Product Guide

McAfee Endpoint Security 10.5

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

McAfee Endpoint Security

McAfee® Endpoint Security is a comprehensive security management solution that runs on network computers to identify and stop threats automatically. This Help explains how to use the basic security features and troubleshoot problems.

To use Endpoint Security Help with Internet Explorer, **Security Settings** | **Scripting** | **Active scripting** must be enabled in the browser.

Getting started

Frequently performed tasks

More information

To access additional information about this product, see:

- *McAfee Endpoint Security Installation Guide*
- *McAfee Endpoint Security Migration Guide*
- *McAfee Endpoint Security Release Notes*
- Endpoint Security Threat Prevention Help
- Endpoint Security Firewall Help
- Endpoint Security Web Control Help
- Endpoint Security Adaptive Threat Protection Help
- McAfee support

1 Introduction

Endpoint Security is a comprehensive security management solution that runs on network computers to identify and stop threats automatically. This Help explains how to use the basic security features and troubleshoot problems.
If your computer is *managed*, an administrator sets up and configures Endpoint Security using one of these management servers:

- McAfee® ePolicy Orchestrator® (McAfee® ePO™)
- McAfee® ePolicy Orchestrator® Cloud (McAfee ePO™ Cloud)
  For the latest Endpoint Security management license and entitlement information, see KB87057.

> Adaptive Threat Protection isn't supported on systems managed by McAfee ePO Cloud.

If your computer is *self-managed*, also called *unmanaged*, you or your administrator configure the software using the Endpoint Security Client.

Contents

Endpoint Security modules

The administrator configures and installs one or more Endpoint Security modules on client computers.

- **Threat Prevention** — Checks for viruses, spyware, unwanted programs, and other threats by scanning items — automatically when users access them or on demand at any time.
- **Firewall** — Monitors communication between the computer and resources on the network and the Internet. Intercepts suspicious communications.
- **Web Control** — Displays safety ratings and reports for websites during online browsing and searching. Web Control enables the site administrator to block access to websites based on safety rating or content.
- **Adaptive Threat Protection** — Analyzes content from your enterprise and decides what to do based on file reputation, rules, and reputation thresholds.
  Adaptive Threat Protection is an optional Endpoint Security module. For additional threat intelligence sources and functionality, deploy the Threat Intelligence Exchange server. For information, contact your reseller or sales representative.

> Adaptive Threat Protection isn't supported on systems managed by McAfee ePO Cloud.

In addition, the Common module provides settings for common features, such as interface security and logging. This module is installed automatically if any other module is installed.

How Endpoint Security protects your computer

Typically, an administrator sets up Endpoint Security, installs the software on client computers, monitors security status, and sets up security rules, called *policies*.

As a client computer user, you interact with Endpoint Security through *client software* installed on your computer. The policies set up by your administrator determine how the modules and features operate on your computer and whether you can modify them.

If Endpoint Security is self-managed, you can specify how the modules and features operate. To determine your management type, view the **About** page.

At regular intervals, the client software on your computer connects to a site on the Internet to update its components. At the same time, it sends data about detections on your computer to the management server. This data is used to generate reports for your administrator about detections and security issues on your computer.

Usually, the client software operates in the background without any interaction on your part. Occasionally, however, you might need to interact with it. For example, you might want to check for software updates or scan for malware manually. Depending on the policies set up by your administrator, you might also be able to customize the security settings.

If you are an administrator, you can centrally configure and manage client software using McAfee ePO or McAfee ePO Cloud.

For the latest Endpoint Security management license and entitlement information, see KB87057.

See also

Get information about your protection on page 21

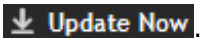
How your protection stays up to date

Regular updates of Endpoint Security make sure that your computer is always protected from the latest threats.

To perform updates, the client software connects to a local or remote McAfee ePO server or directly to a site on the Internet. Endpoint Security checks for:

- Updates to the *content files* used to detect threats. Content files contain definitions for threats such as viruses and spyware, and these definitions are updated as new threats are discovered.
- Upgrades to software components, such as patches and hotfixes.

To simplify terminology, this Help refers to both updates and upgrades as *updates*.

Updates usually occur automatically in the background. You might also need to check for updates manually. Depending on settings, you can manually update your protection from the Endpoint Security Client by clicking 

.

See also

Update content and software manually on page 22

How content files work

When searching files for threats, the scan engine compares the contents of the scanned files to known threat information stored in the AMCore content files. Exploit Prevention uses its own content files to protect against exploits.

McAfee Labs finds and adds known threat information (*signatures*) to the content files. With the signatures, content files include information about cleaning and counteracting damage that the detected malware can cause. New threats appear, and McAfee Labs releases updated content files, regularly.

If the signature of a threat isn't in the installed content files, the scan engine can't detect that threat, leaving your system vulnerable to attack.

Endpoint Security stores the currently loaded content file and the previous two versions in the Program Files\Common Files\McAfee\Engine\content folder. If required, you can revert to a previous version.

If new malware is discovered and extra detection is required outside of the regular content update schedule, McAfee Labs releases an Extra.DAT file.

AMCore content package

McAfee Labs releases AMCore content packages daily by 7:00 p.m. (GMT/UTC). If a new threat warrants it, daily AMCore content files might be released earlier and, sometimes, releases might be delayed.

To receive alerts regarding delays or important notifications, subscribe to the Support Notification Service (SNS). See KB67828.

The AMCore content package includes these components:

- **AMCore — Engine and content**
  Contains updates to the Threat Prevention scan engine and signatures based on results of ongoing threat research.
- **Adaptive Threat Protection — Scanner and rules**
  Contains rules to dynamically compute the reputation of files and processes on the endpoints.

  McAfee releases new Adaptive Threat Protection content files every two months.

  Adaptive Threat Protection is an optional Endpoint Security module. For additional threat intelligence sources and functionality, deploy the Threat Intelligence Exchange server. For information, contact your reseller or sales representative.
- **Real Protect — Engine and content**
  Contains updates to the Real Protect scan engine and signatures based on results of ongoing threat research.

  Real Protect is a component of the optional Adaptive Threat Protection module.

Exploit Prevention content package

The Exploit Prevention content package includes:

- Memory protection signatures — Generic Buffer Overflow Protection (GBOP), caller validation, Generic Privilege Escalation Prevention (GPEP), and Targeted API Monitoring.
- Application Protection List — Processes that Exploit Prevention protects.

Exploit Prevention content is similar to the McAfee Host IPS content files. See KB51504.

McAfee releases new Exploit Prevention content files once a month.

Interacting with Endpoint Security

Endpoint Security provides visual components for interacting with the Endpoint Security Client.

- McAfee icon in the Windows system tray — Enables you to start the Endpoint Security Client and view security status.
- *Notification messages* — Alert you to scan and firewall intrusion detections, and files with unknown reputations, and prompt you for input.
- On-Access Scan page — Displays the threat detection list when the on-access scanner detects a threat.
- Endpoint Security Client — Displays the current protection status and provides access to features.

For managed systems, the administrator configures and assigns policies to specify which components appear.

See also

Accessing Endpoint Security tasks from the McAfee system tray icon on page 12
About notification messages on page 13
Manage threat detections on page 59
About the Endpoint Security Client on page 14

Accessing Endpoint Security tasks from the McAfee system tray icon

The McAfee icon in the Windows system tray provides access to the Endpoint Security Client and some basic tasks.

Configuration settings determine if the McAfee icon is available.

Right-click the McAfee system tray icon to:

Check the security status.	Select **View Security Status** to display the **McAfee Security Status** page.
Open Endpoint Security Client.	Select **McAfee Endpoint Security**.
Update protection and software manually.	Select **Update Security**.

Disable or re-enable Firewall.	Select **Disable Endpoint Security Firewall** from the **Quick Settings** menu. When Firewall is disabled, the option is **Enable Endpoint Security Firewall**.
Enable, disable, or view Firewall timed groups.	Select an option from the **Quick Settings** menu: • **Enable Firewall Timed Groups** — Enables timed groups for a set amount of time to allow access to the Internet before rules restricting access are applied. When timed groups are enabled, the option is **Disable Firewall Timed Groups**. Each time you select this option, you reset the time for the groups. Depending on settings, you might be prompted to provide the administrator with a reason for enabling timed groups. • **View Firewall Timed Groups** — Displays the names of the timed groups and the amount of time remaining for each group to be active. These options might not be available, depending on how the settings are configured.

How the icon indicates the status of Endpoint Security

The appearance of the icon changes to indicate the status of the Endpoint Security. Hold the cursor over the icon to display a message describing the status.

Icon	Indicates...
	Endpoint Security is protecting your system and no issues exist.

	Endpoint Security detects an issue with your security, such as a module or technology is disabled.
	• Firewall is disabled.
	• Threat Prevention — Exploit Prevention, On-Access Scan, or ScriptScan is disabled.
	Endpoint Security reports issues differently, depending on the management type.
	• Self-managed:
	  • One or more technologies is disabled.
	  • One or more technologies is not responding.
	• Managed:
	  • One or more technologies is disabled, not as a result of a policy enforcement from the management server or from the Endpoint Security Client.
	  • One or more technologies is not responding.
	When an issue is detected, the **McAfee Security Status** page indicates which module or technology is disabled.

See also

What gets updated on page 23

About notification messages

Endpoint Security uses two types of messages to notify you of issues with your protection or to request input. Some messages might not appear, depending on how settings are configured.

The McTray.exe process must be running for Endpoint Security to display notification messages.

Endpoint Security sends two types of notifications:

- **Alerts** pop up from the McAfee icon for five seconds, then disappear.

  Alerts notify you of threat detections, such as Firewall intrusion events, or when an on-demand scan is paused or resumed. They don't require any action from you.

- **Prompts** open a page at the bottom of your screen and stay visible until you select an option.

  For example:

  - When a scheduled on-demand scan is about to start, Endpoint Security might prompt you to defer the scan.
  - When the on-access scanner detects a threat, Endpoint Security might prompt you to respond to the detection.
  - When Adaptive Threat Protection detects a file with an unknown reputation, Endpoint Security might prompt you to allow or block the file.

Windows 8 and 10 use *toast notifications* — messages that pop up to notify you of both alerts and prompts. Click the toast notification to display the notification in Desktop mode.

See also

Respond to a threat-detection prompt on page 20
Respond to a scan prompt on page 21
Respond to a file-reputation prompt on page 171

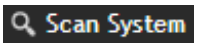
About the Endpoint Security Client

The Endpoint Security Client enables you to check the protection status and access features on your computer.

- Options on the **Action** menu provide access to features.

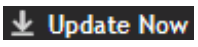
Settings	Configures feature settings. This menu option is available if either of the following is true: • The Client Interface Mode is set to **Full access**. • You are logged on as administrator.
Load Extra.DAT	Enables you to install a downloaded Extra.DAT file.
Roll Back AMCore Content	Reverts AMCore content to a previous version. This menu option is available if a previous version of AMCore content exists on the system and either of the following is true: • The Client Interface Mode is set to **Full access**. • You are logged on as administrator.
Help	Displays Help.
Support Links	Displays a page with links to helpful pages, such as the McAfee ServicePortal and Knowledge Center.
Administrator Logon	Logs on as the site administrator. (Requires administrator credentials.) This menu option is available if the Client Interface Mode isn't set to **Full access**. If you are already logged on as administrator, this option is **Administrator Logoff**.
About	Displays information about Endpoint Security.
Exit	Exits the Endpoint Security Client.

- Buttons on the top right of the page provide quick access to frequent tasks.

  Checks for malware with a Full Scan or Quick Scan of your system.

  This button is available only if the Threat Prevention module is installed.

  Updates content files and software components on your computer.

  This button might not appear, depending on how settings are configured.

- Buttons on the left side of the page provide information about your protection.

Status	Returns you to the main Status page.
Event Log	Displays the log of all protection and threat events on this computer.
Quarantine	Opens the **Quarantine Manager**.

  This button is available only if the Threat Prevention module is installed.

- The Threat Summary gives you information about threats that Endpoint Security detected on your system in the last 30 days.

See also

Load an Extra.DAT file on page 28
Log on as administrator on page 26
Scan your computer for malware on page 55
Update content and software manually on page 22
View the Event Log on page 23
Manage quarantined items on page 59
Managing Endpoint Security on page 26
About the Threat Summary on page 15

About the Threat Summary

The Endpoint Security Client Status page provides a real-time summary of any threats detected on your system in the last 30 days.

As new threats are detected, the Status page dynamically updates the data in the Threat Summary area in the bottom pane.

The Threat Summary includes:

- Date of the last eliminated threat
- Top two threat vectors, by category:

Web	Threats from webpages or downloads.
External Device or Media	Threats from external devices, such as USB, 1394 firewire, eSATA, tape, CD, DVD, or disk.
Network	Threats from the network (not network file share).
Local System	Threats from the local boot file system drive (usually C:) or drives other than those classified as External Device or Media.
File Share	Threats from a network file share.
Email	Threats from email messages.
Instant Message	Threats from instant messaging.
Unknown	Threats where attack vector isn't determined (due to error condition or other failure case).

- Number of threats per threat vector

If the Endpoint Security Client can't reach the Event Manager, Endpoint Security Client displays a communication error message. In this case, reboot your system to view the Threat Summary.

How settings affect your access to the client

Client Interface Mode settings assigned to your computer determine which modules and features you can access.

Change the Client Interface Mode in the Common settings.

For managed systems, policy changes from McAfee ePO might overwrite changes from the Settings page.

The Client Interface Mode options for the client are:

Full access	Enables access to all features, including: • Enable and disable individual modules and features. • Access the Settings page to view or modify all settings for the Endpoint Security Client. (Default)
Standard access	Displays protection status and allows access to most features: • Update the content files and software components on your computer (if enabled by the administrator). • Perform a thorough check of all areas of your system, recommended if you suspect your computer is infected. • Run a quick (2-minute) check of the areas of your system most susceptible to infection. • Access the Event Log. • Manage items in the Quarantine. From **Standard access** interface mode, you can log on as administrator to access all features, including all settings.
Lock client interface	Requires a password to access the client. Once you unlock the client interface, you can access all features.

If you can't access the Endpoint Security Client or specific tasks and features that you need to do your job, talk to your administrator.

See also

Control access to the client interface on page 31

How installed modules affect the client

Some aspects of the client might not be available, depending on the modules installed on your computer.

These features are available only if Threat Prevention is installed:

- Scan System button
- **Quarantine** button

The features installed on the system determine the features that appear:

- In the Event Log **Filter by Module** drop-down list.
- On the **Settings** page.

Common	Appears if any module is installed.
Threat Prevention	Appears only if Threat Prevention is installed.
Firewall	Appears only if Firewall is installed.
Web Control	Appears only if Web Control is installed.
Adaptive Threat Protection	Appears only if Adaptive Threat Protection and Threat Prevention are installed.

Adaptive Threat Protection isn't supported on systems managed by McAfee ePO Cloud.

Depending on the Client Interface Mode and how the administrator configured your access, some or all features might not be available.

See also

How settings affect your access to the client on page 16

2 Using the Endpoint Security Client

Use the client in Standard access mode to perform most functions, including system scans and managing quarantined items.

Contents

Open the Endpoint Security Client

Open the Endpoint Security Client to display the status of the protection features installed on the computer.

If the interface mode is set to **Lock client interface**, you must enter the administrator password to open Endpoint Security Client.

Task

1 Use one of these methods to display the Endpoint Security Client:

- Right-click the system tray icon, then select **McAfee Endpoint Security**.
- Select **Start** | **All Programs** | **McAfee** | **McAfee Endpoint Security**.
- On Windows 8 and 10, start the **McAfee Endpoint Security** app.
  1 Press the **Windows** key.
  2 Enter `McAfee Endpoint Security` in the search area, then double-click or touch the **McAfee Endpoint Security** app.

2 If prompted, enter the administrator password on the **Administrator Log On** page, then click **Log On**.

Endpoint Security Client opens in the interface mode that the administrator configured.

See also

Unlock the client interface on page 26

Get help

The two methods for getting help while working in the client are the **Help** menu option and the **?** icon.

To use Endpoint Security Help with Internet Explorer, **Security Settings** | **Scripting** | **Active scripting** must be enabled in the browser.

Task

1 Open the Endpoint Security Client.

2 Depending on the page you're on:

- **Status**, **Event Log**, and **Quarantine** pages: from the **Action** menu, select **Help**.
- **Settings**, **Update**, **Scan System**, **Roll Back AMCore Content**, and **Load Extra.DAT** pages: click **?** in the interface.

