevalence Report** button is disabled.

1. Click **Prevalence Report**.

   Step Result: The ***Application Prevalence Report*** dialog opens.

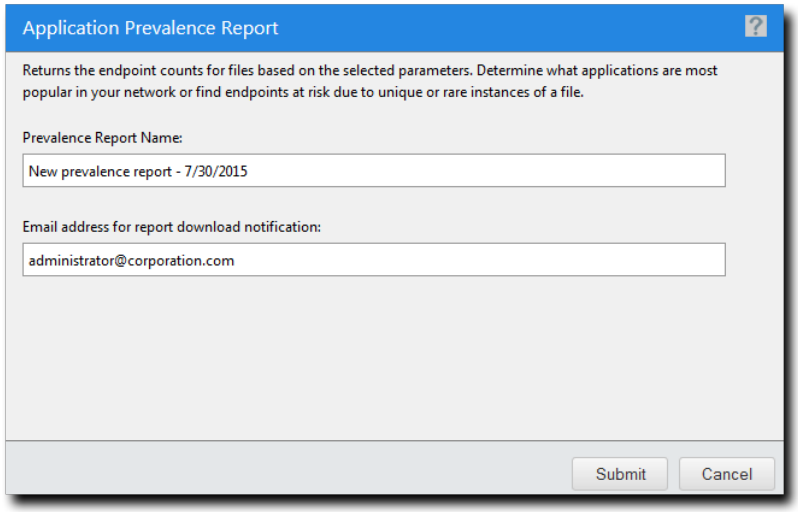


Figure 103: Application Prevalence Report Dialog

2. Type a name for the new prevalence report.
3. Type an email address that you can access.
4. Click **Submit**.

   Step Result: The dialog closes and Ivanti Application Control generates the report. When complete, it sends an email message to the address specified.

   Note: It can take up to two minutes to complete this operation.

5. Check your email program for the message.
6. Click the **Download** link in the message.

   Step Result: The prevalence report is downloaded in `.csv` format, and you are prompted to open or save the file.

7. Open the file with your computer's default application for opening `.csv` files (this is often *Microsoft Excel*). Alternatively, save the file for later analysis.

Listing Endpoints with File

Application Library allows you to view a list of endpoints which contain a specific file.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. Select an appropriate container in Application Browser (a container that has the file you are interested in).
3. Click the arrow (**>**) to expand the row to view file details.
4. Locate the **Endpoints with file** row and click the **endpoint(s) found** link.

   Step Result: The ***Endpoints With File*** dialog opens, listing all the endpoints on which the file was discovered.

5. [Optional] Click **Export** for a list of the endpoints as a comma-separated value file (`.csv`).

Application Library Drag and Drop

The Application Library has drag-and-drop functionality for its list and Application Browser.

You can drag items from the Application Library list to the Application Browser tree. You can also drag a container to a different location in the tree. The following table summarizes the drag-and-drop functionality.

Table 49: Application Library Drag and Drop

Location	Behavior
Files to Applications	The selected files are always **moved** from one container to another.
Applications to other Applications	The selected container in the tree is always **moved** from one container to another.
Applications to Application Groups	The applications in the list grid are always **moved** from one container to another.
Application Groups to other Application Groups	The selected container in the tree is always **moved** from one container to another.
Files to Application Groups	The files are always **moved** from one container to another.
Files to Applications or Application Groups	The files are always **copied** to the drop container in the APPLICATIONS or APPLICATION GROUPS section.

Location	Behavior
Applications to Application Groups	The application container from the APPLICATIONS section will always be **copied** when dropped to a container in the APPLICATION GROUPS section. **Note:** Applications can be copied into multiple application groups.

Important: Note that while most drag-and-drop operations **move** an item from one location to another, some operations **copy** the item, leaving the original in place.

Note: Application Library will not allow you to perform an invalid operation with drag and drop. If you attempt such an action, it will display an error dialog that explains what is wrong.

Organizing Application Library by Application

Application Library files can be organized in Application categories.

Once the Application Library contains a number of executable files, the first stage in organizing them is to group them into distinct applications.

1. In ***Application Browser***, you create *application containers* for each software program. You can nest these containers up to three deep to create a logical structure.
2. In the ***Application Control*** list, you select all the application's executable files and move them into its application container. Applications often have large numbers of executables, apart from the principal `.exe` file, and all of them must be moved.
3. Sometimes the same file is used by more than one application. After you move the file to the first application container, you can *copy* it to other application containers.

When you have grouped all files into applications, you can start creating *application groups* to represent application usage in your organization. See Organizing Application Library by Application Group on page 262 for more information.

Creating Applications

Application Browser allows you to create nested *applications* that help you organize and manage the files in Application Library.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In ***Application Browser***, click **Ungrouped Files**.

   Step Result: The ***Application Control*** list displays all files that have not yet been associated with an application.

   Note: Based on the files displayed and the company's software licences, determine the applications needed and the best way to organize them. Applications can be nested up to three deep.

3. Create the applications you need:

   a) Right-click **APPLICATIONS**.
   b) Select **New** from the contextual menu.
   c) Type a name for the new application.
   d) You can repeat this procedure to create all the application containers you need at this first level.

   Step Result: One or more application containers are added to the Application Browser.

4. If required, create nested applications at the second level:
   a) Right-click one of the applications that have already been created.
   b) Select **New** from the contextual menu.
   c) Type a name for the new application.
   d) You can repeat this procedure to create all the applications you need at this level.

   Step Result: One or more new applications are added to the ***Application Browser*** at the second level.

Note: Application names must be unique at each level. For example, if you create two first-level applications called (say) *Browsers* and *Business Applications*, you cannot have a second-level application called *Microsoft* under both of them. This restriction is necessary because applications are subsequently organized into application groups.

5. If required, create nested applications at the third level:
   a) Right-click one of the second-level applications already created.
   b) Select **New** from the contextual menu.
   c) Type a name for the new application.
   d) You can repeat this procedure to create all the applications you need at this level.

   Step Result: One or more new applications are added to the ***Application Browser*** at the third level.

Result: The Application Browser has a set of application containers that provide an appropriate structure to organize and manage the files in Application Library.

Adding Files to an Application

You can add executable files associated with a particular software program to an appropriate application container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select one of the the **FILES** containers: **By Path**, **By Company**, **By Product**, **Unknown Files**.
3. In the ***Application Control*** list, select the files you want to add to the application.

Tip: Sort the files by folder to help identify the files for a particular application.

4. Select **Add** > **Files To Application**.

   Step Result: The ***Add To Application*** dialog opens.

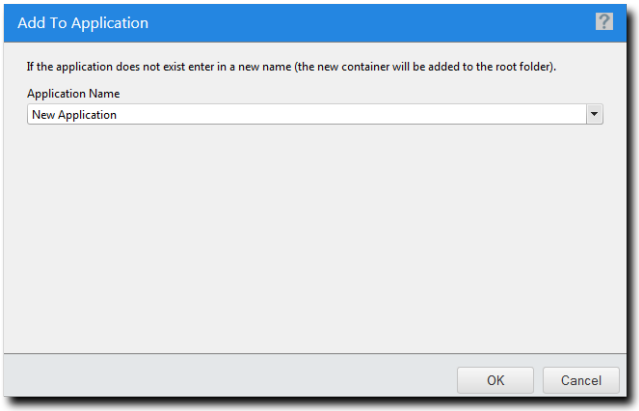


Figure 104: Application Library

5. a) Click the drop-down button and select an application from the list.

   Note: The dialog displays an alphabetically ordered flat list of all the applications that have been defined under **APPLICATIONS**. Ensure that the container you select is the correct one for the files you are moving.

   b) If the list does not contain the application you need, type its name in the **Application Name** field. This adds a new application container to the **APPLICATIONS** root folder.

6. Click **OK**.

Result: The files are added to the application container.

Note: The files will remain in the original **FILES** container.

Moving Files to Applications

You can move all the executable files associated with a particular software program into an appropriate application container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select the **Ungrouped Files** container (under **APPLICATIONS**).
3. In the ***Application Control*** list, select the files you require for a particular application.

Tip: Sort the files by folder to help identify the files for a particular application.

4. Click **Move**.

   Step Result: The ***Move Files to Application*** dialog opens.

5. Select an **Application** from the list.

   Note: The dialog displays an alphabetically ordered flat list of all the applications that have been defined under **APPLICATIONS**. Depending on how you have defined and nested these containers, not all of them may be suitable for holding application files. Ensure that the container you select is the correct one for the files you are moving.

6. Click **OK**.

Result: The files are moved from **Ungrouped Files** to an application container.

Copying Files into Applications

You can copy files from one application container to another.

Application suites from certain manufacturers often contain files that are used by more than one application. In this case, you must copy the file(s) into each relevant application container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select the application container that contains the file(s) you want to copy.
3. In the **Application Control** list, select the file(s) that you want to copy.
4. Click **Copy**.

   Step Result: The ***Copy to Application*** dialog opens.

5. Select an **Application** from the list.

   Note: The dialog displays an alphabetically ordered flat list of all the application containers that have been created. Depending on how you have defined and nested them, they may not all be suitable for holding application files. Ensure that the container you select is the correct one for the files you are moving.

6. Click **OK**.

Result: The selected files are copied from the source application container to the target container.

Moving an Application to an Application

You can associate an application container with an existing application container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select an applicaton container.
3. Right-click the application container and select **Move**.

   Step Result: The ***Move to Application*** dialog opens. The dialog displays an alphabetically ordered flat list of all the applications that have been defined under **APPLICATIONS**.
4. Select an **Application** from the list.
5. Click **OK**.

Result: The application container becomes a subgroup of the application container you moved it to.

Select an Applications File to Import

Use this window to import Applications into the Application Library using a valid XML file.

Generating the file using the Application Scan in the Agent Control Console

You can scan the applications on an endpoint to generate a list of applications installed on it.

1. On the endpoint, select **Start** > **Control Panel**.
2. Double-click **Agent Control Panel**.
3. From the main menu, click **Application Control**.
4. Click **Scan**.

Creating the file manually using the appropriate schema

You can create your own XML file using the following schema:

```
<?xml version="1.0"?>
<xs:schema id="NewDataSet" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="appdiscovery">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="publishers" minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="publisher" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:attribute name="publishername" type="xs:string" />
                  <xs:attribute name="issuer" type="xs:string" />
                  <xs:attribute name="version" type="xs:string" />
                  <xs:attribute name="serialnumber" type="xs:string" />
                  <xs:attribute name="validfrom" type="xs:string" />
                  <xs:attribute name="validto" type="xs:string" />
                  <xs:attribute name="subject" type="xs:string" />
                  <xs:attribute name="thumbprint" type="xs:string" />
                  <xs:attribute name="certificateformat" type="xs:string" />
                  <xs:attribute name="certificatebinary" type="xs:string" />
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="files" minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="file" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="hash" minOccurs="0" maxOccurs="unbounded">
                      <xs:complexType>
                        <xs:attribute name="algorithm" type="xs:string" />
                        <xs:attribute name="base64" type="xs:string" />
                      </xs:complexType>
                    </xs:element>
                    <xs:element name="info" minOccurs="0" maxOccurs="unbounded">
                      <xs:complexType>
                        <xs:attribute name="key" type="xs:string" />
                        <xs:attribute name="value" type="xs:string" />
                      </xs:complexType>
                    </xs:element>
                    <xs:element name="signature" minOccurs="0" maxOccurs="unbounded">
                      <xs:complexType>
                        <xs:attribute name="thumbprint" type="xs:string" />
                        <xs:attribute name="iscertificatevalid" type="xs:string" />
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                  <xs:attribute name="name" type="xs:string" />
                  <xs:attribute name="size" type="xs:string" />
                  <xs:attribute name="type" type="xs:string" />
                  <xs:attribute name="creation" type="xs:string" />
                  <xs:attribute name="lastaccessed" type="xs:string" />
                  <xs:attribute name="lastmodified" type="xs:string" />
                  <xs:attribute name="archive" type="xs:string" />
                  <xs:attribute name="isfiletrusted" type="xs:string" />
                  <xs:attribute name="sourceguid" type="xs:string" />
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
      <xs:attribute name="version" type="xs:string" />
      <xs:attribute name="timestamp" type="xs:string" />
      <xs:attribute name="agentname" type="xs:string" use="required" />
      <xs:attribute name="endpointguid" type="xs:string" />
      <xs:attribute name="jobname" type="xs:string" />
      <xs:attribute name="jobid" type="xs:string" />
```

Organizing Application Library by Application Group

An *application group* is a set of applications typically used by a group or organizational unit within the enterprise.

Once the Application Library's files have been categorized by application, you then organize them in application groups to represent software use in your organization. The general process is as follows:

1. In ***Application Browser*** create application groups to represent program usage in your organization. Application groups can be nested up to three deep.
2. In the ***Application Control*** list, you select all the applications used by a particular group and move them into the appropriate application group container in ***Application Browser***.
3. Sometimes one group's use of applications is similar to another group's. In these cases it is convenient to create a new application group by copying an existing one.

When you have created a set of application groups that model application use in your organization, you can apply authorization policies to these groups.

Creating Application Groups

Application Browser allows you to create nested application groups that help you organize and manage the programs in the Application Library.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

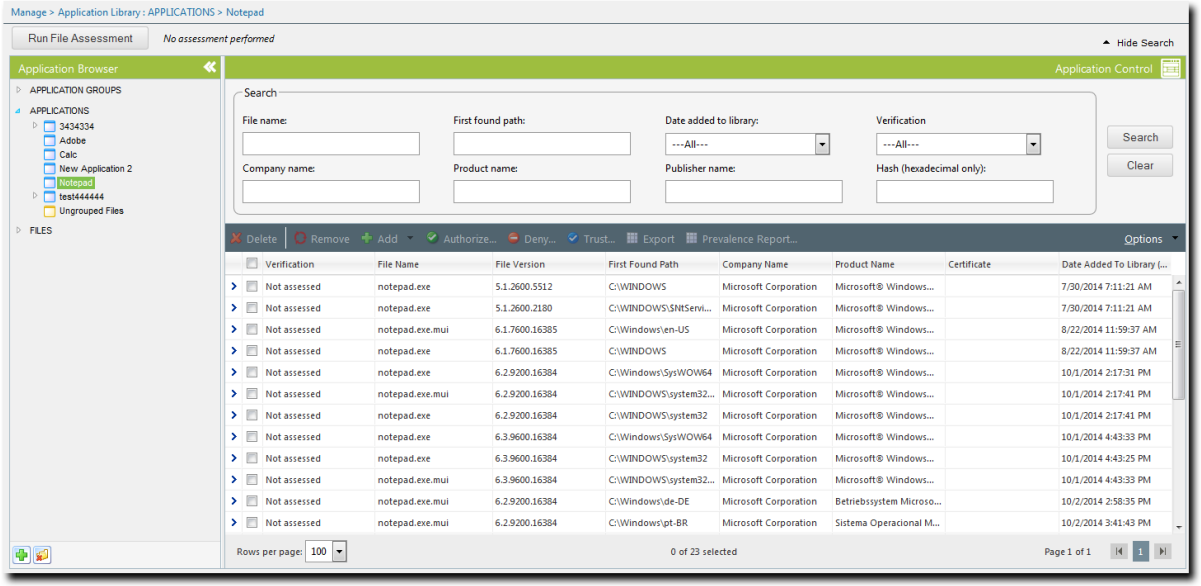


Figure 105: Application Library

2. In ***Application Browser***, click **Ungrouped Applications**.

   Step Result: The ***Application Control*** list displays all applications that have not yet been associated with an application group.

   Note: Based on the organization's and departments' use of applications, determine the application group containers needed and the best way to organize them. These containers can be nested up to three levels deep.

3. Create the application group containers you need:

   a) Right-click **APPLICATION GROUPS**.
   b) Select **New** from the contextual menu.
   c) Type a name for the new application group container.

   Step Result: A new application group is added to the Application Browser.

   Note: You can repeat this procedure to create all the application groups you need at this first level.

4. If required, start creating nested application groups at the second level:

   a) Right-click one of the application groups that has already been created.
   b) Select **New** from the contextual menu.
   c) Type a name for the new application group.

   Step Result: A new nested application group is added to the Application Browser at the second level.

   Note: You can repeat this procedure to create all the application groups you need at this level.

5. If required, start creating nested application groups at the third level:

   a) Right-click one of the nested application groups already created at the second level.
   b) Select **New** from the contextual menu.
   c) Type a name for the new application group.

   Step Result: A new nested application group is added to the Application Browser at the third level.

   Note: You can repeat this procedure to create all the application groups you need at this level.

Result: The Application Browser has a set of application groups that provide a structure to organize and manage the programs in Application Library.

Adding Files to an Application Group

You can add executable files into an appropriate application group container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select one of the the **FILES** containers: **By Path**, **By Company**, **By Product**, **Unknown Files**.
3. In the ***Application Control*** list, select the files you want to add to the application group.

   Tip: Sort the files by folder to help identify the files for a particular application.

4. Select **Add** > **Files To Application Group**.

   Step Result: The ***Add To Application Group*** dialog opens.

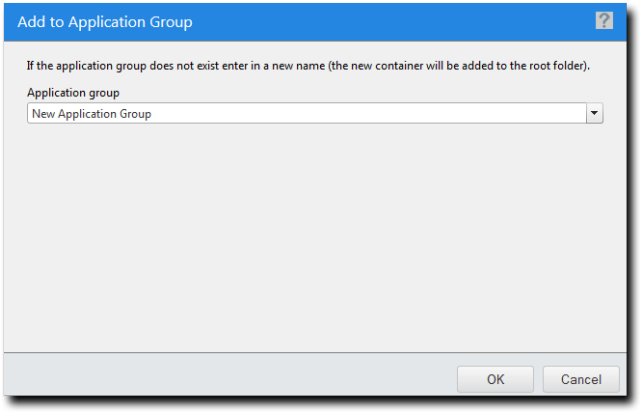


Figure 106: Add To Application Group Dialog

5. a) Click the drop-down button and select an application group from the list.

   Note: The dialog displays an alphabetically ordered flat list of all the application groups that have been defined under **APPLICATION GROUPS**. Ensure that the container you select is the correct one for the files you are adding.

   b) If the list does not contain the application group you need, type its name in the **Application group** field. This adds a new application group container to the **APPLICATION GROUPS** root folder.

6. Click **OK**.

Result: The files are added to the application group container.

> **Note:** The files will remain in the original **FILES** container.

Moving Files to an Application Group

You can move files from one application group to another application group container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select an application group container (under **APPLICATION GROUPS**).
3. Above the ***Application Control*** list, click the **Files** tab.
4. In the ***Application Control*** list, select the files(s) you want to move to an application group.
5. Click **Move**.

   Step Result: The ***Move Files to Application Group*** dialog opens.

6. a) Click the drop-down button and select an application group from the list.

   > **Note:** The dialog displays an alphabetically ordered flat list of all the application groups that have been defined under **APPLICATION GROUPS**. Ensure that the container you select is the correct one for the files(s) you are moving.

   b) If the list does not contain the application group you need, type its name in the **Application group** field. This adds a new application group container to the **APPLICATION GROUPS** root folder.
7. Click **OK**.

Result: The files are moved from one application group to another application group.

Copying Files to an Application Group

You can copy files from one application group to another application group.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select an application group container (under **APPLICATION GROUPS**).
3. Above the ***Application Control*** list, click the **Files** tab.
4. In the ***Application Control*** list, select the files(s) you want to copy to an application group.
5. Click **Copy**.

   Step Result: The ***Copy Files to Application Group*** dialog opens.

6. a) Click the drop-down button and select an application group from the list.

   Note: The dialog displays an alphabetically ordered flat list of all the application groups that have been defined under **APPLICATION GROUPS**. Ensure that the container you select is the correct one for the files(s) you are copying.

   b) If the list does not contain the application group you need, type its name in the **Application group** field. This adds a new application group container to the **APPLICATION GROUPS** root folder.

7. Click **OK**.

Result: The files are copied from one application group to another application group.

Moving Applications to an Application Group

You can move applications needed by an organizational group or user into an appropriate application group container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select the **Ungrouped Applications** category (under **APPLICATION GROUPS**).
3. In the ***Application Control*** list, select the application(s) you want to move to an application group.
4. Click **Move**.

   Step Result: The ***Move Applications to Application Group*** dialog opens.

5. a) Click the drop-down button and select an application group from the list.

   Note: The dialog displays an alphabetically ordered flat list of all the application groups that have been defined under **APPLICATION GROUPS**. Ensure that the container you select is the correct one for the application(s) you are moving.

   b) If the list does not contain the application group you need, type its name in the **Application group** field. This adds a new application group container to the **APPLICATION GROUPS** root folder.

6. Click **OK**.

Result: The applications are moved from **Ungrouped Applications** to an application group.

Copying Applications into Application Groups

You can copy applications needed by an organizational group or user into an appropriate application group container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select an application group container (under **APPLICATION GROUPS**).
3. Above the ***Application Control*** list, click the **Applications** tab.
4. In the ***Application Control*** list, select the application(s) you want to copy to an application group.
5. Click **Copy**.

   Step Result: The ***Copy Applications to Application Group*** dialog opens.

6. a) Click the drop-down button and select an application group from the list.

   Note: The dialog displays an alphabetically ordered flat list of all the application groups that have been defined under **APPLICATION GROUPS**. Ensure that the container you select is the correct one for the application(s) you are moving.

   b) If the list does not contain the application group you need, type its name in the **Application group** field. This adds a new application group container to the **APPLICATION GROUPS** root folder.
7. Click **OK**.

Result: The applications are copied from one application group to another application group.

Moving an Application Group to an Application Group

You can associate an application group container with an existing application group container.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In the ***Application Browser***, select an applicaton group container.
3. Right-click the application group container and select **Move**.

   Step Result: The ***Move to Application Group*** dialog opens. The dialog displays an alphabetically ordered flat list of all the applications that have been defined under **APPLICATION GROUPS**.

4. Select an **Application Group** from the list.

5. Click **OK**.

Result: The application group container becomes a subgroup of the application group container you moved it to.

Assigning Policies in Application Library

You can assign policies to the files, applications, and application groups in Application Library.

After you have organized the files in Application Library into applications and application groups, you can assign Authorized Applications and Denied Applications policies to them.

Authorizing Files, Applications, and Application Groups in Application Library

You can authorize files, applications, or application groups in Application Library by creating a new Authorized Applications policy or adding them to an existing Authorized Applications policy.

This has the effect of adding the application file(s) to the endpoint whitelist.

Authorizing Selected Files in Application Library

You can authorize files selected in Application Library using the ***Authorize Selected Files*** dialog.

Selected files can be authorized in two ways:

- By creating a new Supplemental Easy Lockdown/Auditor policy for them.
- By adding them to an existing Supplemental Easy Lockdown/Auditor policy.

1. Display the required file(s).

Context	Steps
APPLICATION GROUPS:	1. Select an APPLICATION GROUPS container. 2. Click the **Files** tab.
APPLICATIONS:	Select an APPLICATIONS container.
FILES:	Select a FILES container.

Step Result: Files are displayed in the Application Library list.

2. Select one or more files and click **Authorize**.

Step Result: The ***Authorize Selected Files*** dialog opens.

3. Authorize the selected file(s) using one of the following methods:

Method	Steps
New policy	1. Click the **Create a new Supplemental Easy Lockdown/ Auditor Policy** option. **Note:** This option is selected by default. 2. Click **OK**. The ***Authorize Selected Files*** dialog changes to the first screen of the ***Supplemental Easy Lockdown/Auditor*** wizard. See Creating a Supplemental Easy Lockdown/Auditor Policy on page 124 to complete the procedure.
Existing policy	1. Click the **Add to one or more existing policies** option. 2. Select one or more of the existing policies. **Note:** You should be familiar with the policies you select, especially the users or endpoints that the policies apply to. 3. Click **OK**.

Step Result: The selected file(s) are added to one or more existing Supplemental Easy Lockdown/ Auditor policies, and the ***Authorize Selected Files*** dialog closes.

Result: One or more files selected in Application Library are authorized to run, having been placed on the endpoint whitelist by a Supplemental Easy Lockdown/Auditor policy.

Authorizing Selected Applications in Application Library

You can authorize applications selected in Application Library using the ***Authorize Selected Applications*** dialog.

Selected applications can be authorized in two ways:

- By creating a new Supplemental Easy Lockdown/Auditor policy for them.
- By adding them to an existing Supplemental Easy Lockdown/Auditor policy.

1. Display the required applications(s).

Context	Steps
APPLICATION GROUPS:	1. Select an APPLICATION GROUPS container. 2. Select one or more applications. 3. Click the **Authorize** button.

Context	Steps
APPLICATIONS:	**1.** Right-click an APPLICATIONS container. **2.** Select **Authorize** on the context menu.

Step Result: The ***Authorize Selected Applications*** dialog opens.

2. Authorize the selected application(s) using one of the following methods:

Method	Steps
New policy	**1.** Click the **Create a new Supplemental Easy Lockdown/ Auditor Policy** option. **Note:** This option is selected by default. **2.** Click **OK**. The ***Authorize Selected Applications*** dialog changes to the first screen of the ***Supplemental Easy Lockdown/Auditor*** wizard. See Creating a Supplemental Easy Lockdown/Auditor Policy on page 124 to complete the procedure.
Existing policy	**1.** Click the **Add to one or more existing policies** option. **2.** Select one or more of the existing policies. **Note:** You should be familiar with the policies you select, especially the users or endpoints that are affected. **3.** Click **OK**.

Step Result: The selected application(s) are added to a Supplemental Easy Lockdown/Auditor policy, and the ***Authorize Selected Applications*** dialog closes.

Result: One or more applications selected in Application Library are authorized to run.

Denying Files, Applications, and Application Groups in Application Library

You can deny files, applications, or application groups in Application Library by creating a new Denied Applications policy or adding them to an existing Denied Applications policy.

This has the effect of adding the application file(s) to the centralized blacklist.

Denying Selected Files in Application Library

You can deny files selected in Application Library using the ***Deny Selected Files*** dialog.

Selected files can be denied in two ways:

- By creating a new Denied Applications policy for them.
- By adding them to an existing Denied Applications policy.

Denying a file in this way places it on a centralized blacklist.

1. Display the required file(s).

Context	Steps
APPLICATION GROUPS:	1. Select an APPLICATION GROUPS container. 2. Click the **Files** tab.
APPLICATIONS:	Select an APPLICATIONS container.
FILES:	Select a FILES container.

   Step Result: Files are displayed in the Application Library list.

2. Select one or more files and click **Deny**.

   Step Result: The ***Deny Selected Files*** dialog opens.

3. Deny the selected file(s) using one of the following methods:

Method	Steps
New policy	1. Click the **Create a new Denied Applications Policy** option. **Note:** This option is selected by default. 2. Click **OK**. The ***Deny Selected Files*** dialog changes to the first screen of the ***Denied Applications*** wizard. See Creating a Denied Applications Policy on page 108 to complete the procedure.

Method	Steps
Existing policy	**1.** Click the **Add to one or more existing policies** option. **2.** Select one or more of the existing policies. **Note:** You should be familiar with the policies you select, especially the users or endpoints that the policies apply to. **3.** Click **OK**.

Step Result: The selected file(s) are added to one or more existing Denied Applications policies, and the ***Deny Selected Files*** dialog closes.

Result: One or more files selected in Application Library are blocked from running, having been placed on a centralized blacklist by a Denied Applications policy.

Denying Selected Applications in Application Library

You can deny applications selected in Application Library using the ***Deny Selected Applications*** dialog.

Selected applications can be denied in two ways:

- By creating a new Denied Applications policy for them.
- By adding them to an existing Denied Applications policy.

Denying an application in this way places it on a centralized blacklist.

1. Display the required application(s).

Context	Steps
APPLICATION GROUPS:	**1.** Select an APPLICATION GROUPS container. **2.** Click the **Applications** tab.

Step Result: Applications are displayed in the Application Library list.

2. Select one or more applications and click **Deny**.

Step Result: The ***Deny Selected Applications*** dialog opens.