Respond to prompts

Depending on how settings are configured, Endpoint Security might prompt you for input when it detects a threat or when a scheduled on-demand scan is about to start.

Tasks

- *Respond to a threat-detection prompt* on page 20
  When the scanner detects a threat, Endpoint Security might prompt you for input to continue, depending on how settings are configured.
- *Respond to a scan prompt* on page 21
  When a scheduled on-demand scan is about to start, Endpoint Security might prompt you for input to continue. The prompt appears only if the scan is configured to allow you to defer, pause, resume, or cancel the scan.

Respond to a threat-detection prompt

When the scanner detects a threat, Endpoint Security might prompt you for input to continue, depending on how settings are configured.

Windows 8 and 10 use *toast notifications* — messages that pop up to notify you of both alerts and prompts. Click the toast notification to display the notification in Desktop mode.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- From the **On-Access Scan** page, select options to manage threat detections.

  You can reopen the scan page to manage detections at any time.

  The on-access scan detection list is cleared when the Endpoint Security service restarts or the system reboots.

See also

Manage threat detections on page 59

Respond to a scan prompt

When a scheduled on-demand scan is about to start, Endpoint Security might prompt you for input to continue. The prompt appears only if the scan is configured to allow you to defer, pause, resume, or cancel the scan.

If you don't select an option, the scan starts automatically.

For managed systems only, if the scan is configured to run only the scan when the computer is idle, Endpoint Security displays a dialog when the scan is paused. If configured, you can also resume these paused scans or reset them to run only when you're idle.

Windows 8 and 10 use *toast notifications* — messages that pop up to notify you of both alerts and prompts. Click the toast notification to display the notification in Desktop mode.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- At the prompt, select one of these options.

  The options that appear depend on how the scan is configured.

Scan Now	Starts the scan immediately.
View Scan	Views detections for a scan in progress.
Pause Scan	Pauses the scan. Depending on the configuration, clicking **Pause Scan** might reset the scan to run only when you're idle. Click **Resume Scan** to resume the scan where it left off.
Resume Scan	Resumes a paused scan.
Cancel Scan	Cancels the scan.
Defer Scan	Delays the scan for the specified number of hours. Scheduled scan options determine how many times that you can defer the scan for one hour. You might be able to defer the scan more than once.
Close	Closes the scan page.

  If the scanner detects a threat, Endpoint Security might prompt you for input to continue, depending on how settings are configured.

Get information about your protection

You can get information about your Endpoint Security protection, including management type, protection modules, features, status, version numbers, and licensing.

Task

1. Open the Endpoint Security Client.
2. From the **Action** menu, select **About**.
3. Click the name of a module or feature on the left to jump to information about that item.
4. Click the browser **Close** button to close the **About** page.

See also

Management types on page 22
Open the Endpoint Security Client on page 19

Management types

The *management type* indicates how Endpoint Security is managed.

For managed systems, policy changes from McAfee ePO might overwrite changes from the Settings page.

Management type	Description
McAfee ePolicy Orchestrator	An administrator manages Endpoint Security using McAfee ePO (on-premise).
McAfee ePolicy Orchestrator Cloud	An administrator manages Endpoint Security using McAfee ePO Cloud. For the latest Endpoint Security management license and entitlement information, see KB87057.
Self-Managed	Endpoint Security is managed locally using Endpoint Security Client. This mode is also called *unmanaged* or *standalone*.

Update content and software manually

You can manually check for and download updated content files and software components from the Endpoint Security Client.

Manual updates are called *on-demand updates*.

You can also run manual updates from the McAfee system tray icon.

Endpoint Security doesn't support manually retrieving and copying updated content files to the client system. If you need assistance updating to a specific content version, contact McAfee support

Task

1 Open the Endpoint Security Client.

2 Click **Update Now**.

If this button doesn't appear in the client, you can enable it in the settings.

Endpoint Security Client checks for updates.

The Update page displays information about the last update: **Never**, **Today**, or the date and time of the last update if not today.

To cancel the update, click **Cancel**.

- If the update completes successfully, the page displays **Update Finished** and the last update as **Today**.
- If the update was unsuccessful, errors appear in the **Messages** area.

  View the PackageManager_Activity.log or PackageManager_Debug.log for more information.

3 Click **Close** to close the **Update** page.

See also

Accessing Endpoint Security tasks from the McAfee system tray icon on page 12
How your protection stays up to date on page 10
Endpoint Security log file names and locations on page 24
What gets updated on page 23
Configure the default behavior for updates on page 35
Open the Endpoint Security Client on page 19

What gets updated

Endpoint Security updates security content and software (hotfixes and patches) differently, depending on update method and settings.

The visibility and behavior of the **Update Now** button is configurable.

Update method	Updates
Update Security option on the McAfee system tray icon menu	Content and software.
Update Now button in the Endpoint Security Client	Content or software, or both, depending on settings.

See also

Update content and software manually on page 22

View the Event Log

The activity and debug logs store a record of events that occur on the McAfee-protected system. You can view the Event Log from the Endpoint Security Client.

Task

For help, from the **Action** menu  , select **Help**.

1 Open the Endpoint Security Client.

2 Click **Event Log** on the left side of the page.

The page shows any events that Endpoint Security has logged on the system in the last 30 days.

If the Endpoint Security Client can't reach the Event Manager, it displays a communication error message. In this case, reboot the system to view the Event Log.

3 Select an event from the top pane to display the details in the bottom pane.

To change the relative sizes of the panes, click and drag the sash widget between the panes.

4 On the **Event Log** page, sort, search, filter, or reload events.

The options that appear depend on how the scan is configured.

To...	Steps
Sort events by date, features, action taken, and severity.	Click the table column heading.
Search the event log.	Enter the search text in the **Search** field and press **Enter**, or click **Search**. The search is case-insensitive and searches all fields of the event log for the search text. The event list shows all elements with matching text. To cancel the search and display all events, click **x** in the **Search** field.
Filter events by severity or module.	From the filter drop-down list, select an option. To remove the filter and display all events, select **Show all events** from the drop-down list.
Refresh the **Event Log** display with any new events.	Click .
Open the folder that contains the log files.	Click **View Logs Folder**.

5 Navigate within the Event Log.

To...	Steps
Display the previous page of events.	Click **Previous page**.
Display the next page of events.	Click **Next page**.
Display a specific page in the log.	Enter a page number and press **Enter** or click **Go**.

By default, the Event Log displays 20 events per page. To display more events per page, select an option from the **Events per page** drop-down list.

See also

Endpoint Security log file names and locations on page 24
Open the Endpoint Security Client on page 19

Endpoint Security log file names and locations

The activity, error, and debug log files record events that occur on systems with Endpoint Security enabled. Configure logging in the Common settings.

Activity log files always appear in the language specified by the default system locale.

All activity and debug log files are stored here:

%ProgramData%\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in one file, EndpointSecurityPlatform_Errors.log.

Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.

Table 2-1 Log files

Module	Feature or technology	File name
Common		EndpointSecurityPlatform_Activity.log
		EndpointSecurityPlatform_Debug.log
	Self Protection	SelfProtection_Activity.log
		SelfProtection_Debug.log
	Updates	PackageManager_Activity.log
		PackageManager_Debug.log
	Errors	EndpointSecurityPlatform_Errors.log Contains error logs for all modules.
	Endpoint Security Client	MFEConsole_Debug.log
Threat Prevention	Enabling debug logging for any Threat Prevention technology also enables debug logging for the Endpoint Security Client.	ThreatPrevention_Activity.log
		ThreatPrevention_Debug.log
	Access Protection	AccessProtection_Activity.log
		AccessProtection_Debug.log
	Exploit Prevention	ExploitPrevention_Activity.log
		ExploitPrevention_Debug.log
	On-Access Scan	OnAccessScan_Activity.log
		OnAccessScan_Debug.log
	On-Demand Scan • Quick Scan • Full Scan • Right-Click Scan	OnDemandScan_Activity.log
		OnDemandScan_Debug.log
Firewall		Firewall_Activity.log
		Firewall_Debug.log
		FirewallEventMonitor.log Logs blocked and allowed traffic events, if configured.
Web Control		WebControl_Activity.log
		WebControl_Debug.log
Adaptive Threat Protection		AdaptiveThreatProtection_Activity.log
		AdaptiveThreatProtection_Debug.log
	Dynamic Application Containment	DynamicApplicationContainment_Activity.log
		DynamicApplicationContainment_Debug.log

By default, installation log files are stored here:

%TEMP%\McAfeeLogs, which is the Windows user TEMP folder.

Managing Endpoint Security

As administrator, you can manage Endpoint Security from the Endpoint Security Client, which includes disabling and enabling features, managing content files, specifying how the client interface behaves, scheduling tasks, and configuring common settings.

For managed systems, policy changes from McAfee ePO might overwrite changes from the Settings page.

See also

Log on as administrator on page 26
Unlock the client interface on page 26
Disable and enable features on page 27
Change the AMCore content version on page 27
Use Extra.DAT files on page 28
Configure common settings on page 29

Log on as administrator

Log on to Endpoint Security Client as administrator to enable and disable features and configure settings.

Before you begin

The interface mode for the Endpoint Security Client must be set to **Standard access**.

Task

For help, from the **Action** menu, select **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Administrator Logon**.

3 In the **Password** field, enter the administrator password, then click **Log On**.

You can now access all features of the Endpoint Security Client.

To log off, select **Action** | **Administrator Logoff**. The client returns to **Standard access** interface mode.

Unlock the client interface

If the interface for Endpoint Security Client is locked, unlock the interface with the administrator password to access all settings.

Before you begin

The interface mode for the Endpoint Security Client must be set to **Lock client interface**.

Task

1 Open the Endpoint Security Client.

2 On the **Administrator Log On** page, enter the administrator password in the **Password** field, then click **Log On**.

Endpoint Security Client opens and you can now access all features of the client.

3 To log off and close the client, from the **Action** menu, select **Administrator Logoff**.

Disable and enable features

As an administrator, you can disable and enable Endpoint Security features from the Endpoint Security Client.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

The **Status** page shows the enabled status of the module, which might not reflect the actual status of features. You can see the status of each feature in the **Settings** page. For example, if the **Enable ScriptScan** setting isn't successfully applied, the status might be (Status: Disabled).

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click the module name (such as **Threat Prevention** or **Firewall**) on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click the module name on the **Settings** page.
3. Select or deselect the **Enable** *module* or *feature* option.

   Enabling any of the Threat Prevention features enables the Threat Prevention module.

See also

Log on as administrator on page 26

Change the AMCore content version

Use Endpoint Security Client to change the version of AMCore content on the client system.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Endpoint Security stores the currently loaded content file and the previous two versions in the Program Files\Common Files\McAfee\Engine\content folder. If required, you can revert to a previous version.

Exploit Prevention content updates cannot be rolled back.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. From the **Action** menu, select **Roll Back AMCore Content**.
3. From the drop-down, select the version to load.
4. Click **Apply**.

The detections in the loaded AMCore content file take effect immediately.

See also

How content files work on page 11
Log on as administrator on page 26

Use Extra.DAT files

You can install an Extra.DAT file to protect your system against a major malware outbreak until the next scheduled AMCore content update is released.

Tasks

- *Download Extra.DAT files* on page 28
  To download an Extra.DAT file, click the download link supplied by McAfee Labs.
- *Load an Extra.DAT file* on page 28
  To install the downloaded Extra.DAT file, use Endpoint Security Client.

See also

About Extra.DAT files on page 28

About Extra.DAT files

When new malware is discovered and extra detection is required, McAfee Labs releases an Extra.DAT file. Extra.DAT files contain information that Threat Prevention uses to handle the new malware.

You can download Extra.DAT files for specific threats from the McAfee Labs Extra.DAT Request Page.

Threat Prevention supports using only one Extra.DAT file.

Each Extra.DAT file has an expiration date built in. When the Extra.DAT file is loaded, this expiration date is compared against the build date of the AMCore content installed on the system. If the build date of the AMCore content set is newer than the Extra.DAT expiration date, the Extra.DAT is considered expired and is no longer loaded and used by the engine. During the next update, the Extra.DAT is removed from the system.

If the next update of AMCore content includes the Extra.DAT signature, the Extra.DAT is removed.

Endpoint Security stores Extra.DAT files in the c:\Program Files\Common Files\McAfee\Engine\content\avengine\extradat folder.

Download Extra.DAT files

To download an Extra.DAT file, click the download link supplied by McAfee Labs.

Task

1 Click the download link, specify a location to save the Extra.DAT file, then click **Save**.

2 If necessary, unzip the EXTRA.ZIP file.

3 Load the Extra.DAT file with Endpoint Security Client.

Load an Extra.DAT file

To install the downloaded Extra.DAT file, use Endpoint Security Client.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. From the **Action** menu, select **Load Extra.DAT**.
3. Click **Browse**, navigate to the location where you downloaded the Extra.DAT file, then click **Open**.
4. Click **Apply**.

The new detections in the Extra.DAT take effect immediately.

See also

Log on as administrator on page 26

Configure common settings

Configure settings that apply to all modules and features of Endpoint Security in the Common module. These settings include Endpoint Security Client interface security and language settings, logging, proxy server settings for McAfee GTI, and update configuration.

Tasks

- *Protect Endpoint Security resources* on page 29
  One of the first things that malware attempts to do during an attack is to disable your system security software. Configure Self Protection in the Common settings to prevent Endpoint Security services and files from being stopped or modified.
- *Configure logging settings* on page 30
  Configure Endpoint Security logging in the Common settings.
- *Allow certificate authentication* on page 30
  Certificates allow a vender to run code within McAfee processes.
- *Control access to the client interface* on page 31
  Control access to the Endpoint Security Client by setting a password in the Common settings.
- *Configure proxy server settings for McAfee GTI* on page 32
  Specify proxy server options for retrieving McAfee GTI reputation in the Common settings.

Protect Endpoint Security resources

One of the first things that malware attempts to do during an attack is to disable your system security software. Configure Self Protection in the Common settings to prevent Endpoint Security services and files from being stopped or modified.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Disabling Endpoint Security Self Protection leaves your system vulnerable to attack.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Settings**.

3 Click **Show Advanced**.

4 From **Self Protection**, verify that **Self Protection** is enabled.

5 Specify the action for each of the following Endpoint Security resources:

- **Files and folders** — Prevents users from changing the McAfee database, binaries, safe search files, and configuration files.
- **Registry** — Prevents users from changing the McAfee registry hive, COM components, and uninstalling using the registry value.
- **Processes** — Prevents stopping McAfee processes.

6 Click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26

Configure logging settings

Configure Endpoint Security logging in the Common settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Settings**.

3 Click **Show Advanced**.

4 Configure **Client Logging** settings on the page.

5 Click **Apply** to save your changes or click **Cancel**.

See also

Endpoint Security log file names and locations on page 24
Log on as administrator on page 26

Allow certificate authentication

Certificates allow a vender to run code within McAfee processes.

When a process is detected, the certificate table is populated with the Vendor, Subject, and Hash of the associated public key.

This setting might result in compatibility issues and reduced security.

For details about product features, usage, and best practices, click **?** or **Help**.

Task

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Settings**.

3 Click **Show Advanced**.

4 In the Certificates section, select **Allow**.

5 Click **Apply** to save your changes or click **Cancel**.

The certificate information appears in the table.

Control access to the client interface

Control access to the Endpoint Security Client by setting a password in the Common settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Client Interface Mode is set to **Full access** by default, allowing users to change their security configuration, which can leave systems unprotected from malware attacks.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Settings**.

3 Configure **Client Interface Mode** settings on the page.

Best practice: To improve security, change **Client Interface Mode** to **Standard** or **Lock client interface**. Both of these options require an Administrator password to access Endpoint Security Client settings.

Best practice: Change Administrator passwords regularly.

4 Click **Apply** to save your changes or click **Cancel**.

See also

Effects of setting an administrator password on page 31
Log on as administrator on page 26

Effects of setting an administrator password

When you set the interface mode to Standard access or Lock client interface, you must also set an administrator password. The administrator can also generate a time-based password that users can enter for temporarily access Endpoint Security Client.

Setting the interface mode to Standard access or Lock client interface affects the following users:

All users	In Lock client interface mode, users must enter the administrator or temporary password to access the Endpoint Security Client. Once entered, the user has access to the whole interface, including configuration settings on the **Settings** page.
Non-administrators (users without administrator rights)	In Standard access mode, non-administrators can: • Get information about which Endpoint Security modules are installed, including version and status. • Run scans. • Check for updates (if enabled). • View and manage items in the Quarantine. • View the Event Log. • Get help and access the FAQ and Support pages. In Standard access mode, non-administrators can't: • View or change configuration settings on the **Settings** page. • Roll back AMCore Content. • Load Extra.DAT files.
Administrators (users with administrator rights)	In Standard access mode, administrators must enter the administrator or temporary password. Once entered, the administrator has access to the whole interface, including configuration settings on the **Settings** page.