3. Deny the selected applications(s) using one of the following methods:

Method	Steps
New policy	1. Click the **Create a new Denied Applications Policy** option. **Note:** This option is selected by default. 2. Click **OK**. The ***Deny Selected Applications*** dialog changes to the first screen of the ***Denied Applications*** wizard. See Creating a Denied Applications Policy on page 108 to complete the procedure.
Existing policy	1. Click the **Add to one or more existing policies** option. 2. Select one or more of the existing policies. **Note:** You should be familiar with the policies you select, especially the users or endpoints that the policies apply to. 3. Click **OK**.

Step Result: The selected application(s) are added to one or more existing Denied Applications policies, and the ***Deny Selected Applications*** dialog closes.

Result: One or more applications selected in Application Library are blocked from running, having been placed on a centralized blacklist by a Denied Applications policy.

Maintaining the Application Library

Application Library provides a number of features that will help you maintain the library as its contents change.

Over time, Application Library's content will change as new software is adopted and older software is dispensed with. You will need to create new applications and delete old ones. Organizations also change, so you may need to modify application groups to reflect new departmental structures and software usage. Application Library allows you to rename, edit, delete, and move applications and application groups.

Maintaining Applications

Using the Application Browser's contextual menu, you can rename and delete applications.

Note: You cannot modify either the top-level predefined **APPLICATIONS** container or the **Ungrouped Files** container.

Renaming an Application

You can rename an application in Application Browser.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In **Application Browser**, right-click the application that you want to rename.
3. Select **Rename**.

   Step Result: The application name becomes editable.

4. Type the new name for the application.

   Note: Be careful not to use the name of any existing application. All application names must be unique, even when nested.

Result: The application has been renamed.

Deleting an Application

You can delete an application from Application Browser when it is no longer required.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In **Application Browser**, right-click the application that you want to delete.

   Step Result: A confirmation dialog appears.

3. Click **Yes**.

Result:
- The selected application is deleted.
- If the application has any child applications, those children are deleted as well.
- Any files in the deleted applications are moved to **Ungrouped Files**.

Note: If the application being deleted contains files that are also used by another application, those files are *not* moved to **Ungrouped Files**.

Maintaining Application Groups

Using the Application Browser's contextual menu, you can rename and delete application groups.

Note: You cannot modify either the top-level predefined **APPLICATION GROUPS** container or the **Ungrouped Applications** container.

Renaming an Application Group

You can rename an application group if required.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In **Application Browser**, right-click the application group that you want to rename.
3. Select **Rename**.

   Step Result: The application group name becomes editable.

4. Type the new name for the application group.

   Note: Be careful not to use the name of any existing application group. All application group names must be unique, even when nested.

Result: The application group has been renamed.

Deleting an Application Group

You can delete an application group from the Application Browser when it is no longer required.

1. Select **Manage** > **Application Library**.

   Step Result: The ***Application Library*** page is displayed.

2. In **Application Browser**, right-click the application group that you want to delete.

   Step Result: A confirmation dialog appears.

3. Click **Yes**.

Result:
- The selected application group is deleted.
- If the application group has any child applications group, those children are deleted as well.
- Any applications in the deleted applications group are moved to **Ungrouped Files**.

Chapter 9

Using Application Control Log Queries

In this chapter:

You can create application control log queries to retrieve detailed Application Control information from the database. In order for the log information to be in the database, you must have created some type of logging policy and assigned it to an endpoint. The endpoint then logs activity and passes it back to the server and database.

Working with Application Control Log Queries

You can create an application control log query to record the applications run or blocked on groups or individual endpoints, or on the network as a whole.

Creating an Application Control Log Query

You can create an application control log query to record details of blocked and authorized applications. A query can run immediately, or be scheduled for later or recurring execution.

1. Select **Review** > **Application Control Log Queries**.

   Step Result: The **Application Control Log Queries** page is displayed.

2. Click **Create**.

   Step Result: The ***Application Control Log Query Wizard*** is displayed.

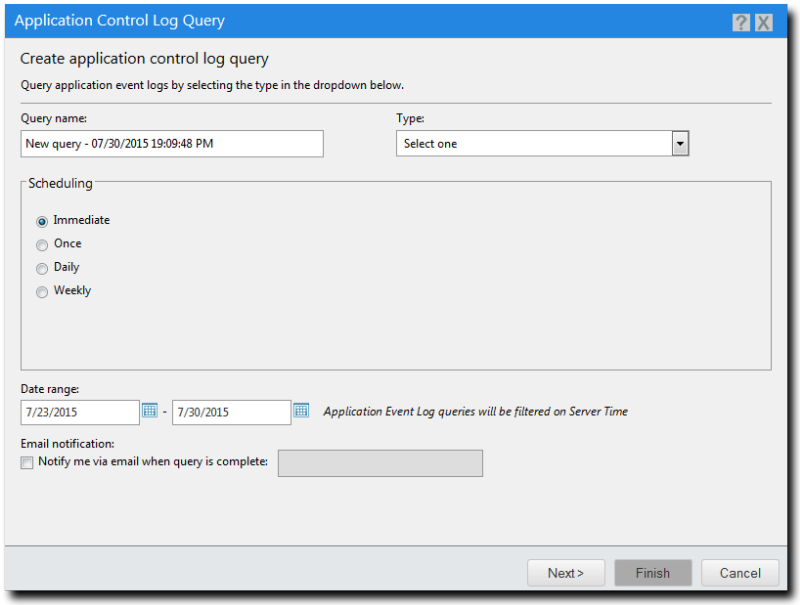


Figure 107: Application Control Log Query Wizard

3. Type a name for the new query in the **Query name** field.

Note: Give the query a descriptive name. For example, if this query relates to blocked applications on laptops in the sales group during July you could name it `Blocked Applications - Sales Laptops - July`.

4. Select the query **Type**.

Query Type	Description
All Application Events	Lists all logged application control events for a given set of endpoints and/or groups.
All Applications Added by Trusted Updaters	Lists applications that are added to the whitelist and can execute as a result of a Trusted Updater policy.
All Applications Allowed by Supplemental Easy Lockdown/Auditor Policy	Lists applications that are added to the whitelist and can execute as a result of a Supplemental Easy Lockdown/Auditor policy.
All Applications Allowed by Trusted Paths	Lists applications that are allowed to execute as a result of a Trusted Path policy.

Query Type	Description
All Applications Allowed by Trusted Publishers	Lists applications that are allowed to execute as a result of a Trusted Publisher policy. **Note:** Only local applications can be authorized by a Trusted Publisher policy, not applications that reside on a network share.
All Applications Executed by Local Authorization	Lists applications that are authorized or denied by a Local Authorization policy. The list includes applications that are denied because they timed out waiting for user input.
All Denied Application Events	Lists applications that are being blocked because they were not present on an endpoint before lockdown nor are they authorized by any trust mechanism. The list includes applications that are explicitly being blocked due to Denied Applications policy.
All Memory Injection Detection Events	Lists all file processes that were detected as being affected by reflective memory injection. As well as the file processes that were stopped, the list includes the processes that were not stopped because they were in audit mode or on an exclusion list.
All Updaters Added by Trusted Updaters	Lists updater applications that are added to an endpoint's Trusted Updater policy as a result of a trusted updater action. Trusted Updater policies on the server may need to be updated with these latest files.
Easy Auditor: Applications Blocked when Enforcement is Enabled	Lists applications that are not on the whitelist or authorized by a trust mechanism. These applications will be blocked as soon as enforcement is enabled (using Easy Lockdown).
Most Frequently Denied Applications	Lists in rank order the applications that are being blocked in your environment. These denials are because an application is not present on an endpoint before lockdown nor is it authorized by any trust mechanism. The list also includes applications that are explicitly being blocked due to a Denied Applications policy.

5. Select from the **Scheduling** options.

Option	Steps
Immediate	Run an on-demand query. The query runs when you click **Finish**.

Option	Steps
Once	Schedule a once-off query: **1.** Enter a start date, or click the calendar icon to select a date from the calendar. **2.** Enter a start time, or click the clock icon to select a time from the time view popup. Times are assigned at half-hour intervals.
Daily	Schedule a daily query: **1.** Enter a start date, or click the calendar icon to select a date from the calendar. **2.** Enter a start time, or click the clock icon to select a time from the time view popup. Times are assigned at half-hour intervals. **3.** Enter the interval in days at which the query will run. Default is 1 (every day).
Weekly	Schedule a weekly query: **1.** Enter a start date, or click the calendar icon to select a date from the calendar. **2.** Enter a start time, or click the clock icon to select a time from the time view popup. Times are assigned at half-hour intervals. **3.** Enter the interval in weeks at which the query will run. Default is 1 (every week). **4.** Select one or more days on which the query will run. At least one day must be selected.

6. Specify the query's start date and end date in the **Date Range** fields.
7. Select whether you want an email notification when the query is complete. If you select this option, type your email address in the field provided.

Tip: If the query results in no data found, then the subject line of the resulting email will contain the message `Report result - No Results Found`.

8. Click **Next**.

Step Result: The ***Select endpoints/groups*** page is displayed.

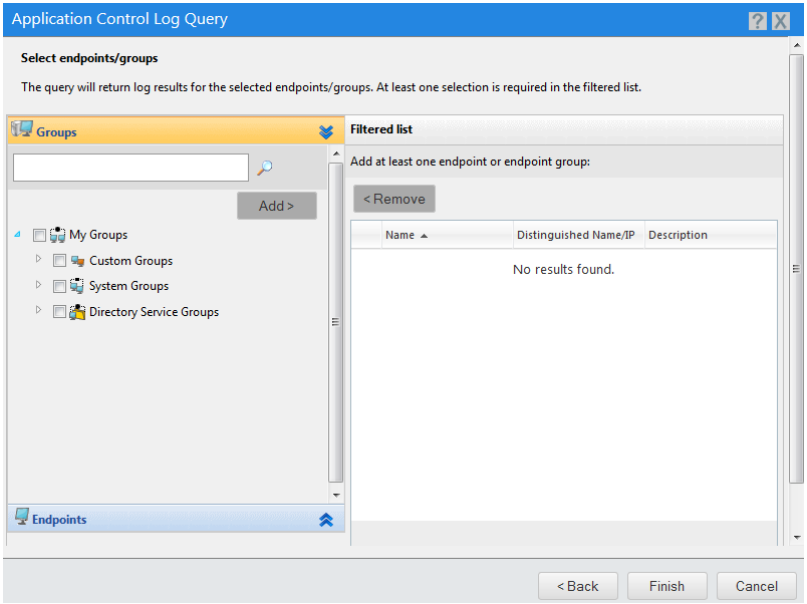


Figure 108: The Select Endpoints/Groups Page

9. Build a list of targets (groups or endpoints) for the query, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned List**.

10. Click **Finish**.

Step Result: The wizard closes and you return to the ***Application Control Log Queries*** page.

Result: A new application control log query is created. If it is a scheduled query, its summary is displayed under the **Scheduled** tab of the ***Application Event Logs*** page. When the query completes, its summary and a link to its results are displayed under the **Completed** tab of that page.

Viewing a Scheduled Application Control Log Query

You can view a list of scheduled application control log queries.

1. Select **Review** > **Application Control Log Queries**.
2. Click the **Scheduled** tab.

Step Result: The **Application Control Log Queries** page displays a list of scheduled queries.

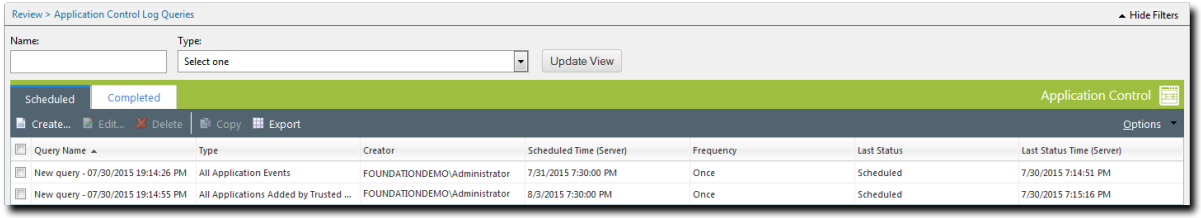


Figure 109: Application Control Log Queries - Scheduled Tab

Table 50: Application Control Log Queries

Column Name	Description
Query Name	The name of the query.
Type	The type of query.
Creator	The user that created the query.

Column Name	Description
Scheduled Time	The last scheduled time for the query.
Frequency	• Immediate • Once • Daily • Weekly
Last Status	• Scheduled - the query has not run before but is scheduled for a once-off or recurring execution. • Running - the query is running. • Finished - the query has run before and the last run was successful. • Error - the query has run before and the last run was unsuccessful.
Last Status Time	The time of the last reported status.

3. If necessary, sort the list to find the query you want to view.

Viewing a Completed Application Control Log Query

You can view a list of completed application control log queries, and examine the details of each query.

1. Select **Review** > **Application Control Log Queries**.

   Step Result: The **Application Control Log Queries** page opens displaying a list of completed queries.

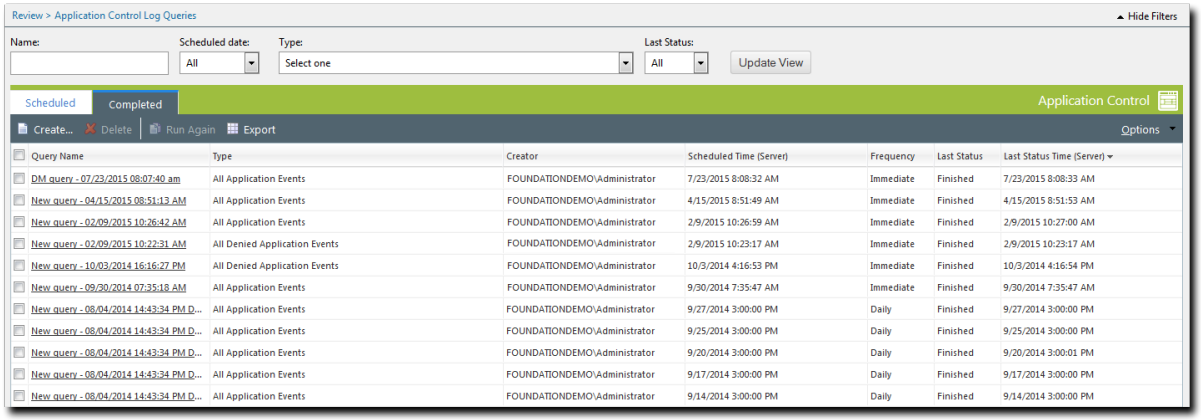


Figure 110: Application Control Log Queries - Completed Tab

Table 51: Application Control Log Queries

Column Name	Description
Query Name	The name of the query.
Type	The type of query.
Creator	The user that created the query.