Configure proxy server settings for McAfee GTI

Specify proxy server options for retrieving McAfee GTI reputation in the Common settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Settings**.

3 Click **Show Advanced**.

4 Configure **Proxy Server for McAfee GTI** settings on the page.

Best practice: Exclude the McAfee GTI addresses from the proxy server. For information, see KB79640 and KB84374.

5 Click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26

Configure update behavior

Specify the behavior for updates initiated from the Endpoint Security Client in the Common settings.

Tasks

- *Configure source sites for updates* on page 33
  You can configure the sites from which Endpoint Security Client gets updated security files in the Common settings.
- *Configure the default behavior for updates* on page 35
  You can specify the default behavior for updates initiated from the Endpoint Security Client in the Common settings.
- *Configure, schedule, and run update tasks* on page 36
  You can configure custom update tasks, or change the **Default Client Update** task schedule, from the Endpoint Security Client in the Common settings.
- *Configure, schedule, and run mirror tasks* on page 37
  You can modify or schedule mirror tasks from the Endpoint Security Client in the Common settings.

Configure source sites for updates

You can configure the sites from which Endpoint Security Client gets updated security files in the Common settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Settings**.

3 Click **Show Advanced**.

4 From **Common**, click **Options**.

5 Configure **Source Sites for Updates** settings on the page.

You can enable and disable the default backup source site, **McAfeeHttp**, and the management server (for managed systems), but you can't otherwise modify or delete them.

The order of the sites determines the order Endpoint Security uses to search for the update site.

To...	Follow these steps
Add a site to the list.	1 Click **Add**. 2 Specify the site settings, then click **OK**. The site appears at the beginning of the list.
Change an existing site.	1 Double-click the site name. 2 Change the settings, then click **OK**.
Delete a site.	Select the site, then click **Delete**.

To...	Follow these steps
Import sites from a source site list file.	1 Click **Import**. 2 Select the file to import, then click **OK**. The site list file replaces the existing source site list.
Export the source site list to a SiteList.xml file.	1 Click **Export All**. 2 Select the location to save the source site list file to, then click **OK**.
Reorder sites in the list.	To move elements: 1 Select elements to move. The grip appears to the left of elements that can be moved. 2 Drag-and-drop the elements to the new location. A blue line appears between elements where you can drop the dragged elements.

6 Click **Apply** to save your changes or click **Cancel**.

See also

What the repository list contains on page 34
How the Default Client Update task works on page 35
Log on as administrator on page 26
Configure, schedule, and run update tasks on page 36

What the repository list contains

The *repository list* specifies information about repositories that McAfee Agent uses to update McAfee products, including Engine and DAT files.

The repository list includes:

- Repository information and location
- Repository order preference
- Proxy server settings, where required
- Encrypted credentials required to access each repository

The McAfee Agent Product Update client task connects to the first enabled repository (update site) in the repository list. If this repository is unavailable, the task contacts the next site in the list until it connects successfully or reaches the end of the list.

If your network uses a proxy server, you can specify which proxy settings to use, the address of the proxy server, and whether to use authentication. Proxy information is stored in the repository list. The proxy settings that you configure apply to all repositories in the repository list.

The location of the repository list depends on your operating system:

Operating system	Repository list location
Microsoft Windows 8	C:\ProgramData\McAfee\Common Framework\SiteList.xml
Microsoft Windows 7	
Earlier versions	C:\Documents and Settings\All Users\Application Data\McAfee\Common Framework\SiteList.xml

Configure the default behavior for updates

You can specify the default behavior for updates initiated from the Endpoint Security Client in the Common settings.

> **Before you begin**
>
> The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Use these settings to:

- Show or hide the Update Now button in the client.
- Specify what to update when the user clicks the button or the Default Client Update task runs.

By default, the Default Client Update task runs every day at 1:00 a.m. and repeats every four hours until 11:59 p.m.

On self-managed systems, the Default Client Update task updates all content and software. On managed systems, this task updates the content only.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. From the **Action** menu, select **Settings**.
3. Click **Show Advanced**.
4. Configure **Default Client Update** settings on the page.
5. Click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26
Configure source sites for updates on page 33
Configure, schedule, and run update tasks on page 36

How the Default Client Update task works

The Default Client Update task downloads the most current protection to the Endpoint Security Client.

Endpoint Security includes the Default Client Update task that runs every day at 1:00 a.m. and repeats every four hours until 11:59 p.m.

The Default Client Update task:

1. Connects to the first enabled source site in the list.

   If this site isn't available, the task contacts the next site until it connects or reaches the end of the list.
2. Downloads an encrypted `CATALOG.Z` file from the site.

   The file contains information required to perform the update, including available files and updates.
3. Checks the software versions in the file against the versions on the computer and downloads any new available software updates.

If the Default Client Update task is interrupted during the update:

Updates from...	If interrupted...
HTTP, UNC, or a local site	Resumes where the update left off the next time the update task starts.
FTP site (single-file download)	Doesn't resume if interrupted.
FTP site (multiple-file download)	Resumes before the file that was being downloaded at the time of the interruption.

See also

Configure source sites for updates on page 33
Configure, schedule, and run update tasks on page 36
What the repository list contains on page 34

Configure, schedule, and run update tasks

You can configure custom update tasks, or change the **Default Client Update** task schedule, from the Endpoint Security Client in the Common settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Use these settings to configure from the client when the **Default Client Update** task runs. You can also configure the default behavior for client updates initiated from the Endpoint Security Client.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Settings**.

3 Click **Show Advanced**.

4 From **Common**, click **Tasks**.

5 Configure the update task settings on the page.

To...	Follow these steps
Create a custom update task.	1 Click **Add**. 2 Enter the name, then from the **Select task type** drop-down list, select **Update**. 3 Configure the settings, then click **OK** to save the task.
Change an update task.	• Double-click the task, make your changes, then click **OK** to save the task.
Remove a custom update task.	• Select the task, then click **Delete**.
Create a copy of an update task.	1 Select the task, then click **Duplicate**. 2 Enter the name, configure the settings, then click **OK** to save the task.

To...	Follow these steps
Change the schedule for a **Default Client Update** task.	1 Double-click **Default Client Update**. 2 Click the **Schedule** tab, change the schedule, then click **OK** to save the task. You can also configure the default behavior for client updates initiated from the Endpoint Security Client.
Run an update task.	• Select the task, then click **Run Now**. If the task is already running, including paused or deferred, the button changes to **View**. If you run a task before applying changes, Endpoint Security Client prompts you to save the settings.

6 Click **Apply** to save your changes or click **Cancel**.

See also

How the Default Client Update task works on page 35
Configure source sites for updates on page 33
Configure the default behavior for updates on page 35

Configure, schedule, and run mirror tasks

You can modify or schedule mirror tasks from the Endpoint Security Client in the Common settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu  , select **Settings**.

3 Click **Show Advanced**.

4 From **Common**, click **Tasks**.

5 Configure the mirror task settings on the page.

To...	Follow these steps
Create a mirror task.	1 Click **Add**. 2 Enter the name, then from the **Select task type** drop-down list, select **Mirror**. 3 Configure the settings, then click **OK**.
Change a mirror task.	• Double-click the mirror task, make your changes, then click **OK**.
Remove a mirror task.	• Select the task, then click **Delete**.
Create a copy of a mirror task.	1 Select the task, then click **Duplicate**. 2 Enter the name, configure the settings, then click **OK**.

To...	Follow these steps
Schedule a mirror task.	1 Double-click the task. 2 Click the **Schedule** tab, change the schedule, then click **OK** to save the task.
Run a mirror task.	• Select the task, then click **Run Now**. If the task is already running, including paused or deferred, the button changes to **View**. If you run a task before applying changes, Endpoint Security Client prompts you to save the settings.

6 Click **Apply** to save your changes or click **Cancel**.

How mirror tasks work

The mirror task replicates the update files from the first accessible repository, defined in the repository list, to a mirror site on your network.

The most common use of this task is to mirror the contents of the McAfee download site to a local server.

After you replicate the McAfee site that contains the update files, computers on your network can download the files from the mirror site. This approach enables you to update any computer on your network, whether or not it has Internet access. Using a replicated site is more efficient because your systems communicate with a server that is closer than a McAfee Internet site, economizing access and download time.

Endpoint Security relies on a directory to update itself. Therefore, when mirroring a site, make sure to replicate the entire directory structure.

Endpoint Security Client interface reference — Common

Provide context-sensitive help for pages in the Endpoint Security Client interface.

Contents

Event Log page

Displays the activity and debug events in the Event Log.

Table 2-2 Options

Option	Definition
Number of events	Indicates the number of events that Endpoint Security logged on the system in the last 30 days.
	Refreshes the Event Log display with any new event data.
View Logs Folder	Opens the folder that contains the log files in Windows Explorer.
Show all events	Removes any filter.

Table 2-2 Options *(continued)*

Option	Definition
Filter by Severity	Filters events by a severity level: **Alert** — Shows level 1 severity events only. **Critical and greater** — Shows levels 1 and 2 severity events only. **Warning and greater** — Shows levels 1, 2, and 3 severity events only. **Notice and greater** — Shows levels 1, 2, 3, and 4 severity levels.
Filter by Module	Filters events by module: **Common** — Shows Common events only. **Threat Prevention** — Shows Threat Prevention events only. **Firewall** — Shows Firewall events only. **Web Control** — Shows Web Control events only. **Adaptive Threat Protection** — Shows Adaptive Threat Protection events only. The features that appear in the drop-down list depend on the features installed on the system at the time you opened the Event Log.
Search	Searches the Event Log for a string.
Events per page	Selects the number of events to display on a page. (By default, 20 events per page)
Previous page	Displays the previous page in the Event Log.
Next page	Displays the next page in the Event Log.
Page x **of** x	Selects a page in the Event Log to navigate to. Enter a number in the **Page** field and press **Enter** or click **Go** to navigate to the page.

Column heading	Sorts the event list by...
Date	Date the event occurred.
Feature	Feature that logged the event.

Column heading	Sorts the event list by...	
Action taken	Action that Endpoint Security took, if any, in response to the event. The action is configured in the settings.	
	Access Denied	Prevented access to file.
	Allowed	Allowed access to file.
	Blocked	Blocked access to the file.
	Cleaned	Removed the threat from the file automatically.
	Contained	Ran the file in a container based on its reputation.
	Continue Scanning	Detected a threat and continued scanning the next file without taking any action, such as Clean or Delete, on the current file.
	Deleted	Deleted file automatically.
	Moved	Moved the file into the Quarantine.
	Would Block	A rule would have blocked access to the file if the rule was being enforced. Observe mode is enabled.
	Would Clean	A rule would have cleaned the file if the rule was being enforced. Observe mode is enabled.
	Would Contain	A rule would have contained the file if the rule was being enforced. Observe mode is enabled.
Severity	Severity level of the event.	
	Critical	1
	Major	2
	Minor	3
	Warning	4
	Informational	5

See also

View the Event Log on page 23

Common — Options

Configure settings for Endpoint Security Client interface, Self Protection, activity and debug logging, and proxy server.

Table 2-3 Options

Section	Option	Definition
Client Interface Mode	**Full access**	Allows access to all features. (Default)
	Standard access	Displays protection status and allows access to most features, such as running updates and scans. **Standard access** mode requires a password to view and change settings on the Endpoint Security Client **Settings** page.
	Lock client interface	Requires a password to access the Endpoint Security Client.

Table 2-3 Options *(continued)*

Section	Option	Definition
	Set Administrator password	For **Standard access** and **Lock client interface**, specifies the Administrator password for accessing all features of the Endpoint Security Client interface. • **Password** — Specifies the password. • **Confirm password** — Confirms the password. **Best practice:** Change Administrator passwords regularly.
Uninstallation	**Require password to uninstall the client**	Requires a password to uninstall Endpoint Security Client and specifies the password. The default password is `mcafee`. (Disabled by default) • **Password** — Specifies the password. • **Confirm password** — Confirms the password.

Table 2-4 Advanced options

Section	Option	Definition
Client Interface Language	**Automatic**	Automatically selects the language to use for Endpoint Security Client interface text based on the language on the client system.
	Language	Specifies the language to use for Endpoint Security Client interface text. For managed systems, language changes made from the Endpoint Security Client override policy changes from the management server. The language change is applied after the Endpoint Security Client restarts. The client language doesn't affect the log files. Log files always appear in the language specified by the default system locale.
Self Protection	**Enable Self Protection**	Protects Endpoint Security system resources from malicious activity.
	Action	Specifies the action to take when malicious activity occurs: • **Block and report** — Blocks activity and reports to McAfee ePO. (Default) • **Block only** — Blocks activity but doesn't report to McAfee ePO. • **Report only** — Reports to McAfee ePO but doesn't block activity.
	Files and folders	Prevents changing or deleting McAfee system files and folders.
	Registry	Prevents changing or deleting McAfee registry keys and values.
	Processes	Prevents stopping McAfee processes.
	Exclude these processes	Allows access for the specified processes. Wildcards are supported. **Add** — Adds a process to the exclusion list. Click **Add**, then enter the exact resource name, such as `avtask.exe`. *Double-click an item* — Changes the selected item. **Delete** — Deletes the selected item. Select the resource, then click **Delete**.

Table 2-4 Advanced options *(continued)*

Section	Option	Definition
Certificates		Specifies certificate options.
	Allow	Allows a vendor to run code in McAfee processes. This setting might result in compatibility issues and reduced security.
	Vendor	Specifies the Common Name (CN) of the authority that signed and issued the certificate.
	Subject	Specifies the Signer Distinguished Name (SDN) that defines the entity associated with the certificate. This information can include: • **CN** — Common Name • **OU** — Organization Unit • **O** — Organization • **L** — Locality • **ST** — State or province • **C** — Country Code
	Hash	Specifies the hash of the associated public key.
Client Logging	**Log files location**	Specifies the location for the log files. The default location is: `<SYSTEM_DRIVE>:\ProgramData\McAfee\Endpoint\Logs` Enter or click **Browse** to navigate to a location.
Activity Logging	**Enable activity logging**	Enables logging of all Endpoint Security activity.
	Limit size (MB) of each of the activity log files	Limits each activity log file to the specified maximum size (between 1 MB and 999 MB). The default is 10 MB. If the log file exceeds this size, new data replaces the oldest 25 percent of the entries in the file. To allow log files to grow to any size, disable this option.
Debug Logging		Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection. **Best practice:** Enable debug logging for at least the first 24 hours during testing and pilot phases. If no issues occur during this time, disable debug logging to avoid performance impact on client systems.

Table 2-4 Advanced options *(continued)*

Section	Option	Definition
	Enable for Threat Prevention	Enables verbose logging of activity for Threat Prevention and individual technologies: **Enable for Access Protection** — Logs to AccessProtection_Debug.log. **Enable for Exploit Prevention** — Logs to ExploitPrevention_Debug.log. **Enable for On-Access Scan** — Logs to OnAccessScan_Debug.log. **Enable for On-Demand Scan** — Logs to OnDemandScan_Debug.log. Enabling debug logging for any Threat Prevention technology also enables debug logging for the Endpoint Security Client.
	Enable for Firewall	Enables verbose logging of activity for Firewall.
	Enable for Web Control	Enables verbose logging of activity for Web Control.
	Enable for Adaptive Threat Protection	Enables verbose logging of activity for Adaptive Threat Protection.
	Limit size (MB) of each of the debug log files	Limits each debug log file to the specified maximum size (between 1 MB and 999 MB). The default is 50 MB. If the log file exceeds this size, new data replaces the oldest 25 percent of the entries in the file. To allow log files to grow to any size, disable this option.
Event Logging	**Send events to McAfee ePO**	Sends all events logged to the **Event Log** on the Endpoint Security Client to McAfee ePO. This option is available on systems managed by McAfee ePO only.
	Log events to Windows Application log	Sends all events logged to the **Event Log** on the Endpoint Security Client to the Windows Application log. The Windows Application log is accessible from the Windows **Event Viewer** | **Windows Logs** | **Application**.
	Severity levels	Specifies the severity level of events to log to the **Event Log** on the Endpoint Security Client: • **None** — Sends no alerts • **Alert only** — Sends alert level 1 only. • **Critical and Alert** — Sends alert levels 1 and 2. • **Warning, Critical, and Alert** — Sends alert levels 1–3. • **All except Informational** — Sends alert levels 1–4. • **All** — Sends alert levels 1–5. • 1 — Alert • 2 — Critical • 3 — Warning • 4 — Notice • 5 — Informational

Table 2-4 Advanced options *(continued)*

Section	Option	Definition
	Threat Prevention events to log	Specifies the severity level of events for each Threat Prevention feature to log: **Access Protection** — Logs to AccessProtection_Activity.log. Enabling event logging for Access Protection also enables event logging for Self Protection. **Exploit Prevention** — Logs to ExploitPrevention_Activity.log. **On-Access Scan** — Logs to OnAccessScan_Activity.log. **On-Demand Scan** — Logs to OnDemandScan_Activity.log.
	Firewall events to log	Specifies the severity level of Firewall events to log.
	Web Control events to log	Specifies the severity level of Web Control events to log.
	Adaptive Threat Protection events to log	Specifies the severity level of Adaptive Threat Protection events to log.
Proxy Server for McAfee GTI	**No proxy server**	Specifies that the managed systems retrieve McAfee GTI reputation information directly over the Internet, not through a proxy server. (Default)
	Use system proxy settings	Specifies the use of the proxy settings from the client system, and optionally enables HTTP proxy authentication.
	Configure proxy server	Customizes proxy settings. • **Address** — Specifies the IP address or fully qualified domain name of the HTTP proxy server. • **Port** — Limits access through the specified port. • **Exclude these addresses** — Don't use the HTTP proxy server for websites or IP addresses that begin with the specified entries. Click **Add**, then enter the address name to exclude. **Best practice:** Exclude the McAfee GTI addresses from the proxy server. For information, see KB79640 and KB84374.
	Enable HTTP proxy authentication	Specifies that the HTTP proxy server requires authentication. (This option is available only when you select an HTTP proxy server.) Enter HTTP proxy credentials: • **User name** — Specifies the user account with permissions to access the HTTP proxy server. • **Password** — Specifies the password for **User name**. • **Confirm password** — Confirms the specified password.
Default Client Update	**Enable the Update Now button in the client**	Displays or hides the **Update Now** button on the main page of the Endpoint Security Client. Click this button to manually check for and download updates to content files and software components on the client system.

Table 2-4 Advanced options *(continued)*

Section	Option	Definition
	What to update	Specifies what to update when the **Update Now** button is clicked. • **Security content, hotfixes, and patches** — Updates all security content (including engine and AMCore and Exploit Prevention content), as well as any hotfixes and patches, to the latest versions. • **Security content** — Updates security content only. (Default) • **Hotfixes and patches** — Updates hotfixes and patches only.
Source Sites for Updates		Configures sites from which to get updates to content files and software components. You can enable and disable the default backup source site, **McAfeeHttp**, and the management server (for managed systems), but you can't otherwise modify or delete them.
		Indicates elements that can be moved in the list. Select elements, then drag and drop to the new location. A blue line appears between elements where you can drop the dragged elements.
	Add	Adds a site to the source site list.
	Double-click an item	Changes the selected item.
	Delete	Deletes the selected site from the source site list.
	Import	Imports sites from a source site list file. Select the file to import, then click **OK**.  The site list file replaces the existing source site list.
	Export All	Exports the source site list to the SiteList.xml file. Select the location to save the source site list file to, then click **OK**.
Proxy server for Source Sites	**No proxy server**	Specifies that the managed systems retrieve McAfee GTI reputation information directly over the Internet directly, not through a proxy server. (Default)
	Use system proxy settings	Specifies to use the proxy settings from the client system, and optionally enable HTTP or FTP proxy authentication.

Table 2-4 Advanced options *(continued)*

Section	Option	Definition
	Configure proxy server	Customizes proxy settings. • **HTTP/FTP address** — Specifies the DNS, IPv4, or IPv6 address of the HTTP or FTP proxy server. • **Port** — Limits access through the specified port. • **Exclude these addresses** — Specifies the addresses for Endpoint Security Client systems that you don't want to use the proxy server for obtaining McAfee GTI ratings. Click **Add**, then enter the address name to exclude.
	Enable HTTP/FTP proxy authentication	Specifies that the HTTP or FTP proxy server requires authentication. (This option is available only when you have selected an HTTP or FTP proxy server.) Enter proxy credentials: • **User name** — Specifies the user account with permissions to access the proxy server. • **Password** — Specifies the password for the specified **User name**. • **Confirm password** — Confirms the specified password.

See also

Protect Endpoint Security resources on page 29
Configure logging settings on page 30
Control access to the client interface on page 31
Configure proxy server settings for McAfee GTI on page 32
Configure the default behavior for updates on page 35
Configure source sites for updates on page 33
Add Site or Edit Site on page 46

Add Site or Edit Site

Adds or edits a site in the source site list.

Table 2-5 Option definitions

Option	Definition
Name	Indicates the name of the source site containing the update files.
Enable	Enables or disables use of the source site for downloading update files.
Retrieve files from	Specifies where to retrieve the files from.

Table 2-5 Option definitions *(continued)*

Option	Definition
HTTP repository	Retrieves files from the designated HTTP repository location.  HTTP offers updating independent of network security, but supports higher levels of concurrent connections than FTP. **URL** • **DNS name** — Indicates that the URL is a domain name. • **IPv4** — Indicates that the URL is an IPv4 address. • **IPv6** — Indicates that the URL is an IPv6 address. **http://** — Specifies the address of the HTTP server and folder where the update files are located. **Port** — Specifies the port number for the HTTP server. **Use authentication** Selects to use authentication and specifies the credentials for accessing the update file folder. • **User name** — Specifies the user account with read permissions to the update file folder. • **Password** — Specifies the password for the specified **User name**. • **Confirm password** — Confirms the specified password.

Table 2-5 Option definitions *(continued)*

Option	Definition
FTP repository	Retrieves files from the designated FTP repository location. An FTP site offers flexibility of updating without having to adhere to network security permissions. Because FTP has been less prone to unwanted code attach than HTTP, it might offer better tolerance. **URL** • **DNS name** — Indicates that the URL is a domain name. • **IPv4** — Indicates that the URL is an IPv4 address. • **IPv6** — Indicates that the URL is an IPv6 address. **ftp://** — Specifies the address of the FTP server and folder where the update files are located. **Port** — Specifies the port number for the FTP server. **Use anonymous login** Selects to use anonymous FTP to access the update file folder. Deselect this option to specify access credentials. • **User name** — Specifies the user account with read permissions to the update file folder. • **Password** — Specifies the password for the specified **User name**. • **Confirm password** — Confirms the specified password.
UNC path or **Local path**	Retrieves files from the designated UNC or local path location. A UNC site is the quickest and easiest to set up. Cross-domain UNC updates require security permissions for each domain, which makes update configuration more involved. **Path** • **UNC path** — Specifies the path using UNC notation (\\servername\path\). • **Local path** — Specifies the path of a folder on a local or network drive. **Use logged on account** Accesses the update files using the logged on account. This account must have read permissions to the folders containing the update files. Deselect this option to specify access credentials. • **Domain** — Specifies the domain for the user account. • **User name** — Specifies the user account with read permissions to the update file folder. • **Password** — Specifies the password for the specified **User name**. • **Confirm password** — Confirms the specified password.

Common — Tasks

Configure and schedule Endpoint Security Client tasks.

On managed systems, you can't start, stop, or delete **Admin** tasks.

Table 2-6 Options

Section	Option	Definition
Tasks		Indicates the currently defined and scheduled tasks. • **Name** — Name of the scheduled task. • **Feature** — Module or feature that the task is associated with. • **Schedule** — When the task is scheduled to run and if it's disabled. For example, on managed systems, the Default Client Update task schedule might be disabled by the administrator. • **Status** — Status of the last time the task ran: • (no status) — Never run • **Running** — Current running or resumed • **Paused** — Paused by the user (such as a scan) • **Deferred** — Deferred by the user (such as a scan) • **Finished** — Completed running without errors • **Finished (errors)** — Finished running with errors • **Failed** — Failed to complete • **Last Run** — Date and time the task last ran. • **Origin** — Origin of the task: • **McAfee** — Provided by McAfee. • **Admin** — (Managed systems only) Defined by the administrator. • **User** — Defined on the Endpoint Security Client. Depending on the origin, some tasks can't be changed or deleted. For example, the Default Client Update task can only be changed on self-managed systems. **Admin** tasks, defined by the administrator on managed systems, can't be changed or deleted on the Endpoint Security Client.
	Double-click an item	Changes the selected item.
	Add	Creates a scan, update, or mirror task.
	Delete	Deletes the selected task.
	Duplicate	Creates a copy of the selected task.
	Run Now	Runs the selected task. If the task is already running, including paused or deferred, the button changes to **View**. • **Quick Scan** — Opens the **Quick Scan** dialog box and starts the scan. • **Full Scan** — Opens the **Full Scan** dialog box and starts the scan. • **Custom Scan** — Opens the **Custom Scan** dialog box and starts the scan. • **Default Client Update** — Opens the **Update** dialog box and starts the update. • **Update** — Opens the **Custom Update** dialog box and starts the update. • **Mirror** — Opens the **Mirror** dialog box and starts the repository replication. If you run a task before applying changes, Endpoint Security Client prompts you to save the settings.

See also

Run a Full Scan or Quick Scan on page 56
Update content and software manually on page 22
Configure, schedule, and run mirror tasks on page 37
Add Task on page 50

Add Task

Adds custom scan, mirror, or update tasks.

Option	Definition
Name	Specifies the name of the task.
Select task type	Specifies the task type: • **Custom scan** — Configures and schedules a custom scan, such as daily memory scans. • **Mirror** — Replicates the updated content and engine files from the first accessible repository to a mirror site on your network. • **Update** — Configures and schedules an update of the content files, scanning engine, or product.

See also

Add Scan Task or Edit Scan Task on page 50
Add Mirror Task or Edit Mirror Task on page 51
Add Update Task or Edit Update Task on page 51

Add Scan Task or Edit Scan Task

Schedule the Full Scan or Quick Scan task or configure and schedule custom scan tasks that run on the client system.

Table 2-7 Options

Tab	Option	Definition
Settings		Configures scan task settings.
	Name	Indicates the name of the task.
	Options	Configures the On-Demand Scan settings for the scan. You can configure **Full Scan** and **Quick Scan** task settings on self-managed systems only.
Schedule		Enables and schedules the task to run at a specified time.

See also

Configure, schedule, and run scan tasks on page 91
Configure On-Demand Scan settings on page 86
Run a Full Scan or Quick Scan on page 56
Threat Prevention — On-Demand Scan on page 114
Schedule on page 52

Add Update Task or Edit Update Task

Schedules the **Default Client Update** or configures and schedules custom update tasks that run on the client system.

Table 2-8 Options

Tab	Option	Definition
Settings		Configures update task settings.
	Name	Indicates the name of the task.
	What to update	Specifies what to update: • Security content, hotfixes, and patches • Security content • Hotfixes and patches You can configure these settings on self-managed systems only.
Schedule		Enables and schedules the task to run at a specified time. By default, the **Default Client Update** task runs every day at 12:00 midnight and repeats every four hours until 11:59 p.m.

See also

Common — Options on page 40
Configure the default behavior for updates on page 35
Configure, schedule, and run update tasks on page 36
Schedule on page 52

Add Mirror Task or Edit Mirror Task

Configures and schedules mirror tasks.

Table 2-9 Options

Tab	Option	Definition
Settings	**Name**	Indicates the name of the task.
	Mirror location	Specifies the folder to store the repository replicate.
Schedule		Enables and schedules the task to run at a specified time.

See also

Configure, schedule, and run mirror tasks on page 37
Schedule on page 52

Schedule

Schedule scan, update, and mirror tasks.

Table 2-10 Options

Category	Option	Definition
Schedule	**Enable schedule**	Schedules the task to run at a specified time. (Enabled by default) This option must be selected to schedule the task.

	Schedule type	Specifies the interval for running the task.
		• **Daily** — Runs the task every day, at a specific time, on a recurring basis between two times of the day, or a combination of both.
		• **Weekly** — Runs the task weekly:
		  • On a specific weekday, all weekdays, weekends, or a combination of days
		  • At a specific time on the selected days, or on a recurring basis between two times of the selected days
		• **Monthly** — Runs the task monthly on either:
		  • The specified day of the month
		  • The specified days of the week — first, second, third, fourth, or last
		• **Once** — Starts the task on the time and date that you specify.
		• **At system startup** — Runs the task when the system starts.
		• **At login** — Starts the task the next time the user logs on to the system.
		• **Run immediately** — Starts the task immediately.

	Frequency	Specifies the frequency for **Daily** and **Weekly** tasks.
	Run on	Specifies the days of the week for **Weekly**, and **Monthly** tasks.
	Run in	Specifies the months of the year for **Monthly** tasks.
	Only run this task once a day	Runs the task once a day for **At system startup** and **At login** tasks.
	Delay this task by	Specifies the number of minutes to delay before running **At system startup** and **At login** tasks.
	Start date	Specifies the start date for **Daily**, **Weekly**, **Monthly**, and **Once** tasks.
	End date	Specifies the end date for **Daily**, **Weekly**, and **Monthly** tasks.
	Start time	Specifies the time to start the task. • **Run once at that time** — Runs the task once at the specified **Start time**. • **Run at that time, and then repeat until** — Runs the task at the specified **Start time**. Then, starts the task every number of hours/minutes specified by **Start task every** until the specified end time. • **Run at that time, and then repeat for** — Runs the task at the specified **Start time**. Then, starts the task every number of hours/minutes specified by **Start task every** until it has run for the specified amount of time.
Options	**Run this task according to Coordinated Universal Time**	Specifies whether the task schedule runs according to the local time on the managed system or Coordinated Universal Time (UTC).

Table 2-10 Options *(continued)*

Category	Option	Definition
	Stop this task if it runs longer than	Stops the task after the specified number of hours and minutes. If the task is interrupted before completing, the next time the task starts, it resumes where it left off.
	Randomize the task start time by	Specifies that this task runs randomly within the time you specify. Otherwise, this task starts at the scheduled time regardless of whether other client tasks are scheduled to run at the same time.
	Run missed task	Runs the task after the number of minutes specified by **Delay start by** once the managed system restarts.
Account		Specifies the credentials to use for running the task. If no credentials are specified, the task runs as the local system Administrator account.
	User name	Specifies the user account.
	Password	Specifies the password for the specified user account.
	Confirm password	Confirms the password for the specified user account.
	Domain	Specifies the domain for the specified user account.

See also

Add Scan Task or Edit Scan Task on page 50
Add Update Task or Edit Update Task on page 51
Add Mirror Task or Edit Mirror Task on page 51

3 Using Threat Prevention

Threat Prevention checks for viruses, spyware, unwanted programs, and other threats by scanning items on your computer.

Contents

Scan your computer for malware

Scan for malware on your computer by selecting options in the Endpoint Security Client or Windows Explorer.

Tasks

- *Run a Full Scan or Quick Scan* on page 56
  Use Endpoint Security Client to perform a manual Full Scan or Quick Scan on your computer.
- *Scan a file or folder* on page 58
  Right-click in Windows Explorer to immediately scan an individual file or folder that you suspect is infected.

See also

Types of scans on page 55

Types of scans

Endpoint Security provides two types of scans: on-access scans and on-demand scans.

- **On-access scan** — The administrator configures on-access scans to run on managed computers. For self-managed computers, configure the on-access scanner in the **Settings** page.

  Whenever files, folders, and programs are accessed, the on-access scanner intercepts the operation and scans the item, based on criteria defined in the settings.

- **On-demand scan**

Manual The administrator (or user, for self-managed systems) configures predefined or custom on-demand scans that users can run on managed computers.

- Run a predefined on-demand scan at any time from the Endpoint Security Client by clicking Scan System, then selecting a scan type:

  Quick Scan runs a quick check of the areas of the system most susceptible to infection.

  Full Scan performs a thorough check of all areas of the system. (Recommended if you suspect the computer is infected.)

- Scan an individual file or folder at any time from Windows Explorer by right-clicking the file or folder and selecting **Scan for threats** from the pop-up menu.
- Configure and run a custom on-demand scan as administrator from the Endpoint Security Client:

  1 Select **Settings** | **Common** | **Tasks**.

  2 Select the task to run.

  3 Click **Run Now**.

Scheduled The administrator (or user, for self-managed systems) configures and schedules on-demand scans to run on computers.

When a scheduled on-demand scan is about to start, Endpoint Security displays a scan prompt at the bottom of the screen. You can start the scan immediately or defer the scan, if configured.