Column Name	Description
Scheduled Time	The last scheduled time for the query.
Frequency	• Immediate • Once • Daily • Weekly
Last Status	• Scheduled - the query has not run before but is scheduled for a once-off or recurring execution. • Running - the query is running. • Finished - the query has run before and the last run was successful. • Error - the query has run before and the last run was unsuccessful.
Last Status Time	The time of the last reported status.

2. If necessary, sort the list to find the query you want to view.
3. In the **Query Name** column, click the name of the query you want to view.

Result: The ***Query Results*** page opens, displaying the detailed results of the query.

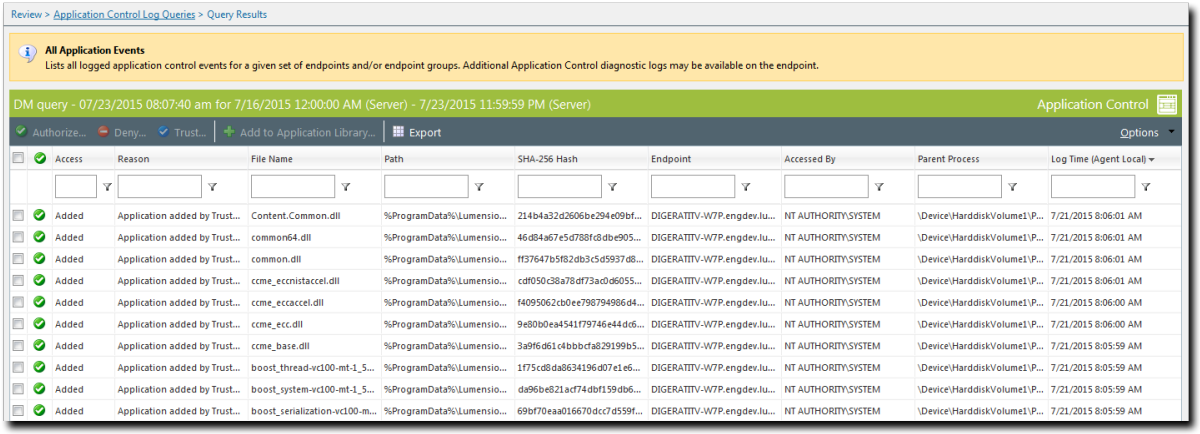


Figure 111: Application Control Log Queries - Query Results

The following table describes the ***Query Results*** page list.

Table 52: Query Results Page List

Column	Description
File Name	The name of the file found during the query.

Column	Description
Path	The file path for the file.
SHA-256 Hash	The hash number for the file.
Endpoint	The endpoint that contains the file.
Accessed By	The user account used to access the file.
Parent Process	The parent process for the file.
Log Time (Agent Local)	The date and time the file was found during the query, by agent local time.
Access	The access status for the file - Added, Allowed, Denied, or Blocked.
Reason	The reason the file was added, allowed, denied or blocked.

Note: If diagnostic logging is switched on, an All Application Events query may contain diagnostic log entries, which are denoted by the **Information** icon/access value and contain "source-of-trust" (SOT) information. Some diagnostic log entries are linked to processes rather than applications, and some may not have SHA-256 Hash values as they are not directly linked to a file.

For more information, see Application Control Diagnostic Logging on page 287.

After Completing This Task:
Now you can refresh the completed query to update the results grid with relevant events sent to the server from endpoints since the query last ran.

Refreshing a Completed Application Control Log Query
You can refresh a completed Application Control Log Query to import the latest events into the results grid list without having to recreate the query.

1. Select **Review** > **Application Control Log Queries**.
2. The ***Application Control Log Queries*** page opens.
3. [Optional] Sort the list to find the query you want to view.
4. Click the name of the query you want to view in the **Name** column.

   Step Result: The Application Control Log Query Results page opens, displaying the detailed results of the query.

5. Click **Refresh**.

Result: The results grid is updated with relevant events sent to the server from endpoints since the query last ran:

Scheduling	Refresh Behavior	
Immediate Once Daily	Results are updated to reflect all events sent from endpoints in the last 24 hour period, from the moment **Refresh** is clicked.	Original query is updated. Duplicate query is created.
Weekly	Results are updated to reflect all events sent from endpoints in the past 7 days from 7*24 hours before to the present moment when **Refresh** is clicked.	

Application Control Diagnostic Logging

Diagnostic logging provides more information than standard logging, but is switched off by default because of the large amount of information it sends to the server.

Application Control diagnostic logging provides a more detailed level of information than standard logging. These log entries appear in All Application Events log queries and are denoted by the **Information** icon/access value.

The diagnostic logs can help a system administrator to diagnose Trusted Updater issues. For example, an administrator creating Trusted Updater policies may sometimes authorize more applications than intended. Analyzing the diagnostic logs and following the "source of trust" can identify the relevant policy and show how it should be modified to restrict trust to the desired applications.

Diagnostic logging increases the volume of log traffic being sent from the endpoints to the server, so it should only be used if the logs are needed for troubleshooting. To switch on diagnostic logging, please contact Ivanti Self Service Support (https://support.heatsoftware.com) .

Editing a Scheduled Application Control Log Query

You can edit a scheduled application control log query.

1. Select **Review** > **Application Control Log Queries**.

2. Click the **Scheduled** tab.

   Step Result: The **Application Control Log Queries** page displays a list of scheduled queries.

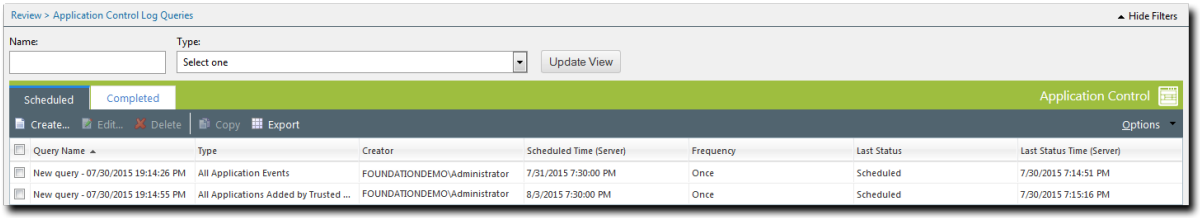


Figure 112: Application Control Log Queries - Scheduled Tab

Table 53: Application Control Log Queries

Column Name	Description
Query Name	The name of the query.
Type	The type of query.
Creator	The user that created the query.
Scheduled Time	The last scheduled time for the query.
Frequency	Immediate, Once, Daily, Weekly.
Last Status	Finished.
Last Status Time	The time of the last reported status.

3. If necessary, sort the list to find the query you want to edit.
4. Select the check box beside the query name.

Note: You can select only one query to edit at a time.

5. Click **Edit**.

   Step Result: The ***Application Control Log Query*** wizard opens, displaying details of the selected query.

6. [Optional] Change the name of the query in the **Query name** field.

Tip: Keep at least part of the original query name so that you will know that this query has been modified.

7. [Optional] Change the query **Type**.

Query Type	Description
All Application Events	Lists all logged application control events for a given set of endpoints and/or groups.

Query Type	Description
All Applications Added by Trusted Updaters	Lists applications that are added to the whitelist and can execute as a result of a Trusted Updater policy.
All Applications Allowed by Supplemental Easy Lockdown/Auditor Policy	Lists applications that are added to the whitelist and can execute as a result of a Supplemental Easy Lockdown/Auditor policy.
All Applications Allowed by Trusted Paths	Lists applications that are allowed to execute as a result of a Trusted Path policy.
All Applications Allowed by Trusted Publishers	Lists applications that are allowed to execute as a result of a Trusted Publisher policy. **Note:** Only local applications can be authorized by a Trusted Publisher policy, not applications that reside on a network share.
All Applications Executed by Local Authorization	Lists applications that are authorized or denied by a Local Authorization policy. The list includes applications that are denied because they timed out waiting for user input.
All Denied Application Events	Lists applications that are being blocked because they were not present on an endpoint before lockdown nor are they authorized by any trust mechanism. The list includes applications that are explicitly being blocked due to Denied Applications policy.
All Memory Injection Detection Events	Lists all file processes that were detected as being affected by reflective memory injection. As well as the file processes that were stopped, the list includes the processes that were not stopped because they were in audit mode or on an exclusion list.
All Updaters Added by Trusted Updaters	Lists updater applications that are added to an endpoint's Trusted Updater policy as a result of a trusted updater action. Trusted Updater policies on the server may need to be updated with these latest files.
Easy Auditor: Applications Blocked when Enforcement is Enabled	Lists applications that are not on the whitelist or authorized by a trust mechanism. These applications will be blocked as soon as enforcement is enabled (using Easy Lockdown).
Most Frequently Denied Applications	Lists in rank order the applications that are being blocked in your environment. These denials are because an application is not present on an endpoint before lockdown nor is it authorized by any trust mechanism. The list also includes applications that are explicitly being blocked due to a Denied Applications policy.

8. [Optional] Change the **Scheduling** option.

Option	Steps
Immediate	Run an on-demand query. The query runs when you click **Finish**.
Once	Schedule a once-off query: **1.** Enter a start date, or click the calendar icon to select a date from the calendar. **2.** Enter a start time, or click the clock icon to select a time from the time view popup. Times are assigned at half-hour intervals.
Daily	Schedule a daily query: **1.** Enter a start date, or click the calendar icon to select a date from the calendar. **2.** Enter a start time, or click the clock icon to select a time from the time view popup. Times are assigned at half-hour intervals. **3.** Enter the interval in days at which the query will run. Default is 1 (every day).
Weekly	Schedule a weekly query: **1.** Enter a start date, or click the calendar icon to select a date from the calendar. **2.** Enter a start time, or click the clock icon to select a time from the time view popup. Times are assigned at half-hour intervals. **3.** Enter the interval in weeks at which the query will run. Default is 1 (every week). **4.** Select one or more days on which the query will run. At least one day must be selected.

9. [Optional] Change the query's start date and end date in the **Date Range** fields.
10. [Optional] Select whether you want an email notification when the query is complete. If you select this option, type your email address in the field provided.

Tip: If the query results in no data found, then the subject line of the resulting email will contain the message `Report result - No Results Found`.

11. Click **Next**.

Step Result: The ***Select endpoints/groups*** page is displayed.

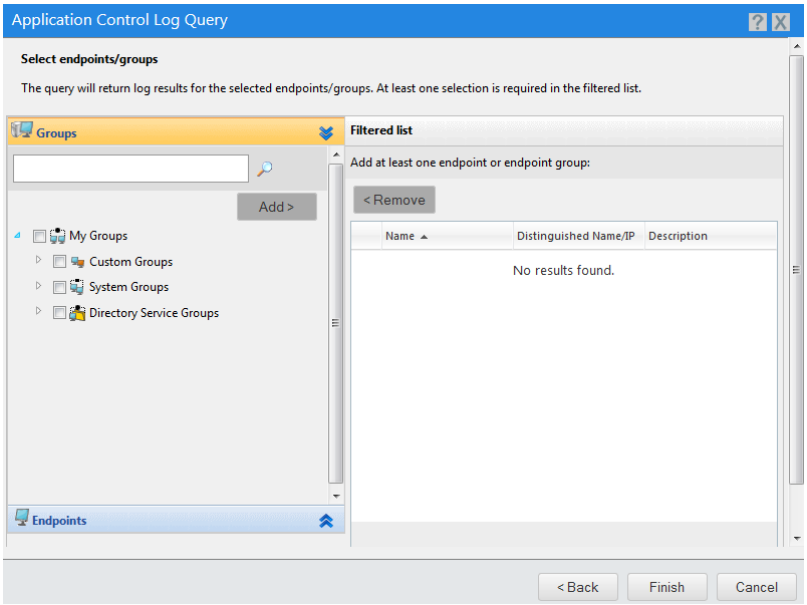


Figure 113: The Select Endpoints/Groups Page

12. [Optional] Change the list of targets (groups or endpoints) for the query, using any of the following methods:

Method	Steps
To add groups of endpoints:	1. Select a group or groups from the **Groups** list. 2. Click **Add >**.
To add individual endpoints:	1. Select an endpoint or endpoints from the **Endpoints** list. 2. Click **Add >**.
To remove groups of endpoints:	1. Select a group or groups from the **Assigned List**. 2. Click **< Remove**.
To remove individual endpoints:	1. Select an endpoint or endpoints from the **Assigned List**. 2. Click **< Remove**.

Note: Use the double-arrows ( ) to switch between groups and endpoints.

Step Result: The selected groups and/or endpoints are displayed in the **Assigned List**.

13. Click **Finish**.

    Step Result: The wizard closes and you return to the ***Application Control Log Queries*** page.

Result: The application control log query has been edited.

Copying a Scheduled Ivanti Application Control Log Query

You can create and run a new Application Control Log Query based on a Scheduled query.

Prerequisites:

You must be assigned the **Manage Application Control Event Logs** access right.

1. Select **Review** > **Application Control Log Queries**.
2. Click the **Scheduled** tab.

   Step Result: A list of scheduled queries is displayed.
3. If necessary, sort the list to find the query you want to copy.
4. Select the check box beside the query name. You can copy only one query at a time.
5. Click **Copy**.

   Step Result: The ***Create application control log query*** wizard opens, displaying the details of the selected query. All the settings are the same as the original query, except "Copy of" is added to the **Query name** and the **Start date** is reset (for Scheduling of type Once, Daily, and Weekly).
6. Complete the wizard to modify the query settings as required.

   Tip: If you need to indicate that this query is based on an exiting one, keep at least part of the original Query Name.

Result: You have created a new Application Control Log Query based on a Scheduled query and executed it. If not run immediately, it will appear under the ***Scheduled*** tab on the Application Control ***Log Quries*** page.

Rerunning a Completed Application Control Log Query

You can create and run a new Application Control Log Query based on a Completed query.

Prerequisites:

You must be assigned the **Manage Application Control Event Logs** access right.

1. Select **Review** > **Application Control Log Queries**.
2. Click the **Completed** tab.

   Step Result: A list of completed queries is displayed.

3. If necessary, sort the list to find the query you want to rerun.
4. Select the check box beside the query name. You can rerun only one query at a time.
5. Click **Run Again**.

   Step Result: The ***Create application control log query*** wizard opens, displaying the details of the selected query. All the settings are the same as the original query, except "Copy of" is added to the **Query name** and the **Start date** is reset (for Scheduling of type Once, Daily, and Weekly).

6. Complete the wizard to modify the query settings as required.

   Tip: If you need to indicate that this query is based on an exiting one, keep at least part of the original Query Name.

Result: You have created a new Application Control Log Query based on a Completed query and executed it. If not run immediately, it will appear under the ***Scheduled*** tab on the Application Control ***Log Quries*** page.

Deleting Application Control Log Queries

You can delete both scheduled and completed application control log queries if they are no longer needed.

If a scheduled application control log query has executed, it will have one or more entries in the list of completed log queries. Deleting the scheduled query does not delete the associated completed queries. You can delete both scheduled and completed log queries independently of each other.

You can delete a scheduled log query if you do not want it to run any more.

You can delete completed log queries if you have gained sufficient information from them and they are no longer needed.

Deleting a Scheduled Application Control Log Query

You can delete a scheduled application control log query if it is no longer needed, even if it has never run.

Deleting a scheduled application control log query does not delete any completed event log queries that it had created.

1. Select **Review** > **Application Control Log Queries**.

2. Click the **Scheduled** tab.

   Step Result: The **Application Control Log Queries** page displays a list of scheduled log queries.

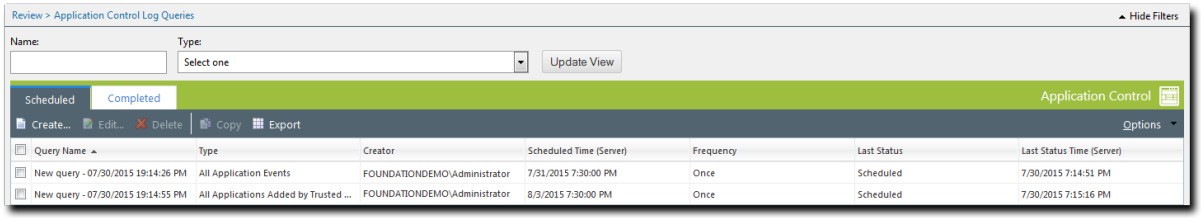


Figure 114: Application Control Log Queries - Scheduled Tab

3. Select the check box(es) next to any query you want to delete.
4. Click **Delete**.

   Step Result: A ***Delete Queries*** confirmation dialog opens.

5. Click **OK**.

Result: One or more scheduled application control log queries are deleted.

Deleting a Completed Application Control Log Query

You can delete completed application control log queries if they are no longer needed.

1. Select **Review** > **Application Control Log Queries**.

   Step Result: The **Application Control Log Queries** page opens to the ***Completed*** tab.

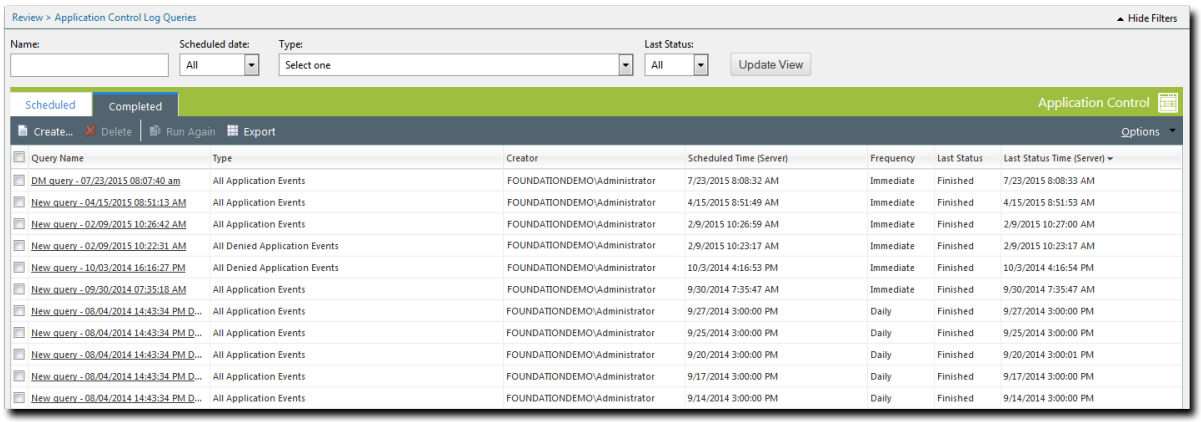


Figure 115: Application Control Log Queries - Completed Tab

2. Select the check box(es) next to any query you want to delete.

3. Click **Delete**.

   Step Result: A ***Delete Queries*** confirmation dialog opens.

4. Click **OK**.

Result: One or more completed application control log queries are deleted.

Authorizing, Denying, and Trusting Files from Logs

You can authorize, deny, or trust files directly from Application Control Log Queries. This is a convenient way to manage files added after an application scan.

You may need to authorize files added to an endpoint after an application scan (Easy Lockdown, for example). One method is to rescan the endpoint to add the new files to the whitelist. But this takes time, impacts endpoint performance, and can result in unwanted files being whitelisted.

It is more convenient to review a log query (for example, All Denied Application Events), identify the required files, and authorize them directly from the log. This adds the files to a Supplementary Easy Lockdown Policy. Similarly, you can add installer files to a Trusted Updater policy directly from the logs.

You may also need to deny files authorized after Easy Lockdown by an end user with Local Authorization privileges. You can review an All Applications Executed By Local Authorization report, select the unwanted files, and add them to a Denied Applications policy.

Note: If you are unsure what to do with a file, you can add it to Application Library first and then decide later what type of policy to apply to it. See Adding Files to Application Library on page 300 for more information.

Most Application Control Log Query types return a list of files and display the **Authorize**, **Deny**, and **Trust** buttons which are enabled when one or more files are selected.

The All Memory Injection Detection Events and the All Updaters Added by Trusted Updaters queries do not display these buttons as their actions are not applicable to the files listed.

Authorizing Files from Logs

You can authorize files directly from an Application Control Log Query.

Prerequisites:

You have run a log query (for example, All Denied Application Events) and determined that one or more of the files that have been blocked should be authorized to run.

1. Select **Review** > **Application Control Log Queries**.

   Step Result: The ***Application Control Log Queries*** page opens displaying a list of completed queries.

2. In the **Query Name** column, click the name of the log query.

   Step Result: The ***Query Results*** page opens, displaying the detailed results of the query.

3. Select the file(s) that you want to authorize.

   Step Result: The **Authorize** button is enabled.

   > **Note:** The All Memory Injection Detection Events and the All Updaters Added by Trusted Updaters queries do not display this button.

4. Click **Authorize**.

   Step Result: The ***Authorize Selected Files*** dialog opens.

5. Authorize the selected file(s) using one of the following methods:

Method	Steps
New policy	1. Click the **Create a new Supplemental Easy Lockdown/ Auditor Policy** option. **Note:** This option is selected by default. 2. Click **OK**. The ***Authorize Selected Files*** dialog changes to the first screen of the ***Supplemental Easy Lockdown/ Auditor*** wizard. See Creating a Supplemental Easy Lockdown/ Auditor Policy on page 124 to complete the procedure. When you click **Finish** the wizard closes and a ***Policy Created*** confirmation dialog is displayed. 3. Click **Close**.
Existing policy	1. Click the **Add to one or more existing policies** option. 2. Select one or more of the existing policies. **Note:** You can click **View details** to review the policies first, paying particular attention to the users or endpoints that are affected. 3. Click **OK**. The ***Authorize Selected Files*** dialog closes and a ***Policies Updated*** confirmation dialog is displayed. 4. Click **Close**.

   Step Result: The selected file(s) are added to one or more Supplemental Easy Lockdown/Auditor policies.

Result: One or more files listed in an Application Control Log Query have been authorized to run.

Denying Files from Logs

You can deny files directly from an Application Control Log Query.

Prerequisites:

You have run a log query (for example, All Applications Executed By Local Authorization) and determined that one or more of the files that have been authorized should be denied.

1. Select **Review** > **Application Control Log Queries**.

   Step Result: The ***Application Control Log Queries*** page opens displaying a list of completed queries.

2. In the **Query Name** column, click the name of the log query you want to view.

   Step Result: The ***Query Results*** page opens, displaying the detailed results of the query.

3. Select the file(s) that you want to deny.

   Step Result: The **Deny** button is enabled.

   Note: The All Memory Injection Detection Events and the All Updaters Added by Trusted Updaters queries do not display this button.

4. Click **Deny**.

   Step Result: The ***Deny Selected Files*** dialog opens.

5. Deny the selected file(s) using one of the following methods.

Method	Steps
New policy	1. Click the **Create a new Denied Application Policy** option. **Note:** This option is selected by default. 2. Click **OK**. The ***Deny Selected Files*** dialog changes to the first screen of the ***Denied Application Policy*** wizard. See Creating a Denied Applications Policy on page 108 to complete the procedure. When you click **Finish** the wizard closes and a ***Policy Created*** confirmation dialog is displayed. 3. Click **Close**.

Method	Steps
Existing policy	1. Click the **Add to one or more existing policies** option. 2. Select one or more of the existing policies. **Note:** You can click **View details** to review the policies first, paying particular attention to the users or endpoints that are affected. 3. Click **OK**. The ***Deny Selected Files*** dialog closes and a ***Policies Updated*** confirmation dialog is displayed. 4. Click **Close**.

Step Result: The selected file(s) are added to one or more Denied Applications policies.

Result: One or more files listed in an Application Control Log Query have been denied from running.

Trusting Files from Logs

You can trust installer files directly from an Application Control Log Query.

Prerequisites:

You have run a log query (for example, All Denied Application Events) and determined that one or more installer files need to be treated as a Trusted Updater.

1. Select **Review** > **Application Control Log Queries**.

   Step Result: The ***Application Control Log Queries*** page opens displaying a list of completed queries.

2. In the **Query Name** column, click the name of the log query you want to view.

   Step Result: The ***Query Results*** page opens, displaying the detailed results of the query.

3. Select the installer file(s) that you want to trust.

   Step Result: The **Trust** button is enabled.

   Note: The All Memory Injection Detection Events and the All Updaters Added by Trusted Updaters queries do not display this button.

4. Click **Trust**.

   Step Result: The ***Trust Selected Files*** dialog opens.

5. Trust the selected file(s) using one of the following methods.

Method	Steps
New policy	1. Click the **Create a new Trusted Updater/Installer policy** option. **Note:** This option is selected by default. 2. Click **OK**. The ***Trust Selected Files*** dialog changes to the first screen of the ***Trusted Updater*** wizard. See Creating a Trusted Updater Policy on page 147 to complete the procedure. When you click **Finish** the wizard closes and a ***Policy Created*** confirmation dialog is displayed. 3. Click **Close**.
Existing policy	1. Click the **Add to one or more existing policies** option. 2. Select one or more of the existing policies. **Note:** You can click **View details** to review the policies first, paying particular attention to the users or endpoints that are affected. 3. Click **OK**. The ***Trust Selected Files*** dialog closes and a ***Policies Updated*** confirmation dialog is displayed. 4. Click **Close**.

Step Result: The selected file(s) are added to one or more Trusted Updater policies.

Result: One or more installer files listed in an Application Control Log Query are able to run as Trusted Updaters.

Viewing Policy Details

The ***View Policy Details*** dialog shows detailed information on the relevant Application Control policy.

This dialog is displayed when you click the **View details** link for an existing Supplemental Easy Lockdown/Auditor Policy, Denied Applications Policy, or Trusted Updater Policy (the policy types that can be assigned directly from an Application Control log query).

Table 54: View Policy Details Dialog Items

Item	Description
Policy name	The name of the policy.

Item	Description
Type	One of the following policy types: • Supplemental Easy Lockdown/Auditor Policy • Denied Applications Policy • Trusted Updater Policy
Logging	On or Off (not applicable to Trusted Updaters)
List	• Authorized applications/files • Denied applications/files • Trusted updaters
Assigned list	The policy can be assigned to the following: • Endpoints • Groups • Users (not applicable to Trusted Updaters) • Blank (a policy that is not assigned to an endpoint/group or a user will be disabled)

Adding Files to Application Library

You can add files to the Application Library directly from Application Control Log Queries.

You may want to add files to Application Library after Easy Lockdown has been applied. One method is to scan an endpoint with the required files, but this can be time consuming. It is more convenient to add the files from an Application Control Log Query. For example, you could:

- Use an All Denied Application Events log query to identify files that have been blocked from running.
- Use an All Applications Executed By Local Authorization log query to find non-whitelisted files that have been running on selected endpoints.

These files can be easily added to Application Library from the query pages. You can then group them into applications and application groups and assign appropriate Application Control policies to them.

Note: If you want to immediately authorize, deny, or trust a file, this can also be done from Application Control Log Queries. See Authorizing, Denying, and Trusting Files from Logs on page 295 for more information.

Most Application Control Log Query types return a list of files and display the **Add to Application Library** button which is enabled when one or more files are selected.

The All Memory Injection Detection Events and the All Updaters Added by Trusted Updaters queries do not display this button as its action is not applicable to the files listed.

Adding Files to Application Library

You can add files to Application Library directly from an Application Control Log Query.

Prerequisites:

You have run an Application Control Log Query and determined that one or more files should be added to Application Library.

1. Select **Review** > **Application Control Log Queries**.

   Step Result: The ***Application Control Log Queries*** page opens displaying a list of completed queries.

2. In the **Query Name** column, click the name of the log query you want to view.

   Step Result: The ***Query Results*** page opens, displaying the detailed results of the query.