To configure and schedule the predefined on-demand scans, Quick Scan and Full Scan:

1 **Settings** | **On-Demand Scan** | **Full Scan** tab or **Quick Scan** tab — Configures on-demand scans.

2 **Settings** | **Common** | **Tasks** — Schedules on-demand scans.

See also

Configure, schedule, and run scan tasks on page 91
Respond to a scan prompt on page 21

Run a Full Scan or Quick Scan

Use Endpoint Security Client to perform a manual Full Scan or Quick Scan on your computer.

Before you begin

The Threat Prevention module must be installed.

The behavior of the **Full Scan** and **Quick Scan** depends on how the settings are configured. With administrator credentials, you can modify and schedule these scans in the **On-Demand Scan** settings.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click Scan System.

3 On the **Scan System** page, click **Scan Now** for the scan you want to run.

Full Scan	Performs a thorough check of all areas of your system (recommended if you suspect your computer is infected).
Quick Scan	Runs a quick check of the areas of your system most susceptible to infection.

If a scan is already in progress, the **Scan Now** button changes to **View Scan**.

You might also see the **View Detections** button for the on-access scanner, depending on how settings are configured and whether a threat has been detected. Click this button to open the **On-Access Scan** page to manage detections at any time.

Endpoint Security Client displays the status of the scan on a new page.

Best practice: The AMCore content creation date indicates the last time the content was updated. If the content is more than two days old, update your protection before running the scan.

4 Click buttons at the top of the status page to control the scan.

Pause Scan	Pauses the scan before it completes.
Resume Scan	Resumes a paused scan.
Cancel Scan	Cancels a running scan.

5 When the scan completes, the page displays the number of files scanned, time elapsed, and any detections.

Detection Name	Identifies the name of the detected malware.
Type	Displays the threat type.
File	Identifies the infected file.
Action Taken	Describes the last security action taken on the infected file: • **Access Denied** • **Cleaned** • **Deleted** • **None**

The on-demand scan detection list is cleared when the next on-demand scan starts.

6 Select a detection in the table, then click **Clean** or **Delete** to clean or delete the infected file.

Depending on the threat type and scan settings, these actions might not be available.

7 Click **Close** to close the page.

See also

Types of scans on page 55
Detection names on page 61
Update content and software manually on page 22
Manage threat detections on page 59
Configure On-Demand Scan settings on page 86
Configure, schedule, and run scan tasks on page 91

Scan a file or folder

Right-click in Windows Explorer to immediately scan an individual file or folder that you suspect is infected.

Before you begin

The Threat Prevention module must be installed.

The behavior of the **Right-Click Scan** depends on how the settings are configured. With administrator credentials, you can modify these scans in the **On-Demand Scan** settings.

Task

1 In Windows Explorer, right-click the file or folder to scan and select **Scan for threats** from the pop-up menu.

Endpoint Security Client displays the status of the scan in the **Scan for threats** page.

2 Click buttons at the top of the page to control the scan.

Pause Scan	Pauses the scan before it completes.
Resume Scan	Resumes a paused scan.
Cancel Scan	Cancels a running scan.

3 When the scan completes, the page displays the number of files scanned, time elapsed, and any detections.

Detection Name	Identifies the name of the detected malware.
Type	Displays the threat type.
File	Identifies the infected file.
Action Taken	Describes the last security action taken on the infected file: • **Access Denied** • **Cleaned** • **Deleted** • **None**

The on-demand scan detection list is cleared when the next on-demand scan starts.

4 Select a detection in the table, then click **Clean** or **Delete** to clean or delete the infected file.

Depending on the threat type and scan settings, these actions might not be available.

5 Click **Close** to close the page.

See also

Types of scans on page 55
Detection names on page 61
Configure On-Demand Scan settings on page 86

Manage threat detections

Depending on how settings are configured, you can manage threat detections from Endpoint Security Client.

Before you begin

The Threat Prevention module must be installed.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Scan Now** to open the **Scan System** page.

3 From **On-Access Scan**, click **View Detections**.

This option isn't available if the list contains no detections or the user messaging option is disabled.

The on-access scan detection list is cleared when the Endpoint Security service restarts or the system reboots.

4 From the **On-Access Scan** page, select one of these options.

Clean Attempts to clean the item (file, registry entry) and place it in the Quarantine.

Endpoint Security uses information in the content files to clean files. If the content file has no cleaner or the file has been damaged beyond repair, the scanner and denies access to it. In this case, McAfee recommends that you delete the file from the Quarantine and restore it from a clean backup copy.

Delete Deletes the item that contains the threat.

Remove Entry Removes the entry from the detection list.

Close Closes the scan page.

If an action isn't available for the threat, the corresponding option is disabled. For example, **Clean** isn't available if the file has already been deleted.

The on-access scan detection list is cleared when the Endpoint Security service restarts or the system reboots.

Manage quarantined items

Endpoint Security saves items that are detected as threats in the Quarantine. You can perform actions on quarantined items.

Before you begin

The Threat Prevention module must be installed.

For example, you might be able to restore an item after downloading a later version of the content that contains information that cleans the threat.

Quarantined items can include various types of scanned objects, such as files, registries, or anything that Endpoint Security scans for malware.

Task

For help, from the **Action** menu, select **Help**.

1 Open the Endpoint Security Client.

2 Click **Quarantine** on the left side of the page.

The page shows any items in the Quarantine.

If the Endpoint Security Client can't reach the Quarantine Manager, it displays a communication error message. In this case, restart the system to view the Quarantine page.

3 Select an item from the top pane to display the details in the bottom pane.

To...	Do this
Change the relative sizes of the panes.	Click and drag the sash widget between the panes.
Sort items in the table by threat name or type.	Click the table column heading.

4 On the **Quarantine** page, perform actions on selected items.

To...	Follow these steps
Delete items from the quarantine.	Select items, click **Delete**, then click **Delete** again to confirm. Deleted items can't be restored.
Restore items from the quarantine.	Select items, click **Restore**, then click **Restore** again to confirm. Endpoint Security restores items to the original location and removes them from the quarantine. If an item is still a valid threat, Endpoint Security returns it to the quarantine the next time the item is accessed.
Rescan items.	Select items, then click **Rescan**. For example, you might rescan an item after updating your protection. If the item is no longer a threat, you can restore the item to its original location and remove it from the quarantine.
View an item in the Event Log.	Select an item, then click the **View in Event Log** link in the details pane. The **Event Log** page opens, with the event related to the selected item highlighted.
Get more information about a threat.	Select an item, then click the **Learn more about this threat** link in the details pane. A new browser window opens to the McAfee Labs website with more information about the threat that caused the item to be quarantined.

See also

Detection names on page 61
Rescanning quarantined items on page 62
Open the Endpoint Security Client on page 19
Update content and software manually on page 22

Detection names

The Quarantine reports threats by detection name.

Detection name	Description
Adware	Generates revenue by displaying advertisements targeted at the user. Adware earns revenue from either the vendor or the vendor's partners. Some types of adware can capture or transmit personal information.
Dialer	Redirects Internet connections to a party other than the user's default ISP. Dialers are designed to add connection charges for a content provider, vendor, or other third party.
Joke	Claims to harm a computer, but has no malicious payload or use. Jokes don't affect security or privacy, but might alarm or annoy a user.
Keylogger	Intercepts data between the user entering it and the intended recipient application. Trojan horse and potentially unwanted program keylogger might be functionally identical. McAfee software detects both types to prevent privacy intrusions.
Password Cracker	Enables a user or administrator to recover lost or forgotten passwords from accounts or data files. Used by an attacker, they provide access to confidential information and are a security and privacy threat.
Potentially unwanted program	Includes often legitimate software (non-malware) that might alter the security state or privacy posture of the system. This software can be downloaded with a program that the user wants to install. It can include spyware, adware, keylogger, password crackers, hacker tools, and dialer applications.
Remote Admin Tool	Gives an administrator remote control of a system. These tools can be a significant security threat when controlled by an attacker.
Spyware	Transmits personal information to a third party without the user's knowledge or consent. Spyware exploits infected computers for commercial gain by: • Delivering unsolicited pop-up advertisements • Stealing personal information, including financial information, such as credit card numbers • Monitoring web-browsing activity for marketing purposes • Routing HTTP requests to advertising sites See also Potentially unwanted program.
Stealth	Is a type of virus that attempts to avoid detection from anti-virus software. Also known as *interrupt interceptor*. Many stealth viruses intercept disk-access requests. When an anti-virus application tries to read files or boot sectors to find the virus, the virus shows a "clean" image of the requested item. Other viruses hide the actual size of an infected file and display the size of the file before infection.

Detection name	Description
Trojan horse	Is a malicious program that pretends to be a benign application. A trojan doesn't replicate but causes damage or compromises the security of your computer. Typically, a computer becomes infected: • When a user opens a trojan attachment in email. • When a user downloads a trojan from a website. • Peer-to-peer networking. Because they don't replicate themselves, trojans aren't considered viruses.
Virus	Attaches to disks or other files and replicates itself repeatedly, typically without user knowledge or permission. Some viruses attach to files, so when the infected file executes, the virus also executes. Other viruses reside in a computer's memory and infect files as the computer opens, modifies, or creates files. Some viruses exhibit symptoms, while others damage files and computer systems.

Rescanning quarantined items

When rescanning items in the quarantine, Endpoint Security uses scan settings designed to provide maximum protection.

Best practice: Always rescan items in the quarantine before restoring them. For example, you might rescan an item after updating your protection. If the item is no longer a threat, you can restore the item to its original location and remove it from the quarantine.

Between when a threat was originally detected and the rescan performed, scanning conditions can change, which can affect the detection of quarantined items.

When rescanning quarantined items, Endpoint Security always:

- Scans MIME-encoded files.
- Scans compressed archive files.
- Forces a McAfee GTI lookup on items.
- Sets the McAfee GTI sensitivity level to **Very high**.

Even using these scan settings, the quarantine rescan might fail to detect a threat. For example, if the item's metadata (path or registry location) changes, rescanning might produce a false positive even though the item is still infected.

Managing Threat Prevention

As administrator, you can specify Threat Prevention settings to prevent threat access and configure scans.

For managed systems, policy changes from McAfee ePO might overwrite changes from the Settings page.

Configuring exclusions

Threat Prevention enables you to fine-tune your protection by specifying items to exclude.

For example, you might need to exclude some file types to prevent a scanner from locking a file used by a database or server. A locked file can cause the database or server to fail or generate errors.

Best practice: To improve performance of on-access and on-demand scans, use scan avoidance techniques rather than adding file and folder exclusions.

Exclusions in exclusion lists are mutually exclusive. Each exclusion is evaluated separately from the others in the list.

To exclude a folder on Windows systems, append a backslash (\) character to the path.

For this feature...	Specify items to exclude	Where to configure	Exclude items by	Use wildcards?
Access Protection	Processes (for all rules or a specified rule)	**Access Protection**	Process file name or path, MD5 hash, or signer	All except MD5 hash
Exploit Prevention	Processes	**Exploit Prevention**	Process file name or path, MD5 hash, or signer	All except MD5 hash
	Caller modules		Caller module file name or path, MD5 hash, or signer	
	APIs		API name	
	Signatures		Signature ID	No
All scans	Detection names	Threat Prevention **Options**	Detection name (case-sensitive)	Yes
	Potentially unwanted programs		Name	Yes
On-access scan • **Default** • **High Risk** • **Low Risk**	Files, file types, and folders	**On-Access Scan**	File name or folder, file type, or file age	Yes
	ScriptScan URLs		URL name	No
On-demand scan • **Quick Scan** • **Full Scan** • **Right-Click Scan**	Files, folders, and drives	**On-Demand Scan**	File name or folder, file type, or file age	Yes
Custom on-demand scan	Files, folders, and drives	**Common** | **Tasks** | **Add Task** | **Custom scan**	File name or folder, file type, or file age	Yes

See also

Wildcards in exclusions on page 64

Wildcards in exclusions

You can use wildcards to represent characters in exclusions for files, folders, detection names, and potentially unwanted programs.

Table 3-1 Valid wildcards

Wildcard character	Name	Represents
?	Question mark	Single character. This wildcard applies only if the number of characters matches the length of the file or folder name. For example: The exclusion W?? excludes WWW, but doesn't exclude WW or WWWW.
*	Asterisk	Multiple characters, except backslash (\). *\ at the beginning of a file path is not valid. Use **\ instead. For example: **\ABC*.
**	Double asterisk	Zero or more of any characters, including backslash (\). This wildcard matches zero or more characters. For example: C:\ABC**\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\XYZ.

Wildcards can appear in front of a backslash (\) in a path. For example, C:\ABC*\XYZ matches C:\ABC\DEF\XYZ.

Root-level exclusions

Threat Prevention requires an absolute path for root-level exclusions. This means that you can't use leading \ or ?:\ wildcard characters to match drive names at the root level.

This behavior differs from VirusScan Enterprise. See the *McAfee Endpoint Security Migration Guide*.

With Threat Prevention, you can use leading **\ wildcard characters in root-level exclusions to match drives *and* subfolders. For example, **\test matches the following:

C:\test

D:\test

C:\temp\test

D:\foo\test

Protecting your system access points

The first line of defense against malware is to protect client system access points from threat access. *Access Protection* prevents unwanted changes to managed computers by restricting access to specified files, shares, and registry keys, registry values, processes, and services.

Access Protection uses both McAfee-defined rules and user-defined rules (also called custom rules) to report or block access to items. Access Protection compares a requested action against the list of rules and acts according to the rule.

Access Protection must be enabled to detect attempts to access files, shares, registry keys, registry values, processes, and services.

How threats gain access

Threats gain access to your system using various access points.

Access point	Description
Macros	As part of word-processing documents and spreadsheet applications.
Executable files	Seemingly benign programs can include viruses with the expected program. Some common file extensions are .EXE, .COM, .VBS, .BAT, .HLP and .DLL.
Scripts	Associated with webpages and email, scripts such as ActiveX and JavaScript, if allowed to run, can include viruses.
Internet Relay Chat (IRC) messages	Files sent with these messages can easily contain malware as part of the message. For example, automatic startup processes can contain worms and trojan threats.
Browser and application Help files	Downloading these Help files exposes the system to embedded viruses and executables.
Email	Jokes, games, and images as part of email messages with attachments.
Combinations of all these access points	Sophisticated malware creators combine all these delivery methods and even embed one piece of malware within another to try to access the managed computer.

How Access Protection stops threats

Access Protection stops potential threats by managing actions based on McAfee-defined and user-defined protection rules.

Threat Prevention follows this basic process to provide Access Protection.

When a threat occurs

When a user or process acts:

1. Access Protection examines the action according to the defined rules.
2. If the action breaks a rule, Access Protection manages the action using the information in the configured rules.
3. Access Protection updates the log file and generates and sends an event to the management server, if managed.

Example of an access threat

1. A user downloads a legitimate program (not malware), MyProgram.exe, from the Internet.
2. The user launches MyProgram.exe and the program seems to launch as expected.
3. MyProgram.exe launches a child process called AnnoyMe.exe.
4. AnnoyMe.exe attempts to modify the operating system to make sure that AnnoyMe.exe always loads on startup.
5. Access Protection processes the request and matches the action against an existing block and report rule.
6. Access Protection prevents AnnoyMe.exe from modifying the operating system and logs the details of the attempt. Access Protection also generates and sends an alert to the management server.

About Access Protection rules

Use McAfee-defined and user-defined Access Protection rules to protect your system’s access points.

McAfee-defined rules are always applied before any user-defined rules.

Rule type	Description
McAfee-defined rules	• These rules prevent modification of commonly used files and settings. • You can enable, disable, and change the configuration of McAfee-defined rules, but you can't delete these rules.
User-defined rules	• These rules supplement the protection provided by McAfee-defined rules. • An empty **Executables** table indicates that the rule applies to all executables. • An empty **User Names** table indicates that the rule applies to all users. • You can add and delete, as well as enable, disable, and change the configuration of these rules.

Exclusions

At the rule level, exclusions and inclusions apply to the specified rule. At the policy level, exclusions apply to all rules. Exclusions are optional.

See also

Exclude processes from Access Protection on page 72

Configure McAfee-defined Access Protection rules

McAfee-defined rules prevent users from modifying commonly used files and settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

You can:

- Change the block and report settings for these rules.
- Add excluded and included executables to these rules.

You can't:

- Delete these rules.
- Modify the files and settings protected by these rules.
- Add subrules or user names to these rules.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Threat Prevention** on the main **Status** page.