3. Select the file(s) that you want to add to Application Library.

   Step Result: The **Add to Application Library** button is enabled.

4. Click **Add to Application Library**.

   Step Result: An ***Add to Application Library*** confirmation dialog opens.

5. Complete the task according to the dialog displayed.

Confirmation Dialog	Action
Your files have been added to the Application Library	Do one of the following: • Click **Close**. • Click **Application Library**. Going directly to the Application Library, you can organize the files into applications or application groups, and you can apply specific policies to them.
This file already exists in the Application Library	Click **Close**. As the file is already in the library, there is no need to add it.
These files already exist in the Application Library	Click **Close**. As the files are already in the library, there is no need to add them.
[Number] of the selected files already exist in the Application Library	Do one of the following: • Click **Add the other [number] files**. • Click **Don't add**.

Result: One or more files listed in an Application Control Log Query have been added to Application Library.

Exporting the Result of an Application Control Log Query

You can export the result of an application control log query to a `csv` (Comma Separated Value) file.

To export data, refer to Exporting Data on page 43.

Chapter 10

Managing Individual Users

In this chapter:

Some Ivanti Endpoint Security (Ivanti Endpoint Security) modules have policy types that need assignment to specific users (or user groups) as well as to endpoints. These are called *user-based policies*, and users with such policies associated with them are called *individual users*.

Ivanti Application Control has the following user-based policies:

- Denied Applications
- Supplemental Easy Lockdown/Auditor
- Trusted Path
- Local Authorization

Before these policies can be assigned to individual users, the users must be added to Ivanti Endpoint Security by synchronizing the server with your network's Active Directory. For more information about synchronizing with Active Directory, see The Directory Sync Schedule Page on page 304.

After synchronization, you can apply Application Control user-based policies to individual users or to organizational units (collections of individual users). For more information, see The Users Page on page 314.

The Directory Sync Schedule Page

Ivanti Endpoint Security can incorporate your Active Directory users and group into product functions. To use this functionality, you must synchronize you server with Active Directory, which you can do from the ***Directory Sync Schedule*** page.

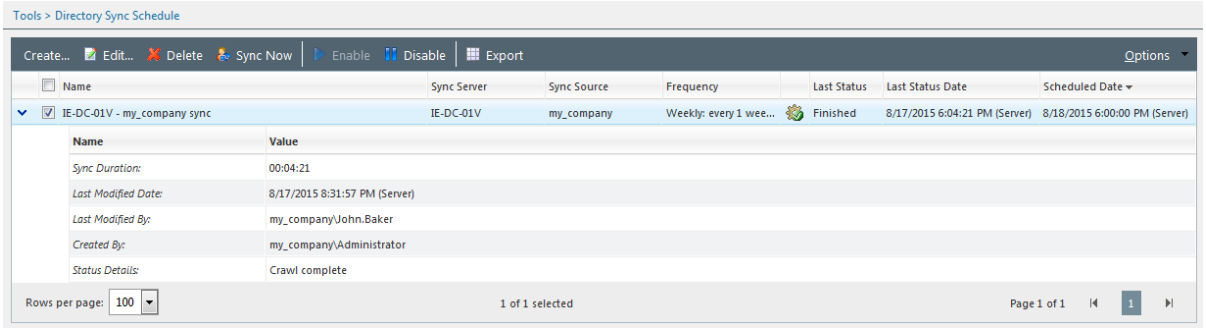


Figure 116: Directory Sync Schedule Page

To open the ***Directory Sync Schedule*** page:

1. From the **Navigation Menu**, select **Tools** > **Directory Sync Schedule**

Synchronizing your server with your Active Directory (AD) compiles a list of network domains, users, and user groups that you can use in the Web console. You can then use these AD objects with product features without accessing the active directory itself.

Note:

- To enable active directory synchronization, open port TCP port 389 on your Ivanti Endpoint Security server and your domain controller, and then complete an active directory synchronization.
- Directory Syncs do not modify Active Directory itself. Your server simply requests information from AD.

About Active Directory Synchronization

You can synchronize Ivanti Endpoint Security with your network Active Directories. Objects found in your Active Directory can then be used to execute module features.

Active Directory synchronizations with your server are scheduled by *Directory Syncs*, which are scans that query your Active Directory for:

- Users
- Computers
- Groups
- Contact Data
- Organizational Units
- Other Information

These objects can then be used by Ivanti Endpoint Security for executing different module features, including:

- Mobile Device Management: Registration Invitations
- Application Control: Assigning Policies
- Device Control: Assigning Policies

Directory Syncs are created from the ***Directory Sync Schedule*** page. When creating a Directory Sync, you define the AD you want to sync, as well as the sync schedule. Sync can be scheduled by each of the following units at a specific time:

- Day
- Week
- Month

You can also launch syncs immediately at any time.

After the sync completes, its results appear in the ***Directory Sync Schedule*** page list. To view sync results, expand it by clicking its **rotating chevron** (**>**).

Viewing the Directory Sync Schedule Page

Navigate to the ***Directory Sync Schedule*** page to view directory syncs and their details.

View the ***Directory Sync Schedule*** page by using the navigation menu.

1. From the **Navigation Menu**, select **Tools** > **Directory Sync Schedule**.
2. [Optional] Define the desired filter criteria.
3. [Optional] Perform a task listed in Working with Active Directory Synchronizations on page 307.

The Directory Sync Schedule Page Toolbar

The page toolbar features buttons you can use to create or edit directory syncs.

The following table describes each toolbar button.

Table 55: Directory Sync Page Toolbar

Button	Description
Create...	Opens the ***Schedule Directory Sync*** dialog to create a new AD sync. For additional information, refer to Creating Directory Syncs on page 307.
Edit	Opens the ***Edit Directory Sync*** dialog to edit an existing AD sync. For additional information, refer to Editing Directory Syncs on page 310.
Delete	Deletes the selected directory sync(s). For additional information, refer to Deleting Directory Syncs on page 312.
Sync Now	Launches an immediate directory sync. For additional information, refer to Syncing Directories Immediately on page 312.

Button	Description
Enable	Enables the selected disabled directory sync(s). For additional information, refer to Enabling Disabled Directory Syncs on page 313.
Disable	Disables the selected enabled directory sync(s). For additional information, refer to Disabling Directory Syncs on page 313.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 43. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options	Opens the **Options** menu. For additional information refer to The Options Menu on page 35.

The Directory Sync Schedule Page List

After creating Directory Syncs, you can view information about their configurations and results.

The following table describes each list column.

Table 56: Directory Sync Schedule Page List

Column	Description
Name	The name of the Directory Sync.
Sync Server	The name of the server that hosts the AD with which you server is synchronizing.
Sync Source	The name of the AD domain or AD containers defined for synchronization with you server.
Frequency	The interval between Directory Syncs.
Icon	The icon that indicates the current status of the Directory Sync.
Last Status	The last status of the Directory Sync.
Last Status Date	The date a time the last time the Directory Sync was scheduled or performed an action.
Scheduled Date	The date and time the Directory Sync is next schedule to synchronize.

Each Directory Sync in the page list can be expanded to show more information. Click the **rotating chevron** (**>**) for a Sync to display this information. The following table describes the information displayed for an expanded Directory Sync.

Table 57: Expanded Directory Sync

Name	Value
Sync Duration	The duration of the last run sync.
Last Modified Date	The date and time the Directory Sync was last edited.
Last Modified By	The user that last modified the Directory Sync (`DOMAIN\Username`).
Created By	The user that created the Domain Sync (`DOMAIN\Username`).
Status Details	Any additional information about the Directory Sync.

Working with Active Directory Synchronizations

You can perform several tasks associated with Active Directory synchronizations.

You can perform the following tasks:

- Creating Directory Syncs on page 307
- Editing Directory Syncs on page 310
- Deleting Directory Syncs on page 312
- Syncing Directories Immediately on page 312
- Disabling Directory Syncs on page 313
- Enabling Disabled Directory Syncs on page 313
- Exporting Directory Sync Information on page 313

Creating Directory Syncs

Use directory syncs to synchronize your active directory (AD) with Ivanti Endpoint Security.

Create directory syncs from the ***Directory Sync Schedule*** page.

Attention: To successfully complete a directory sync, port 389 must be open on:

- The Ivanti Endpoint Security Server
- The network domain controller

1. From the **Navigation Menu**, select **Tools** > **Directory Sync Schedule**.
2. Click **Create**.

   Step Result: The ***Schedule Directory Sync*** dialog opens.
3. Type the domain controller name in the **Directory server/computer** field.

4. Type the domain name in the **Domain name** field.

Note: If you select the **Specify one or more directory containers as sync sources** options, defining this field is unnecessary.

5. In the **Domain\user name** field, type a user name that authenticates with the domain controller in the following format: `DOMAIN\username`
6. Type the password associated with the user in the **Password** field.
7. In the **Confirm password**, retype the password.
8. Select the appropriate **Sync scope** option.

   These options define whether the directory sync synchronizes with entire directory or individual containers within the directory.

Tip: Select the **Specify one or more directory containers as sync sources** options for one of the following reasons:

- The AD is large, causing long synchronization times.
- Portions of the directory are geographically dispersed and thus require a sync at different starting and ending times.
- Portions of the directory may be updated more frequently than others and thus require a sync at different intervals.
- The credentials defined in the **Domain\user name** field cannot access the entire domain.

Option	Step
To sync the entire domain:	1. Select the **Sync the entire domain (recommended)** option. 2. Click **Next**.
To specify one or more directory containers as sync sources:	1. Select the **Specify one or more directory containers as sync sources** option. 2. Click **Next**. 3. In the field, type the fully-qualified domain name of the directory containers you want to sync (for example, `OU=Sub-Organization Unit,OU=Organization Unit,DC=Domain Controller`). 4. Click **Add Directory Path**. 5. Specify additional directory containers by repeating the previous two steps. 6. Review the **Directory Path** list. Click the applicable **Delete** icon to remove directory paths you do not want to add. 7. Click **Next**.

Step Result: The ***Schedule Sync*** page opens.

9. Schedule the sync.

Option	Step
To schedule a daily sync:	**1.** Select the **Daily** option. **2.** Type the desired **Start date** in a `mm/dd/yyyy` format. **3.** Type the desired **Start time** in a `hh:mm` format. You may use 12-hour or 24-hour formatting. **4.** In the **Run every *x* days** field, type how often you want your sync to run. **5.** Schedule an **End by** date. To schedule an **End by** date, select the check box and type an end date in a `mm/dd/yyyy` format.
To schedule a weekly sync:	**1.** Select the **Weekly** option. **2.** Type the desired **Start date** in a `mm/dd/yyyy` format. **3.** Type the desired **Start time** in a `hh:mm` format. You may use 12-hour or 24-hour formatting. **4.** In the **Run every *x* weeks on** field, type the desired increment. **5.** Select the check boxes associated with the days you want the sync to run. **6.** Schedule an **End by** date. To schedule an **End by** date, select the check box and type an end date in a `mm/dd/yyyy` format.
To schedule a monthly sync:	**1.** Select the **Monthly** option. **2.** Type the desired **Start date** in a `mm/dd/yyyy` format. **3.** Type the desired **Start time** in a `hh:mm` format. You may use 12-hour or 24-hour formatting. **4.** Select an option: **a.** To schedule the sync for a specific date, select the **Run on the *x* day every *x* months** option. Then define the **day** and **months** fields. **b.** To schedule the sync for a relative day, selec the **Run on the *x x*** every *x* month. Then define the drop-down lists and the **months** field. **5.** Schedule an **End by** date. To schedule an **End by** date, select the check box and type an end date in a `mm/dd/yyyy` format.

Note: Rather than typing a specific date or time when scheduling the sync, you may select them from a menu. Click the **Calendar** and **Clock** icons to open these menus.

10. Click **Finish**.

Result: The ***Schedule Directory Sync*** dialog closes and the sync is scheduled. An item for the sync displays in the ***Schedule Directory Sync*** page list.

> **Tip:** After you create the sync, select it from the ***Schedule Directory Sync*** page and click **Sync Now** to run it immediately.

Editing Directory Syncs

After creating a directory sync, you can edit its synchronization schedule and its synchronization target.

Edit directory syncs from the ***Directory Sync Schedule*** page.

1. From the **Navigation Menu**, select **Tools** > **Directory Sync Schedule**.
2. Select the check box associated with the directory sync you want to edit.
3. Click **Edit**.

   Step Result: The ***Schedule Directory Sync*** dialog opens.
4. [Optional] Edit the **Directory server/computer** field.
5. [Optional] Edit the **Domain name** field.
6. [Optional] Edit the **Domain\user name** field.
   a) Edit the **Password** field to the password associated with the new user name.
   b) Retype the password in the **Confirm password** field.
7. [Optional] Edit the **Sync scope** option.

   Follow the applicable substeps to edit the sync scope.

Option	Step
To sync the entire domain:	1. Select the **Sync the entire domain (recommended)** option. 2. Click **Next**.

Option	Step
To specify one or more directory containers as sync sources:	1. Select the **Specify one or more directory containers as sync sources** option. 2. Click **Next**. 3. In the field, type the fully-qualified domain name of the directory containers you want to sync (for example, `OU=Sub-Organization Unit,OU=Organization Unit,DC=Domain Controller`). 4. Click **Add Directory Path**. 5. Specify additional directory containers by repeating the previous two steps. 6. Review the **Directory Path** list. Click the applicable **Delete** icon to remove directory paths you do not want to add. 7. Click **Next**.

8. Schedule the sync.

Option	Step
To schedule a daily sync:	1. Select the **Daily** option. 2. Type the desired **Start date** in a `mm/dd/yyyy` format. 3. Type the desired **Start time** in a `hh:mm` format. You may use 12-hour or 24-hour formatting. 4. In the **Run every *x* days** field, type how often you want your sync to run. 5. Schedule an **End by** date. To schedule an **End by** date, select the check box and type an end date in a `mm/dd/yyyy` format.
To schedule a weekly sync:	1. Select the **Weekly** option. 2. Type the desired **Start date** in a `mm/dd/yyyy` format. 3. Type the desired **Start time** in a `hh:mm` format. You may use 12-hour or 24-hour formatting. 4. In the **Run every *x* weeks on** field, type the desired increment. 5. Select the check boxes associated with the days you want the sync to run. 6. Schedule an **End by** date. To schedule an **End by** date, select the check box and type an end date in a `mm/dd/yyyy` format.

Option	Step
To schedule a monthly sync:	**1.** Select the **Monthly** option. **2.** Type the desired **Start date** in a `mm/dd/yyyy` format. **3.** Type the desired **Start time** in a `hh:mm` format. You may use 12-hour or 24-hour formatting. **4.** Select an option: **a.** To schedule the sync for a specific date, select the **Run on the *x* day every *x* months** option. Then define the **day** and **months** fields. **b.** To schedule the sync for a relative day, selec the **Run on the *x x*** every *x* month. Then define the drop-down lists and the **months** field. **5.** Schedule an **End by** date. To schedule an **End by** date, select the check box and type an end date in a `mm/dd/yyyy` format.

Note: Rather than typing a specific date or time when scheduling the sync, you may select them from a menu. Click the **Calendar** and **Clock** icons to open these menus.

9. Click **Finish**.

Result: The ***Schedule Directory Sync*** dialog closes and the changes are saved. The associated list item for the sync changes according to your edits, and the sync runs against the applicable AD at the new schedule time.

Deleting Directory Syncs

Delete Directory Syncs when they are no longer needed.

Delete syncs from the ***Directory Sync Schedule*** page.

1. From the **Navigation Menu**, select **Tools** > **Directory Sync Schedule**.

2. Ensure the page is filtered to display disabled syncs.

3. Select the Directory Syncs you want to delete.

4. Click **Delete**.

Result: The Directory Syncs are deleted.

Syncing Directories Immediately

After creating a directory sync, you can trigger it to synchronize with its targeted Active Directory at any time, regardless of its schedule.

Run immediate directory syncs from the ***Directory Sync Schedule*** page.

1. From the **Navigation Menu**, select **Tools** > **Directory Sync Schedule**.

2. Select the Directory Syncs you want to run immediately.

Note: You can only run immediate directory syncs for enabled syncs. For additional information refer to Enabling Disabled Directory Syncs on page 313.

3. Click **Sync Now**.

Result: The selected syncs run immediately.

Disabling Directory Syncs

Rather than deleting a directory sync, you can temporarily disable it when unnecessary. Disabling unnecessary directory syncs can improve network bandwidth at the applicable syncs scheduled time.

Disable directory syncs from the ***Directory Sync Schedule*** page.

1. From the **Navigation Menu**, select **Tools** > **Directory Sync Schedule**.
2. Select the Directory Sync you want to disable.

Tip: In some instances, you may need to filter the page to display to show enabled syncs.

3. Click **Disable**.

Result: The selected Directory Sync are disabled and will not run at its scheduled date and times. Synchronization will not occur until the sync is re-enabled.

Enabling Disabled Directory Syncs

After disabling a directory sync, you may re-enable it at any time.

Re-enable directory syncs from the ***Directory Sync Schedule*** page.

1. From the **Navigation Menu**, select **Tools** > **Directory Sync Schedule**.
2. Ensure the page is filtered to display disabled Directory Syncs.
3. Select the Directory Syncs you want to re-enable.
4. Click **Enable**.

Result: The selected directory syncs are re-enabled. Synchronization occurs at the next scheduled time.

Exporting Directory Sync Information

To export the directory sync information listed on ***Schedule Sync Schedule*** page to a comma separated value (`.csv`) file, click the **Export** button. Exporting data lets you work with that data in other programs for reporting and analytical purposes.

For additional information refer to Exporting Data on page 43.

The Users Page

This page lists users discovered during active directory synchronization jobs (directory syncs). Use this page to view or create individual users, which you can manage using Ivanti Endpoint Security features.

This page features a directory tree, which lists users and user groups discovered during directory syncs. You can select items in this tree. After selecting an item, information about that item displays on the page.

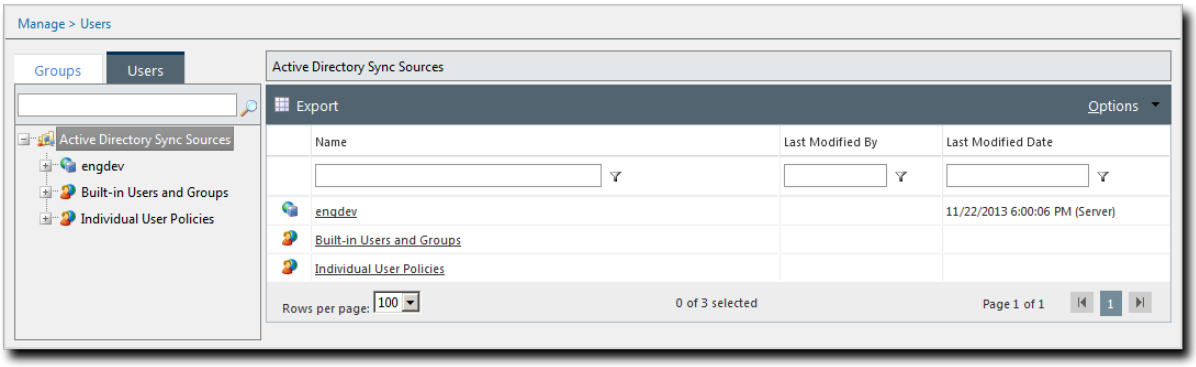


Figure 117: Users Page

The **Users** page contains a breadcrumb that indicates your position in the user browser directory tree. Click links in the breadcrumb to move closer to the directory tree root level.

The User Browser Directory Tree

Use the **User Browser**, a **Users** page pane, to select users found during directory syncs. The number of users in the tree depends on the number of users detected during syncs.

Click an **Expand** icon (+) to view active directory sync sources, built-in users and groups, or individual user policies. By expanding the tree, information for selected items becomes more detailed.

To display detailed user information, select a user or group name. After selecting a user or group name from **Built-in Users and Groups** or **Individual User Policies**, use the **View** list to access different

views. After selecting a **Built-in Users and Groups** or **Individual User Policies** item, you can select from the following view:

- ***Information***
- ***Application Control Policies***
- ***Device Control Policies***

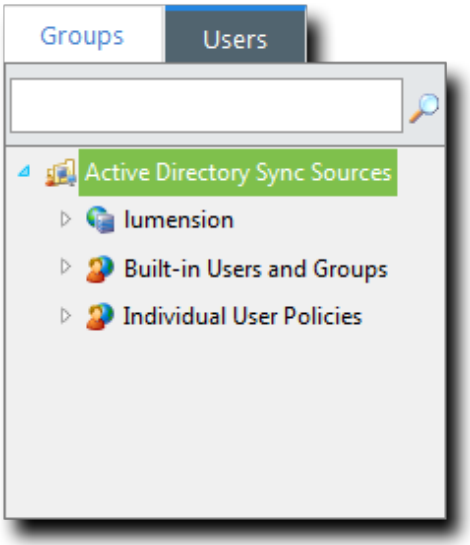


Figure 118: User Browser Directory Tree

Tip: Click the ***Groups*** tab to open the ***Groups*** page.

The Users Page Toolbar

This toolbar contains buttons related to assignment of policies to individual users. The buttons that display change based on the item selected from the **User Browser** directory tree.

The following topics describe the toolbar buttons that display based on the **User Browser** directory tree item selected:

- The Users Page Toolbar (Active Directory Sync Sources) on page 316
- The Users Page Toolbar (Built-in Users and Groups) on page 316
- The Users Page Toolbar (Built-in Users and Groups Items) on page 317
- The Users Page Toolbar (Individual User Policies) on page 318
- The Users Page Toolbar (Individual User Policies Items) on page 319

The Users Page Toolbar (Active Directory Sync Sources)
This toolbar contains buttons related to data exportation.

The following table describes the buttons available when **Active Directory Sync Sources** is selected from the **User Browser** directory tree.

Table 58: Users Page Toolbar Buttons (Active Directory Sync Sources)

Button	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 43. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu.

Note: The ***Users*** page toolbar only appears when the **Application Control Policies** or the ***Device Control Policies*** view is selected.

The Users Page Toolbar (Built-in Users and Groups)
This toolbar contains buttons related to data exportation.

The following table describes the buttons available when **Built-in Users and Groups** is selected from the **User Browser** directory tree.

Table 59: Users Page Toolbar Buttons (Built-in Users and Groups)

Button	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 43. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu.

Note: The ***Users*** page toolbar only appears when the **Application Control Policies** or the ***Device Control Policies*** view is selected.

The Users Page Toolbar (Built-in Users and Groups Items)
This toolbar contains buttons related to data exportation.

The following table describes the buttons available when an item is selected from the **Built-in Users and Groups** subitems in the **User Browser** directory tree and the ***Application Control Policies*** view is selected (Application Control only).

Table 60: Users Page Toolbar Buttons (Built-in Users and Groups Items)

Button	Description
Unassign	Unassigns the selected policy (or policies) from the selected user(s). For additional information, refer to Unassigning Policies from Users on page 328.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 43. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu.

The following table describes the buttons available when an item is selected from the **Built-in Users and Groups** subitems in the **User Browser** directory tree and the ***Device Control Policies*** view is selected (Device Control only).

Table 61: Users Page Toolbar Buttons (Built-in Users and Groups Items)

Button	Description
Create...	Opens the **Create** menu.
Device Class Policy (**Create...** Menu Item)	Opens the ***Device Class Policy Wizard***. Use this wizard to create a device class policy. When you complete the wizard, the policy is assigned to selected user or group.
Device Collection Policy (**Create...** Menu Item)	Opens the ***Device Collection Policy Wizard***. Use this wizard to create a device collection policy. When you complete the wizard, the policy is assigned to selected user or group
Media Collection Policy (**Create...** Menu Item)	Opens the ***Media Collection Policy Wizard***. Use this wizard to create a media collection class policy. When you complete the wizard, the policy is assigned to selected user or group

Button	Description
Port Collection Policy (**Create...** Menu Item)	Opens the ***Port Collection Wizard***. Use this wizard to create a port collection policy. When you complete the wizard, the policy is assigned to selected user or group
Assign...	Opens the ***Assign Policy*** dialog. Use this dialog to assign an existing policy to the user or group.
Unassign	Unassigns any policies assigned to the selected user or group.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 43. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu.

Note: The ***Users*** page toolbar only appears when the **Application Control Policies** or the ***Device Control Policies*** view is selected.

The Users Page Toolbar (Individual User Policies)
This toolbar contains buttons related to individual user management and data exportation.

The following table describes the toolbar buttons that are available when ***Individual User Policies*** is selected from the **User Browser** directory tree.

Table 62: Users Page Toolbar Buttons (Individual User Policies)

Button	Description
Add	Adds a user to **Individual User Policies**. For additional information on adding users to **Individual User Policies**, refer to Adding an Individual User to a Policy on page 115.
Remove	Removes a user from **Individual User Policies**. For additional information on removing users from **Individual User Policies**, refer to Removing an Individual User from the User Browser on page 327.

Button	Description
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 43. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu.

Note: The ***Users*** page toolbar only appears when the **Application Control Policies** or the ***Device Control Policies*** view is selected.

The Users Page Toolbar (Individual User Policies Items)
This toolbar contains buttons related to data exportation.

The following table describes the buttons available when an item is selected from the **Individual User Policies** subitems in the **User Browser** directory tree.

Table 63: Users Page Toolbar Buttons (Individual User Policies Items)

Button	Description
Unassign	Unassigns the selected policy (or policies) from the selected user(s). For additional information, refer to Unassigning Policies from Users on page 328.
Export	Exports the page data to a comma-separated value (`.csv`) file. For additional information, refer to Exporting Data on page 43. **Important:** The Enhanced Security Configuration feature for Internet Explorer suppresses export functionality and must be disabled to export data successfully. Pop-up blockers in Internet Explorer or other supported browsers may also suppress export functionality and should be disabled.
Options (menu)	Opens the **Options** menu.

Note: The ***Users*** page toolbar only appears when the **Application Control Policies** or the ***Device Control Policies*** view is selected.

The Users Page List

On the main portion of the **Users** page, information about the item selected from the **User Browser** directory tree is displayed. This main portion is called the **Users** page list.

Information displayed in the list changes depending on the item selected from the **User Browser**.

The following topics describe the information that displays when you select a **User Browser** directory tree item:

- The Users Page List (Active Directory Sync Sources) on page 320
- The Users Page List (Built-in Users and Groups) on page 320
- The Users Page List (Built-in Users and Groups Items) on page 321
- The Users Page List (Individual User Policies) on page 323
- The Users Page List (Individual User Policies Items) on page 324

The Users Page List (Active Directory Sync Sources)

When **Active Directory Sync Sources** is selected from the ***Users*** page **User Browser** directory tree, information about built-in users and groups and individual user policies is displayed.

The following table describes each column that displays when **Active Directory Sync Sources** is selected.

Table 64: Users Page List (Active Directory Sync Sources)

Column	Description
Name	The name of an active directory sync source. Clicking a **Name** link selects the applicable group within the **User Browser** directory tree.
Last Modified By	The Ivanti Endpoint Security user that last modified an item within the applicable sync source.
Last Modified Date	The date that the sync source was last modified.

The Users Page List (Built-in Users and Groups)

When **Built-in Users and Groups** is selected from the **Users Browser** directory tree, information about standard built-in users and groups found in active directories are displayed.

The following table describes each column that displays when **Built-in Users and Groups** is selected.

Table 65: Users Page List (Built-in Users and Groups)

Column	Description
Name	The name of a user or group built in to active directory.
Last Modified By	The last user that last modified an item within the applicable sync source.
Last Modified Date	The date that the sync source was last modified.

The Users Page List (Built-in Users and Groups Items)
When an item under **Built-in Users and Groups** is selected from the **User Browser** directory tree, information about that built-in user or group is displayed.

There are several views for each **Built-in Users and Groups** item. After you select a **Built-in Users and Groups** item, you can change the data displayed by selecting a different item from the **View** list. You can select from the following views:

- **Information**
- **Application Control Policies** (Application Control only)
- **Device Control Policies** (Device Control only)

The following table describes each field that displays when a **Built-in Users and Groups** item is selected from the **User Browser** and **Information** is selected from the **View** list.