Or, from the **Action** menu , select **Settings**, then click **Threat Prevention** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **Access Protection**.

5 Modify the rule:

a In the **Rules** section, select **Block**, **Report**, or both for the rule.

- To block or report all, select **Block** or **Report** in the first row.
- To disable the rule, deselect both **Block** and **Report**.

b Double-click a McAfee-defined rule to edit.

c On the **Edit McAfee-defined Rule** page, configure the settings.

d In the **Executables** section, click **Add**, configure the settings, then click **Save** twice to save the rule.

6 Click **Apply** to save your changes or click **Cancel**.

See also

McAfee-defined Access Protection rules on page 67
Log on as administrator on page 26
Exclude processes from Access Protection on page 72

McAfee-defined Access Protection rules

Use McAfee-defined Access Protection rules to protect your computer from unwanted changes.

McAfee-defined rule	Description
Browsers launching files from the Downloaded Program Files folder	Prevents software from installing through the web browser. Because this rule might also block the installation of legitimate software, install the application before enabling this rule or add the installation process as an exclusion. This rule is set to **Report** by default. This rule prevents adware and spyware from installing and running executables from this folder.
Changing any file extension registrations	Protects the registry keys under HKEY_CLASSES_ROOT where file extensions are registered. This rule prevents malware from changing the file extension registrations to allow malware to execute silently. **Best practice:** Disable this rule when installing valid applications that change file extension registrations in the registry. This rule is a more restrictive alternative to **Hijacking .EXE and other executable extensions**.
Changing user rights policies	Protects registry values that contain Windows security information. This rule prevents worms from changing accounts that have administrator rights.
Creating new executable files in the Program Files folder	Prevents the creation new executable files in the Program Files folder. This rule prevents adware and spyware from creating new .EXE and .DLL files and installing new executable files in the Program Files folder. **Best practice:** Install applications before enabling this rule, or place the blocked processes in the exclusion list.

McAfee-defined rule	Description
Creating new executable files in the Windows folder	Prevents the creation of files from any process, not just from over the network. This rule prevents the creation of .EXE and .DLL files in the Windows folder.  **Best practice:** Add processes that must place files in the Windows folder to the exclusion list.
Disabling Registry Editor and Task Manager	Protects Windows registry entries, preventing disabling the registry editor and Task Manager.  In an outbreak, disable this rule to be able to change the registry, or open Task Manager to stop active processes.
Executing scripts by Windows script host (CScript.exe or Wscript.exe) from common user folders	Prevents the Windows scripting host from running VBScript and JavaScript scripts in any folder with "temp" in the folder name. This rule protects against many trojans and questionable web installation mechanisms used by adware and spyware applications. This rule might block legitimate scripts and third-party applications from being installed or run.
Hijacking .EXE or other executable extensions	Protects .EXE, .BAT, and other executable registry keys under HKEY_CLASSES_ROOT. This rule prevents malware from changing registry keys to run the virus when another executable runs. This rule is a less restrictive alternative to **Changing any file extension registrations**.
Installing Browser Helper Objects or Shell Extensions	Prevents adware, spyware, and trojans that install as Browser Helper Objects from installing on to the host computer. This rule prevents adware and spyware from installing on systems.  **Best practice:** Allow legitimate custom or third-party applications to install these objects by adding them to the exclusion list. After installation, you can re-enable the rule because it doesn't prevent installed Browser Helper Objects from working.
Installing new CLSIDs, APPIDs, and TYPELIBs	Prevents the installation or registration of new COM servers. This rule protects against adware and spyware programs that install themselves as a COM add-on Internet Explorer or Microsoft Office applications.  **Best practice:** Allow legitimate applications that register COM add-ons, including some common applications like Adobe Flash by adding them to the exclusion list.
Modifying core Windows processes	Prevents files from being created or executed with the most commonly spoofed names. This rule prevents viruses and trojans from running with the name of a Windows process. This rule excludes authentic Windows files.
Modifying Internet Explorer settings	Blocks processes from changing settings in Internet Explorer. This rule prevents start-page trojans, adware, and spyware from changing browser settings, such as changing the start page or installing favorites.

McAfee-defined rule	Description
Modifying network settings	Prevents processes that aren't listed in the exclusion list from changing a system's network settings. This rule protects against Layered Service Providers that transmit data, like your browsing behavior, by capturing network traffic and sending it to third-party sites.  **Best practice:** Add processes that must change network settings to the exclusion list or disable the rule while changes are made.
Registering of programs to autorun	Blocks adware, spyware, trojans, and viruses from trying to register themselves to load every time a system is restarted. This rule prevents processes that aren't on the excluded list from registering processes that execute each time a system restarts.  **Best practice:** Add legitimate applications to the exclusion list, or install them before this rule is enabled.
Remotely accessing local files or folders	Prevents read and write access from remote computers to the computer. This rule prevents a share-hopping worm from spreading. In a typical environment, this rule is suitable for workstations, but not servers, and is only useful when computers are actively under attack. If a computer is managed by pushing files to it, this rule prevents updates or patches from being installed. This rule doesn't affect the management functions of McAfee ePO.
Remotely creating autorun files	Prevents other computers from making a connection and creating or changing autorun (autorun.inf) files. Autorun files are used to automatically start program files, typically setup files from CDs. This rule prevents spyware and adware distributed on CDs from being executed. This rule is selected to **Block** and **Report** by default.
Remotely creating or modifying files or folders	Blocks write access to all shares. This rule is useful in an outbreak by preventing write access to limit the spread of infection. The rule blocks malware that would otherwise severely limit use of the computer or network. In a typical environment, this rule is suitable for workstations, but not servers, and is only useful when computers are actively under attack. If a computer is managed by pushing files to it, this rule prevents updates or patches from being installed. This rule doesn't affect the management functions of McAfee ePO.
Remotely creating or modifying Portable Executable, .INI, .PIF file types, and core system locations	Prevents other computers from making a connection and changing executables, such as files in the Windows folder. This rule affects only file types that viruses typically infect. This rule protects against fast spreading worms or viruses, which traverse a network through open or administrative shares.

McAfee-defined rule	Description
Running files from common user folders	Blocks any executable from running or starting from any folder with "temp" in the folder name. This rule protects against malware that is saved and run from the user or system temp folder. Such malware might include executable attachments in email and downloaded programs. Although this rule provides the most protection, it might block legitimate applications from being installed.
Running files from common user folders by common programs	Blocks applications from installing software from the browser or from the email client. This rule prevents email attachments and executables from running on webpages. **Best practice:** To install an application that uses the Temp folder, add the process to the exclusion list.

See also

Configure McAfee-defined Access Protection rules on page 66

Configure user-defined Access Protection rules

User-defined rules supplement the protection provided by McAfee-defined rules. You can add and delete, as well as enable, disable, and change the configuration of these rules.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Best practice: For information about creating Access Protection rules to protect against ransomware, see PD25203.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Threat Prevention** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Access Protection**.
5. Create the rule: In the **Rules** section, click **Add**.

   On the **Add Rule** page, configure the settings.

   a. In the **Executables** section, click **Add**, configure executable properties, then click **Save**.

      An empty **Executables** table indicates that the rule applies to all executables.

   b. In the **User Names** section, click **Add**, then configure user name properties.

      An empty **User Names** table indicates that the rule applies to all users.

c In the **Subrules** section, click **Add**, then configure subrule properties.

Best practice: To avoid impacting performance, don't select the **Read** operation.

In the **Targets** section, click **Add**, configure target information, then click **Save** twice.

6 In the **Rules** section, select **Block**, **Report**, or both for the rule.

- To block or report all, select **Block** or **Report** in the first row.
- To disable the rule, deselect both **Block** and **Report**.

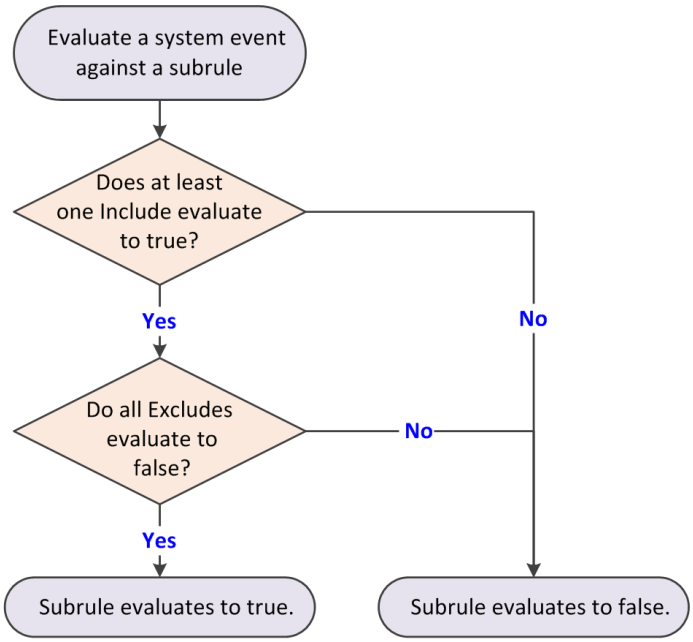
7 Click **Apply** to save your changes or click **Cancel**.

See also

Exclude processes from Access Protection on page 72

How targets in Access Protection subrules are evaluated

Each target is added with an Include or Exclude directive.



When evaluating a system event against a subrule, the subrule evaluates to *true* if:

- At least one *Include* evaluates to *true*.

  and

- All *Excludes* evaluate to *false*.

Exclude takes precedence over Include. Here are examples:

- If a single subrule both includes and excludes a file C:\marketing\jjohns, the subrule does not trigger for that file.
- If a subrule includes *all* files but excludes the file C:\marketing\jjohns, the subrule triggers if the file is not C:\marketing\jjohns.
- If a subrule includes file C:\marketing* but excludes C:\marketing\jjohns, the subrule triggers for C:\marketing\anyone, but doesn't trigger for C:\marketing\jjohns.

Exclude processes from Access Protection

If a trusted program is blocked, exclude the process by creating a policy-based or rule-based exclusion.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Threat Prevention** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **Access Protection**.

5 Verify that Access Protection is enabled.

6 Perform one of the following:

To...	Do this...
Exclude processes from all rules.	1 In the **Exclusions** section, click **Add** to add processes to exclude from all rules. 2 On the **Add Executable** page, configure the executable properties. 3 Click **Save**, then click **Apply** to save the settings.
Specify processes for inclusion or exclusion in a user-defined rule.	1 Edit an existing user-defined rule or add a rule. 2 On the **Add Rule** or **Edit Rule** page, in the **Executables** section, click **Add** to add an executable to exclude or include. 3 On the **Add Executable** page, configure the executable properties, including whether to include or exclude the executable. 4 Click **Save** twice, then click **Apply** to save the settings.

Blocking buffer overflow exploits

Exploit Prevention stops exploited buffer overflows from executing arbitrary code. This feature monitors user-mode API calls and recognizes when they are called as a result of a buffer overflow.

When a detection occurs, information is recorded in the activity log, displayed on the client system, and sent to the management server, if configured.

Threat Prevention uses the Exploit Prevention content file to protect applications such as Microsoft Internet Explorer, Microsoft Outlook, Outlook Express, Microsoft Word, and MSN Messenger.

Host Intrusion Prevention 8.0 can be installed on the same system as Endpoint Security version 10.5. If McAfee Host IPS is enabled, Exploit Prevention is disabled even if enabled in the policy settings.

How buffer overflow exploits occur

Attackers use buffer overflow exploits to run executable code by overflowing the fixed-size memory buffer reserved for an input process. This code allows the attacker to take over the target computer or compromise its data.

A large percentage of malware attacks are buffer overflow attacks that try to overwrite adjacent memory in the stack frame.

The two types of buffer overflow exploits are:

- *Stack-based attacks* use the stack memory objects to store user input (most common).
- *Heap-based attacks* flood the memory space reserved for a program (rare).

The fixed-size stack memory object is empty and waiting for user input. When a program receives input from the user, the data is stored on top of the stack and assigned a return memory address. When the stack is processed, the user's input is sent to the return address specified by the program.

The following process describes a stack-based buffer overflow attack:

1 **Overflow the stack.**

When the program is written, a specific amount of memory space is reserved for the data. The stack overflows if the data written is larger than the space reserved for it in the memory stack. This situation is only a problem when combined with malicious input.

2 **Exploit the overflow.**

The program waits for input from the user. If the attacker enters an executable command that exceeds the stack size, that command is saved outside the reserved space.

3 **Run the malware.**

The command doesn't automatically run when it exceeds the stack buffer space. Initially, the program starts to crash because of the buffer overflow. If the attacker provided a return memory address that references the malicious command, the program tries to recover by using the return address. If the return address is valid, the malicious command is executed.

4 **Exploit the permissions.**

The malware now runs with the same permissions as the application that was compromised. Because programs usually run in kernel mode or with permissions inherited from a service account, the attacker can now gain full control of the operating system.

Signatures and how they work

Exploit Prevention *signatures* are collections of rules that compare behavior against known attacks and perform an action when a match is detected. McAfee delivers signatures in Exploit Prevention content updates.

Signatures protect specific applications, which are defined in the Application Protection Rules list. When an attack is detected, Exploit Prevention can stop the behavior initiated by the attack.

When the Exploit Prevention content file is updated, the list of signatures is updated if needed.

You can change the action settings of these signatures, but you can't add, delete, or otherwise change these signatures. To protect specific files, shares, registry keys, registry values, processes, and services, create custom Access Protection rules.

Actions

An action is what the Exploit Prevention does when a signature is triggered.

- **Block** — Prevents the operation.
- **Report** — Allows the operation and reports the event.

If neither are selected, the signature is disabled — Exploit Prevention allows the operation and doesn't report the event.

The Exploit Prevention content file automatically sets the action for signatures depending on severity level. You can change the action for a specific signature in the Signatures section of the Exploit Prevention settings. Any changes you make to the signature actions persist through content updates.

Behavioral rules

Behavioral rules block zero-day attacks and enforce proper operating system and application behavior. Heuristic behavioral rules define a profile of legitimate activity. Activity not matching these rules is considered suspicious and triggers a response. For example, a behavioral rule might state that only a web server process can access HTML files. If any other process tries to access HTML files, Exploit Prevention takes the specified action. This type of protection, called *application shielding and enveloping*, prevents applications and their data from being compromised and prevents applications from being used to attack other applications.

Behavioral rules also block buffer overflow exploits, preventing code execution that results from a buffer overflow attack, one of the most common methods of attack.

Severity levels

Each signature has a default severity level, which describes the potential danger of an attack.

- **High** — Signatures that protect against clearly identifiable security threats or malicious actions. Most of these signatures are specific to well-identified exploits and are mostly non-behavioral in nature.

  To prevent exposing systems to exploit attacks, set signatures with a severity of High to **Block** on every host.

- **Medium** — Signatures that are behavioral in nature and prevent applications from operating outside of their environment (relevant for clients protecting web servers and Microsoft SQL Server 2000).

  Best practice: On critical servers, set signatures with a severity of Medium to **Block** after fine-tuning.

- **Low** — Signatures that are behavioral in nature and shield applications. Shielding means locking down application and system resources so that they can't be changed.

  Setting signatures with a severity of Low to **Block** increases the security of the system, but requires additional tuning.

- **Informational** — Indicates a change to the system configuration that might create a benign security risk or an attempt to access sensitive system information. Events at this level occur during normal system activity and generally aren't evidence of an attack.

- **Disabled** — Lists signatures that are disabled in the Exploit Prevention content file.

  You can't enable signatures with a severity of Disabled.

Application protection rules and how they work

Application protection rules define the executables that are monitored for Exploit Prevention signatures. If an executable isn't included in the list, it isn't monitored.

Exploit Prevention signatures include two classes:

- **Buffer Overflow signatures** provide memory protection by monitoring the memory space that the processes use.
- **API signatures** monitor API calls between the processes running in user mode and the kernel.

The Exploit Prevention content provided by McAfee includes a list of applications that are protected. Threat Prevention displays these applications in the Application Protection Rules section of the Exploit Prevention settings.

To keep protection current, updates to Exploit Prevention content replace the McAfee-defined application protection rules in the **Exploit Prevention** settings with the latest application protection rules.

You can enable, disable, delete, and change the inclusion status of McAfee-defined application protection rules. In addition, you can create and duplicate your own application protection rules. Any changes you make to these rules persist through content updates.

If the list includes conflicting application protection rules, rules with the Inclusion Status of Exclude take precedence over Include.

Endpoint Security Client displays the complete list of protected applications, not just the applications currently running on the client system. This behavior is different from McAfee Host IPS.

For managed systems, application protection rules created in the Endpoint Security Client are not sent to McAfee ePO and might be overwritten when the administrator deploys an updated policy.

Configure Exploit Prevention settings

To prevent applications from executing arbitrary code on the client system, configure the Exploit Prevention exclusions, McAfee-defined signatures, and application protection rules.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

You can set the action for McAfee-defined signatures. You can enable, disable, delete, and change the inclusion status of McAfee-defined application protection rules.You can also create and duplicate your own application protection rules. Any changes you make to these rules persist through content updates.

For the list of processes protected by Exploit Prevention, see KB58007.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Threat Prevention** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Exploit Prevention**.
5. Configure settings on the page, then click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26

Exclude processes from Exploit Prevention

If a trusted program is blocked, create an exclusion to exclude it from Exploit Prevention. You can exclude the process by process name, caller module, API, or signature ID. You can also create Application Protection rules to include or exclude processes from protection.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Threat Prevention** on the main **Status** page.

Or, from the **Action** menu , select **Settings**, then click **Threat Prevention** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **Exploit Prevention**.

5 Verify that **Exploit Prevention** is enabled.

6 Perform one of the following:

To...	Do this...
Exclude processes from all rules.	1 In the **Exclusions** section, click **Add**. 2 On the **Add Exclusion** page, configure the exclusion properties. 3 Click **Save**, then click **Apply** to save the settings.
Specify processes for inclusion or exclusion in a user-defined Application Protection rule.	1 Edit an existing user-defined rule or add an Application Protection rule. 2 On the **Add Rule** or **Edit Rule** page, in the **Executables** section, click **Add** to add executables to exclude or include. 3 On the **Add Executable** page, configure the executable properties. 4 Click **Save** twice, then click **Apply** to save the settings.

Exploit Prevention exclusions and how they work

A *false positive* occurs when behavior that is a normal part of a user's work routine is interpreted as an attack. To prevent false positives, create an *exclusion* for that behavior.

Exclusions enable you to reduce false positive alerts, minimizing needless data flow and ensuring that alerts are legitimate security threats.

For example, during the process of testing clients, a client recognizes the "Java - Creation of suspicious files in Temp folder" signature. This signature signals that the Java application is trying to create a file in the Windows Temp folder. An event triggered by this signature is cause for alarm, because a Java application might be being used to download malware to the Windows Temp folder. In this instance, you might reasonably suspect that a trojan horse has been planted. But, if the process normally creates files in Temp, for example, saving a file using the Java application, create an exclusion to allow this action.

When an Exploit Prevention violation event occurs, the event includes an associated process and a possible caller module, API, or signature. If you suspect the violation event is a false positive, you can add an exclusion that one or more of these identifiers.

For managed systems, Exploit Prevention exclusions created in the Endpoint Security Client are not sent to McAfee ePO and might be overwritten when the administrator deploys an updated policy. Configure global exclusions in the Exploit Prevention policy in McAfee ePO.

When specifying exclusions, consider the following:

- Each exclusion is independent: multiple exclusions are connected by a logical OR so that if one exclusion matches, the violation event doesn't occur.
- You must specify at least one of Process, Caller Module, API, or Signature.
- Exclusions with Caller Module or API don't apply to DEP.
- For Process exclusions, you must specify at least one identifier: File name or path, MD5 hash, or Signer.
- If you specify more than one identifier, all identifiers apply.
- If you specify more than one identifier and they don't match (for example, the file name and MD5 hash don't apply to the same file), the exclusion is invalid.
- Exclusions are case insensitive.
- Wildcards are allowed for all except MD5 hash.
- If you include signature IDs in an exclusion, the exclusion only applies to the process in the specified signatures. If no signature IDs are specified, the exclusion applies to the process in all signatures.

Detecting potentially unwanted programs

To protect the managed computer from potentially unwanted programs, specify files and programs to detect in your environment, then enable detection.

Potentially unwanted programs are software programs that are annoying or can alter the security state or the privacy policy of the system. Potentially unwanted programs can be embedded in programs that users download intentionally. Unwanted programs might include spyware, adware, and dialers.

1. Specify custom unwanted programs for the on-access and on-demand scanners to detect in the Options settings.
2. Enable unwanted program detection and specify actions to take when detections occur in these settings:
   - On-Access Scan settings
   - On-Demand Scan settings

See also

Specify custom potentially unwanted programs to detect on page 77
Enable and configure potentially unwanted program detection and responses on page 78
Configure On-Access Scan settings on page 80
Configure On-Demand Scan settings on page 86

Specify custom potentially unwanted programs to detect

Specify additional programs for the on-access and on-demand scanners to treat as unwanted programs in the Options settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

The scanners detect the programs you specify as well as programs specified in the AMCore content files.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Threat Prevention** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **Options**.

5 From **Potentially Unwanted Program Detections**:

- Click **Add** to specify the name and optional description of a file or program to treat as a potentially unwanted program.

  The **Description** appears as the detection name when a detection occurs.

- Double-click the name or description of an existing potentially unwanted program to modify.
- Select an existing potentially unwanted program, then click **Delete** to remove it from the list.

See also

Log on as administrator on page 26

Enable and configure potentially unwanted program detection and responses

Enable the on-access and on-demand scanners to detect potentially unwanted programs and specify responses when one is found.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Configure On-Access Scan settings.

a Open the Endpoint Security Client.

b Click **Threat Prevention** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.

c Click **Show Advanced**.

d Click **On-Access Scan**.

e Under **Process Settings**, for each On-Access Scan type, select **Detect unwanted programs**.

f Under **Actions**, configure responses to unwanted programs.

2 Configure On-Demand Scan settings.

   a Open the Endpoint Security Client.

   b Click **Threat Prevention** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.

   c Click **Show Advanced**.

   d Click **On-Demand Scan**.

   e For each scan type (**Full Scan**, **Quick Scan**, and **Right-Click Scan**):

   - Select **Detect unwanted programs**.
   - Under **Actions**, configure responses to unwanted programs.

See also

Configure On-Access Scan settings on page 80
Configure On-Demand Scan settings on page 86
Log on as administrator on page 26

Configure common scan settings

To specify settings that apply to both on-access and on-demand scans, configure the Threat Prevention Options settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

These settings apply to all scans:

- Quarantine location and the number of days to keep quarantined items before automatically deleting them
- Detection names to exclude from scans
- Potentially unwanted programs to detect, such as spyware and adware
- McAfee GTI-based telemetry feedback

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Threat Prevention** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **Options**.

5 Configure settings on the page, then click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26
Configure On-Access Scan settings on page 80
Configure On-Demand Scan settings on page 86

How McAfee GTI works

If you enable McAfee GTI for the on-access or on-demand scanner, the scanner uses heuristics to check for suspicious files.

The scanner submits fingerprints of samples, or *hashes*, to a central database server hosted by McAfee Labs to determine if they are malware. By submitting hashes, detection might be made available sooner than the next content file update, when McAfee Labs publishes the update.

You can configure the sensitivity level that McAfee GTI uses when it determines if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. But, allowing more detections can result in more false positive results. The McAfee GTI sensitivity level is set to Medium by default. Configure the sensitivity level for each scanner in the On-Access Scan and On-Demand Scan settings.

You can configure Endpoint Security to use a proxy server for retrieving McAfee GTI reputation information in the Common settings.

For frequently asked questions about McAfee GTI, see KB53735.

Configure On-Access Scan settings

These settings enable and configure on-access scanning, which includes specifying messages to send when a threat is detected and different settings based on process type.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

See the Help for the Threat Prevention **Options** settings for more scan configuration options.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Threat Prevention** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **On-Access Scan**.
5. Select **Enable On-Access Scan** to enable the on-access scanner and modify options.
6. Specify whether to use Standard settings for all processes, or different settings for high-risk and low-risk processes.
   - **Standard settings** — Configure the scan settings on the **Standard** tab.
   - **Different settings based on process type** — Select the tab (**Standard**, **High Risk**, or **Low Risk**) and configure the scan settings for each process type.
7. Click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26
Configure common scan settings on page 79

Choosing when to scan files with the on-access scanner

You can specify when the on-access scanner examines files: when writing to disk, when reading from disk, or let McAfee decide when to scan.

When writing to disk ("Write scan")

The Write scan option doesn't prevent access to files, either before or after scanning, and so can leave your system vulnerable to attack.

When you select Write scan, the scanner examines the file only after it has been written to disk and closed. A process can perform a Read, Open, or Execute operation on the file before the scanner can perform a Write scan, potentially resulting in infection. Applications might also encounter SHARING_VIOLATION errors if they access the file again after writing it, while a Write scan is in progress.

The on-access scanner examines when files are:

- Created or changed on the local hard drive.
- Copied or moved from a mapped drive to the local hard drive (if the **On network drives** option is also enabled).
- Copied or moved from the local hard drive to a mapped drive (if the **On network drives** option is also enabled).

When reading from disk ("Read scan")

Best practice: Enable the Read scan option to provide security against outbreaks.

When you select Read scan, the scanner prevents access to files unless they are determined to be clean.

The on-access scanner examines when files are:

- Read, opened, or executed from the local hard drive.
- Read, opened, or executed from mapped network drives (if the **On network drives** option is also enabled).

Let McAfee decide

Best practice: Enable this option for the best protection and performance.

When you select this option, the on-access scanner uses *trust logic* to optimize scanning. Trust logic improves your security and boosts performance with *scan avoidance* — avoiding unnecessary scans. For example, McAfee analyzes and considers some programs to be trustworthy. If McAfee verifies that these programs haven't been tampered with, the scanner might perform reduced or optimized scanning.

How on-access scanning works

The on-access scanner integrates with the system at the lowest levels (File-System Filter Driver) and scans files where they first enter the system.

When detections occur, the on-access scanner delivers notifications to the Service Interface.

If you configure McAfee GTI, the scanner uses heuristics to check for suspicious files.

Windows 8 and 10 — If the scanner detects a threat in the path of an installed Windows Store app, the scanner marks it as *tampered*. Windows adds the tampered flag to the tile for the app. When you attempt to run it, Windows notifies you of the problem and directs you to the Windows Store to reinstall.

The scanner uses this criteria to determine whether to scan an item:

- The file extension matches the configuration.
- The file information isn't in the global scan cache.
- The file hasn't been excluded or previously scanned.

Read scan

When Read scan is selected and an attempt is made to read, open, or execute a file:

1. The scanner blocks the request.
2. The scanner determines whether the item must be scanned.
   - If the file doesn't need to be scanned, the scanner unblocks the file, caches the file information, and grants the operation.
   - If the file needs to be scanned, the scan engine scans the file, comparing it to signatures in the currently loaded AMCore content file.
     - If the file is clean, the scanner unblocks the file and caches the result.
     - If the file contains a threat, the scanner denies access to the file and takes the configured action.

       For example, if the action is to clean the file, the scanner:

       1. Uses information in the currently loaded AMCore content file to clean the file.
       2. Records the results in the activity log.
       3. Notifies the user that it detected a threat in the file, and prompts for the action to take (clean or delete the file).

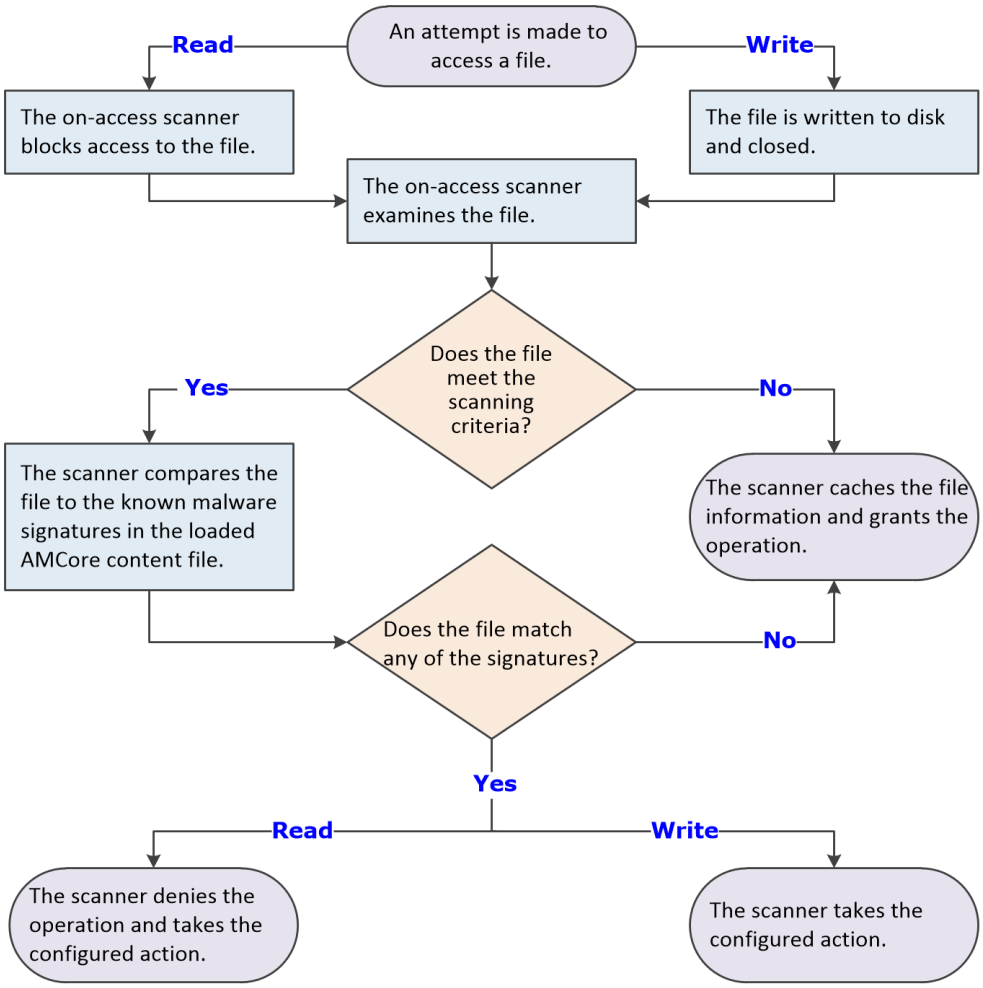
Write scan

The scanner examines the file only after it is written to disk and closed.

When Write scan is selected and a file is written to disk:

1. The scanner determines whether the item must be scanned.
   a. If the file doesn't need to be scanned, the scanner caches the file information, and grants the operation.
   b. If the file needs to be scanned, the scan engine scans the file, comparing it to signatures in the currently loaded AMCore content file.
      - If the file is clean, the scanner caches the result.
      - If the file contains a threat, the scanner takes the configured action.

        The scanner doesn't deny access to the file.



When is the global scan cache flushed?

The on-access scan detection list is cleared when the Endpoint Security service restarts or the system reboots.

Threat Prevention flushes the global scan cache and rescans all files when:

- The On-Access Scan configuration changes.
- An Extra.DAT file is added.
- The system reboots in safe mode.

If the process is signed by a trusted certificate, the signing certificate is cached and remains in the cache after the system reboots. The scanner is less likely to scan files accessed by processes that are signed by a cached trusted certificate, resulting in scan avoidance and improved performance.

Best practices: Reducing the impact of on-access scans on users

To minimize the impact that on-access scans have on a system, select options to avoid impacting system performance and scan only what you need to.

Choose performance options

Some scan options can negatively affect system performance. For this reason, select these options only if you need to scan specific items. Select or deselect these options in the On-Access Scan settings.

- **Scan processes on service startup and content update** — Rescans all processes that are currently in memory each time:
  - You re-enable on-access scans.
  - Content files are updated.
  - The system starts.
  - The McShield.exe process starts.

  Because some programs or executables start automatically when you start your system, deselect this option to improve system startup time.
- **Scan trusted installers** — Scans MSI files (installed by msiexec.exe and signed by McAfee or Microsoft) or Windows Trusted Installer service files.

  Deselect this option to improve the performance of large Microsoft application installers.

Scan only what you need to

Scanning some types of files can negatively affect system performance. For this reason, select these options only if you need to scan specific types of files. Select or deselect these options in the What to Scan section of the On-Access Scan settings.

- **On network drives** — Scans resources on mapped network drives.

  Deselect this option to improve performance.
- **Opened for backups** — Scans files when accessed by backup software.

  For most environments, you don't need to select this setting.
- **Compressed archive files** — Examines the contents of archive (compressed) files, including .jar files.

  Even if an archive contains infected files, the files can't infect the system until the archive is extracted. Once the archive is extracted, the On-Access Scan examines the files and detects any malware.