Table 66: Users Page List (Information View)

Field	Description
Name	The name of the built-in user or group.
Distinguished Name	The organizational unit and common name for the select item.
Last Modified Date	The date the user or group was last modified.
Last Modified By	The user that last modified the user or group.
Sync Name	The name of the sync job that detected the user or group.
Frequency	The frequency of the sync job that detected the user or group.
Last Status	The last status of the sync job that detected the user or group.
Last Status Date	The date that the last status was updated.
Started On	The date the sync job that detected the user or group first ran.
Ended On	The date the sync job that detected the user or group is scheduled to run for the last time.

The following table describes each column that displays when a **Built-in Users and Groups** item is selected from the **User Browser** directory tree and **Application Control Policies** is selected from the **View** list.

Table 67: Users Page List (Application Control Policies View)

Column	Description
Action	Contains a **Remove** icon you can user to unassign the policy from the selected user.

Column	Description
Status	Indicates the policy status. Mouse over the icon for a description of the status.
Policy Name	Indicates the policy assigned to the user.
Policy Type	Indicates the policy type (`Denied Applications` , `Supplemental Easy Lockdown/Auditor`, `Trusted Path`, and `Local Authorization`).
Blocking	Indicates the policy blocking value (`N/A`, `Off`, `Non-authorized`).
Logging	Indicates the policy logging value (`Off`, `On`, `Authorized`, `Non-authorized`, `Non-authorized Authorized`)
Source	Indicates the policy source (`Assigned` or `Unassigned`).
Assigned Date	Indicates the date and time the policy was assigned to the selected network user.

Additionally, when the **Application Control Policies** view is selected, you can expand each list item. Expand an item by clicking a rotating chevron. The following table describes each field that displays when you expand a list item.

Table 68: Users Page List Expanded Items (Application Control Policies View)

Field	Description
Created by	The Ivanti Endpoint Security user who created the policy applied to the selected network user.
Created date	The date and time the policy was created.
Last updated by	The Ivanti Endpoint Security user who last modified the applicable policy.
Last updated date	The date and time the policy was last modified.
Trusted Paths	The trusted path(s) applied to the selected network user. **Note:** This field only appears for Trusted Path policies.

The following table describes each column that displays when a **Built-in Users and Groups** item is selected from the **User Browser** directory tree and **Device Control Policies** is selected from the **View** list.

Table 69: Users Page List (Device Control Policies View)

Column	Description
Status	Indicates the policy status. Mouse over the icon for a description of the status.

Column	Description
Policy Name	Indicates the policy assigned to the user.
Policy Type	Indicates the policy type (`Device Class Policy`, `Device Collection Policy`, `Media Collection Policy`, and `Port Control Policy`).
Device Collection	Indicates the device collection the policy applies to.
Source	Indicates the policy source (`Assigned` or `Unassigned`).
Device Class	Indicates the device class the policy applies to.
Last Update	Indicates the date and time the policy was last updated.

Additionally, when the **Device Control Policies** view is selected, you can expand each list item. Expand an item by clicking a rotating chevron. The following table describes each field that displays when you expand a list item.

Table 70: Users Page List Expanded Items (Device Control Policies View)

Field	Description
Name	The name of the individual policy.
Value	The value of the individual policy.
Description	The description of the individual policy.

The Users Page List (Individual User Policies)
When **Individual User Policies** is selected from the **User Browser** directory tree, a list of manually added network users that have policies directly applied to them is displayed.

The following table describes each column that displays when **Individual User Policies** is selected.

Table 71: Users Page List (Individual User Policies)

Column	Description
Name	The name of the user. Click the name to move to that user in the **User Browser** directory tree.
Email	The email address of the user.
Last Modified By	The user that last modified the user within the **User Browser** directory tree.
Last Modified Date	The date that the user was last modified.

The Users Page List (Individual User Policies Items)
When you select an item beneath **Individual User Policies** in the **Users Browser** directory tree, information about that user and its associated policies are displayed.

There are several views for each **Individual User Polices** item. After you select a **Individual User Polices** item, you can change the data displayed by selecting a different item from the **View** list. You can select from the following views:

- **Information**
- **Application Control Policies** (Application Control only)
- **Device Control Policies** (Device Control only)

The following table describes each column that displays when an **Individual User Policies** item is selected from the **User Browser** directory tree and **Information** is selected from the **View** list.

Table 72: Users Page List (Information View)

Field	Description
Name	The name of the individually added user or group.
Distinguished Name	The organizational unit and common name for the select item.
Last Modified Date	The date the user or group was last modified.
Last Modified By	The user that last modified the user or group.
Sync Name	The name of the sync job that detected the user or group.
Frequency	The frequency of the sync job that detected the user or group.
Last Status	The last status of the sync job that detected the user or group.
Last Status Date	The date that the last status was updated.
Started On	The date the sync job that detected the user or group first ran.
Ended On	The date the sync job that detected the user or group is scheduled to run for the last time.

The following table describes each column that displays when an **Individual User Policies** item is selected from the **User Browser** directory tree and **Application Controll Policies** is selected from the **View** list.

Table 73: Users Page List (Application Control Policies View)

Column	Description
Action	Contains a **Remove** icon you can user to unassign the policy from the selected user.

Column	Description
Status	Indicates the policy status. Mouse over the icon for a description of the status.
Policy Name	Indicates the policy assigned to the user.
Policy Type	Indicates the policy type (`Denied Applications` , `Supplemental Easy Lockdown/Auditor`, `Trusted Path`, and `Local Authorization`).
Blocking	Indicates the policy blocking value (`N/A`, `Off`, `Non-authorized`).
Logging	Indicates the policy logging value (`Off`, `On`, `Authorized`, `Non-authorized`, `Non-authorized Authorized`)
Source	Indicates the policy source (`Assigned` or `Unassigned`).
Assigned Date	Indicates the date and time the policy was assigned to the selected network user.

Additionally, when the **Application Control Policies** view is selected, you can expand each list item. Expand an item by clicking a rotating chevron. The following table describes each field that displays when you expand a list item.

Table 74: Users Page List Expanded Items (Application Control Policies View)

Field	Description
Name	The name of the individual policy.
Value	The value of the individual policy.

The following table describes each column that displays when an **Individual User Policies** item is selected from the **User Browser** directory tree and **Device Control Policies** is selected from the **View** list.

Table 75: Users Page List (Device Control Policies View)

Column	Description
Status	Indicates the policy status. Mouse over the icon for a description of the status.
Policy Name	Indicates the policy assigned to the user.
Policy Type	Indicates the policy type (`Device Class Policy`, `Device Collection Policy`, `Media Collection Policy`, `Port Control Policy`)
Device Class	Indicates the device class the policy applies to.
Device Collection	Indicates the device collection the policy applies to.

Column	Description
Source	Indicates the policy source (`Assigned` or `Unassigned`).
Last Update	Indicates the date and time the policy was last updated.

Additionally, when the **Device Control Policies** view is selected, you can expand each list item. Expand an item by clicking a rotating chevron. The following table describes each field that displays when you expand a list item.

Table 76: Users Page List Expanded Items (Device Control Policies View)

Field	Description
Name	The name of the individual policy.
Value	The value of the individual policy.
Description	The description of the individual policy.

Working with Network Users

After directory syncs complete, you can incorporate user data into management of denied application, supplemental easy lockdown/auditory, trusted path, and local authorization policies. Tasks associated with users found during directory syncs are completed from the ***Users*** page.

You can perform the following tasks related to network users:

- Adding an Individual User to a Policy on page 115
- Removing an Individual User from the User Browser on page 327
- Unassigning Policies from Users on page 328
- Exporting User Data on page 328

Adding an Individual User to a Policy

You can add one or more individual users to a policy using the ***Add Individual Users*** dialog.

This dialog is accessed by clicking the **Add Individual User** button on a **User** pane. This feature is available on wizards that support user assignment.

1. Search for users using either of the following methods:

Option	Steps
Search for all users	Leave the **Username** field blank and click **Search**. This returns all existing users in the current domain.

Option	Steps
Search for one or more selected users	1. Type a user name in the **Username** field. **Note:** Sub-string matching is supported, so you do not have to type the full name. Typing a partial name may result in multiple matches 2. Click **Search**.

Step Result: One or more users appear in the results list.

Note: If you cannot find the user(s) you want, try searching other available domains. Select a searchable domain controller from the **Domain** drop-down list.

2. Select one or more users.
3. Click **Add Users**.

   Step Result: The users are added to the selection list.

4. Click **OK**.

   Step Result: The ***Add Individual Users*** dialog closes and you return to the **Users** pane of the policy wizard, with the new user(s) added to the **Users** list.

Removing an Individual User from the User Browser

When you no longer want to apply a policy to an individual user, remove that user from **Individual User Policies** in the **User Browser** directory tree.

Remove individual users from the **User Browser** from the ***Users*** page.

1. Select **Manage** > **Users**.

   Step Result: The ***Users*** page opens.

2. Expand the directory tree to **Individual User Policies**.
3. From the page list, select the individual user(s) you want to remove.
4. Click **Remove**.

   Step Result: A dialog opens, asking if you want to remove the selected user(s).

5. Click **OK**.

Result: The user is removed from **Individual User Policies**.

Unassigning Policies from Users

You can unassign user-based Application Control policies from individual users. You can unassign policies from **Built-in Users and Groups** items and **Individual User Policies** items.

Unassign policies from individual users from the ***Users*** page.

1. Select **Manage** > **Users**.
2. Expand the **User Browser** directory tree to the user you want to remove a policy from.
   Users can be found in the following User Browser directory tree items:
   - **Built-in Users and Groups**
   - **Individual User Policies**
3. Ensure the **Application Control Policies** view is selected.
4. From the list, select the policy (or policies) you want to unassign.
5. Click **Unassign**.

Exporting User Data

From the **Users** page, you can export all information about the item selected from the User Browser directory tree to a comma separated value (.csv) file. The exported information, which changes based on the **View** selected, can be used for reporting and analytical purposes.

For additional information, refer to Exporting Data on page 43.

Chapter 11

Configuration Options

In this chapter:

You can configure a number of settings for Application Control. These settings determine what is displayed to the user when an application is blocked.

The user will then understand why an executable has been blocked, and will know how to escalate the issue if the executable is required for business purposes.

Working with Configuration Options

You can set a number of options to control the behavior of Application Control.

Select **Tools** > **Options** and click the **Application Control** tab.

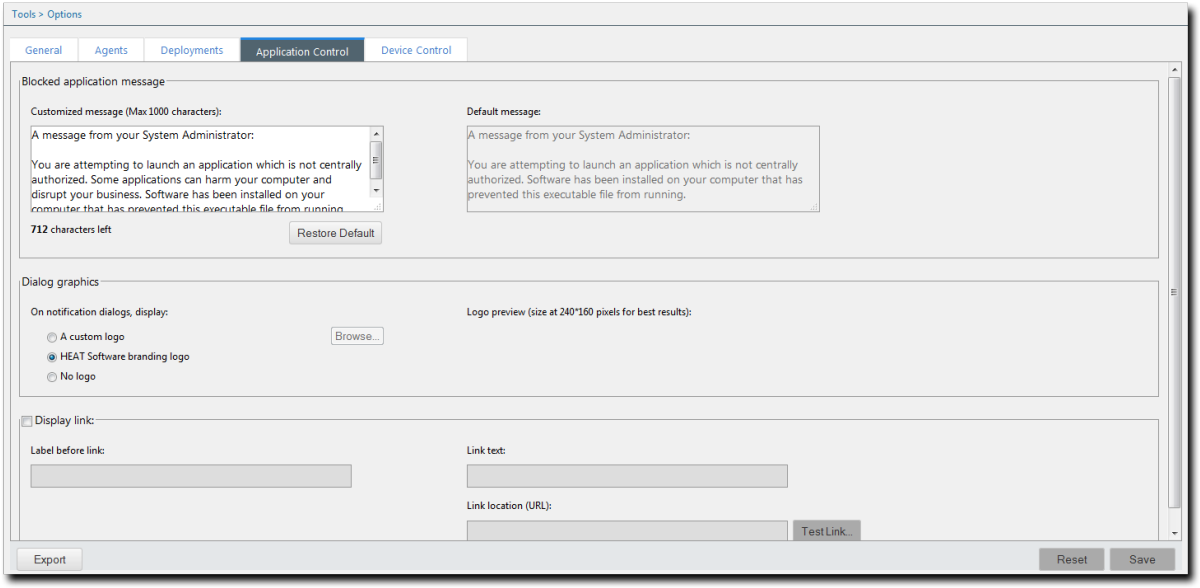


Figure 119: Application Control Configuration Options

Setting the Blocked Application Message

The **Blocked Application Message** area allows you to specify the message displayed on the ***Blocked Application Detected*** notification dialog.

You can type directly into the **Customized message** box. There is a maximum limit of 1000 characters on this message.

The **Default message** box displays the default message and can not be edited.

Clicking **Restore Default** overwrites the contents of the **Customized message** box with the contents of the **Default message** box.

Setting the Blocked Application Graphic

The **Dialog Graphics** area allows you to specify the graphic displayed on the ***Blocked Application Detected*** notification dialog.

You can select from the following options:

- A custom logo
- Ivanti branding logo
- No logo

Click **Browse** to locate a custom graphic to be displayed on the endpoint.

Note: Graphics must meet the following criteria:

- format - bitmap (*.bmp, *.png, etc.)
- size - 240 x 160 pixels

Bitmaps that are larger than the standard will be either truncated or sized to fit (if possible).

If a custom logo is selected, a preview of the logo is displayed.

Setting the Blocked Application Information Link

The **Display Link** area allows you to configure the link displayed on the ***Blocked Application Detected*** notification dialog.

If you want to display a link:

- check the **Display Link** check box
- type the text to display before the link in the **Label before link** field
- type the text to display as the link in the **Link text** field
- type the link URL in the **Link location (URL)** field

Click **Test Link** to verify that the hyperlink works (goes to the expected destination) by invoking a web browser window with the specified link pre-populated.