About ScriptScan

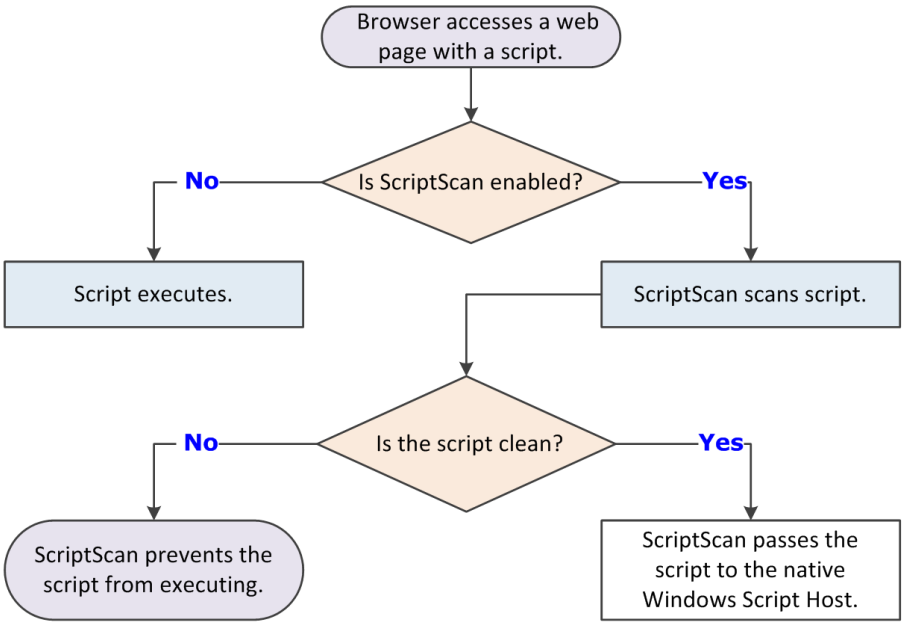
ScriptScan is a Browser Helper Object that examines JavaScript and VBScript code for malicious scripts before they execute. If the script is clean, it passes to JavaScript or VBScript for handling. If ScriptScan detects a malicious script, it blocks the script from executing.

ScriptScan examines scripts for Internet Explorer only. It doesn't look at scripts system-wide and doesn't examine scripts run by wscript.exe or cscript.exe.

When Threat Prevention is installed, the first time that Internet Explorer starts, a prompt to enable one or more McAfee add-ons appears. For ScriptScan to scan scripts:

- The Enable ScriptScan setting must be selected. ScriptScan is disabled by default.
- The add-on must be enabled in the browser.

If ScriptScan is disabled when Internet Explorer is launched and then is enabled, it doesn't detect malicious scripts in that instance of Internet Explorer. You must restart Internet Explorer after enabling ScriptScan for it to detect malicious scripts.



- If the script is clean, the script scanner passes the script to the native Windows Script Host.
- If the script contains a potential threat, the script scanner prevents the script from executing.

Best practices: ScriptScan exclusions

Script-intensive websites and web-based applications might experience poor performance when ScriptScan is enabled. Instead of disabling ScriptScan, we recommend specifying URL exclusions for trusted sites, such as sites in an intranet or web applications that are known safe.

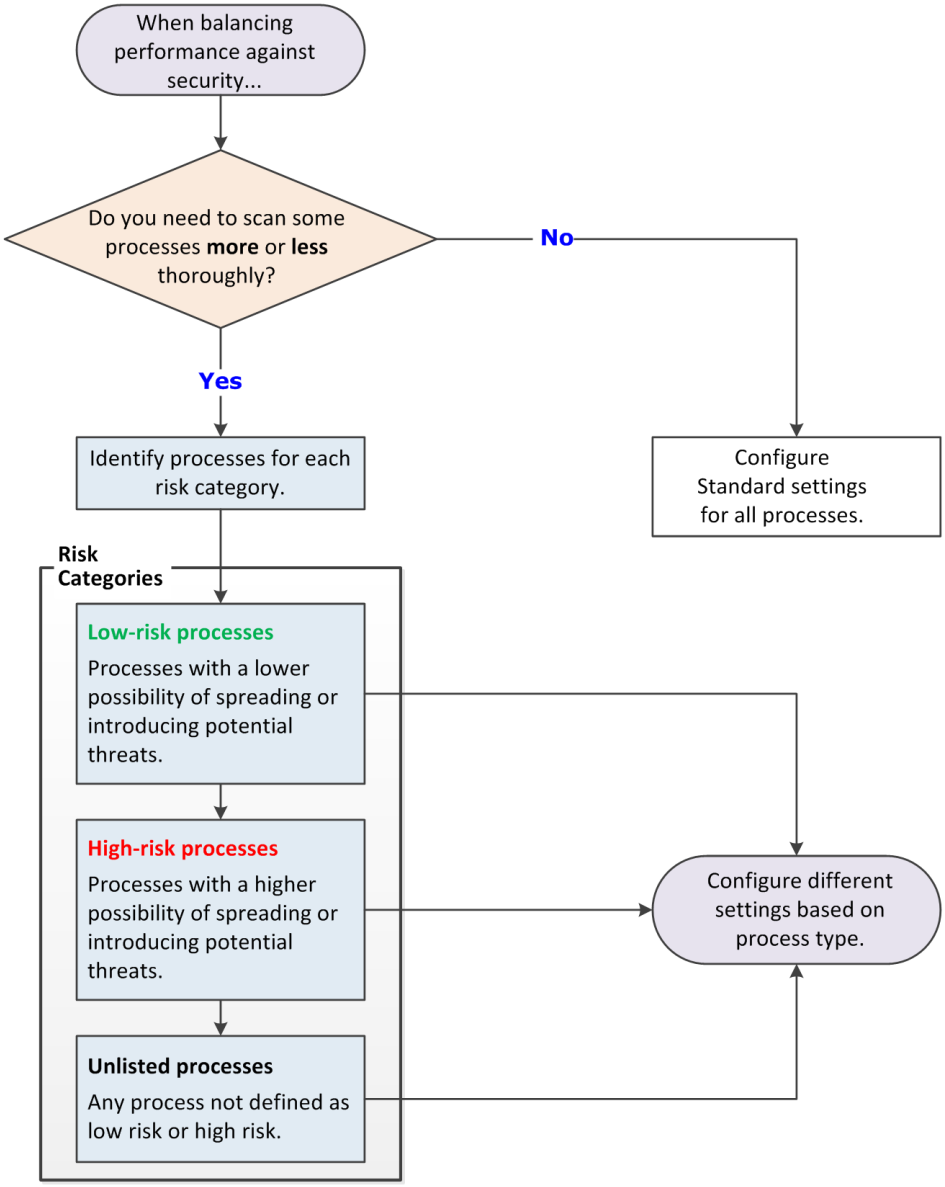
You can specify substrings or partial URLs for ScriptScan exclusions. If an exclusion string matches any part of the URL, the URL is excluded.

When creating URL exclusions:

- Wildcard characters aren't supported.
- More complete URLs result in improved performance.
- Don't include port numbers.
- Use only Fully Qualified Domain Names (FQDN) and NetBIOS names.

How to determine scanning settings for processes

Follow this process to determine whether to configure different settings based on process type.



Configure On-Demand Scan settings

These settings configure the behavior of three predefined on-demand scans: Full Scan, Quick Scan, and Right-Click Scan.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

See the Help for the Threat Prevention **Options** settings for more scan configuration options.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Threat Prevention** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Threat Prevention** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **On-Demand Scan**.

5 Click a tab to configure settings for the specified scan.

- **Full Scan**
- **Quick Scan**
- **Right-Click Scan**

6 Configure settings on the page, then click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26
Configure common scan settings on page 79
Configure, schedule, and run scan tasks on page 91

How on-demand scanning works

The on-demand scanner searches files, folders, memory, and registry, looking for any malware that could have infected the computer.

You decide when and how often the on-demand scans occur. You can scan systems manually, at a scheduled time, or at startup.

1 The on-demand scanner uses the following criteria to determine if the item must be scanned:

- The file extension matches the configuration.
- The file hasn't been cached, excluded, or previously scanned (if the scanner uses the scan cache).

If you configure McAfee GTI, the scanner uses heuristics to check for suspicious files.

2 If the file meets the scanning criteria, the scanner compares the information in the item to the known malware signatures in the currently loaded AMCore content files.

- If the file is clean, the result is cached, and the scanner checks the next item.
- If the file contains a threat, the scanner takes the configured action.

  For example, if the action is to clean the file, the scanner:

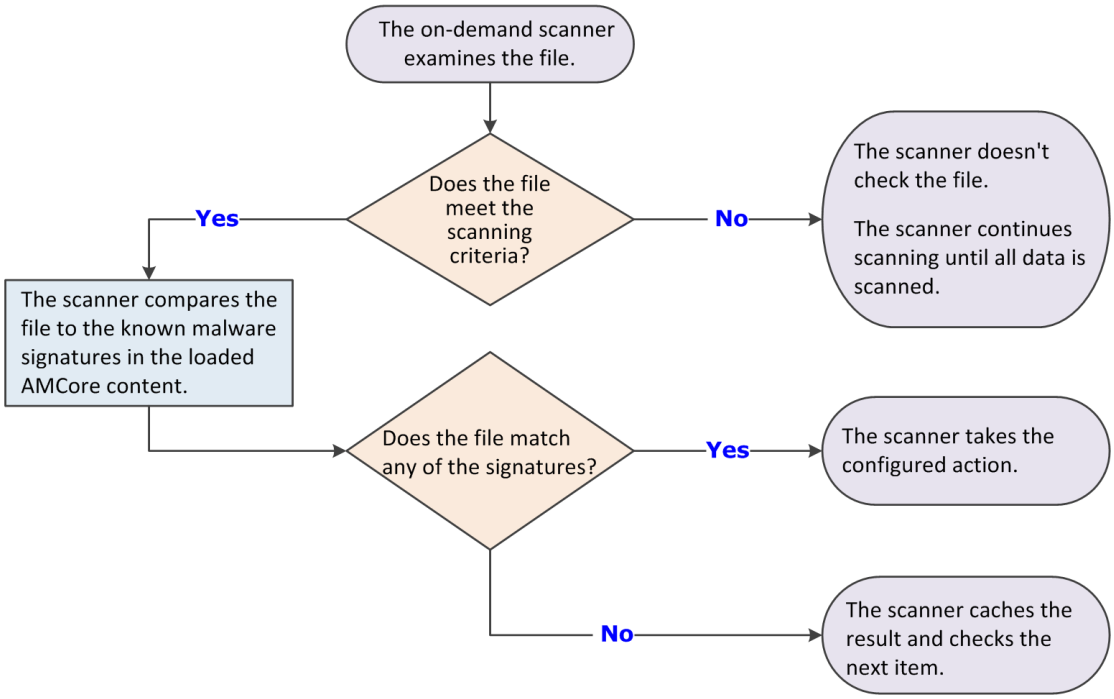
  1 Uses information in the currently loaded AMCore content file to clean the file.

  2 Records the results in the activity log.

  3 Notifies the user that it detected a threat in the file, and includes the item name and the action taken.

Windows 8 and 10 — If the scanner detects a threat in the path of an installed Windows Store app, the scanner marks it as *tampered*. Windows adds the tampered flag to the tile for the app. When you attempt to run it, Windows notifies you of the problem and directs you to the Windows Store to reinstall.

3 If the item doesn't meet the scanning requirements, the scanner doesn't check it. Instead, the scanner continues until all data is scanned.



The on-demand scan detection list is cleared when the next on-demand scan starts.

Threat Prevention flushes the global scan cache and rescans all files when an Extra.DAT is loaded.

Best practices: Reducing the impact of on-demand scans on users

To minimize the impact that on-demand scans have on a system, select options to avoid impacting system performance and scan only what you need to.

Scan only when the system is idle

The easiest way to make sure that the scan has no impact on users is to run the on-demand scan only when the computer is idle.

When this option is enabled, Threat Prevention pauses the scan when it detects disk or user activity, such as access using the keyboard or mouse. Threat Prevention resumes the scan when the user hasn't accessed the system for three minutes.

You can optionally:

- Allow users to resume scans that have been paused due to user activity.
- Return the scan to run only when the system is idle.

Disable this option only on server systems and systems that users access using Remote Desktop Connection (RDP). Threat Prevention depends on McTray to determine if the system is idle. On systems accessed only by RDP, McTray doesn't start and the on-demand scanner never runs. To work around this issue, users can start McTray (in C:\Program Files\McAfee\Agent\mctray.exe, by default) manually when they log on using RDP.

Select **Scan only when the system is idle** in the Performance section of the Scan Task Settings tab.

Pause scans automatically

To improve performance, you can pause on-demand scans when the system is running on battery power. You can also pause the scan when an application, such as a browser, media player, or presentation, is running in full-screen mode. The scan resumes immediately when the system is connected to power or is no longer in full-screen mode.

- **Do not scan when the system is on battery power**
- **Do not scan when the system is in presentation mode** (available when **Scan anytime** is enabled)

Select these options in the Performance section of the Scan Task Settings tab.

Allow users to defer scans

If you choose **Scan anytime**, you can allow users to defer scheduled scans in one-hour increments, up to 24 hours, or forever. Each user deferral can last one hour. For example, if the **Maximum number of hours user can defer** option is set to 2, the user can defer the scan twice (two hours). When the maximum specified number of hours elapses, the scan continues. If you allow unlimited deferrals by setting the option to 0, the user can continue to defer the scan forever.

Select **User can defer scans** in the Performance section of the Scan Task Settings tab.

Limit scan activity with incremental scans

Use incremental, or *resumable*, scans to limit when on-demand scan activity occurs, and still scan the whole system in multiple sessions. To use incremental scanning, add a time limit to the scheduled scan. The scan stops when the time limit is reached. The next time this task starts, it continues from the point in the file and folder structure where the previous scan stopped.

Select **Stop this task if it runs longer than** in the Options section of the Scan Task Schedule tab.

Configure system utilization

System utilization specifies the amount of CPU time that the scanner receives during the scan. For systems with end-user activity, set system utilization to **Low**.

Select **System utilization** in the Performance section of the Scan Task Settings tab.

Scan only what you need to

Scanning some types of files can negatively affect system performance. For this reason, select these options only if you need to scan specific types of files. Select or deselect these options in the What to Scan section of the Scan Task Settings tab.

- **Files that have been migrated to storage**

  Some offline data storage solutions replace files with a *stub* file. When the scanner encounters a stub file, which indicates that the file has been migrated, the scanner restores the file to the local system before scanning. The restore process can negatively impact system performance.

  Deselect this option unless you have a specific need to scan files in storage.

- **Compressed archive files**

  Even if an archive contains infected files, the files can't infect the system until the archive is extracted. Once the archive is extracted, the On-Access Scan examines the files and detects any malware.

  Best practice: Because scanning compressed archive files can negatively affect system performance, deselect this option to improve system performance.

See also

Configure On-Demand Scan settings on page 86
Configure, schedule, and run scan tasks on page 91

How system utilization works

The on-demand scanner uses the Windows Set Priority setting for the scan process and thread priority. The system utilization (*throttling*) setting enables the operating system to specify the amount of CPU time that the on-demand scanner receives during the scan process.

Setting the system utilization for the scan to Low provides improved performance for other running applications. The low setting is useful for systems with end-user activity. Conversely, by setting the system utilization to Normal, the scan completes faster. The normal setting is useful for systems that have large volumes and little end-user activity.

Each task runs independently, unaware of the limits for other tasks.

Table 3-2 Default process settings

Threat Prevention process setting	This option...	Windows Set Priority setting
Low	Provides improved performance for other running applications. Select this option for systems with end-user activity.	Low
Below normal	Sets the system utilization for the scan to the McAfee ePO default value.	Below normal
Normal (Default)	Enables the scan to complete faster. Select this option for systems that have large volumes and little end-user activity.	Normal

How Remote Storage scanning works

You can configure the on-demand scanner to scan the content of files managed by Remote Storage.

Remote Storage monitors the amount of available space on the local system. When necessary, Remote Storage automatically migrates the content (data) from eligible files from the client system to a storage device, such as a tape library. When a user opens a file whose data has been migrated, Remote Storage automatically recalls the data from the storage device.

Select the **Files that have been migrated to storage** option to configure the on-demand scanner to scan files that Remote Storage manages. When the scanner encounters a file with migrated content, it restores the file to the local system before scanning.

For more information, see What is Remote Storage.

Configure, schedule, and run scan tasks

You can schedule the default **Full Scan** and **Quick Scan** tasks or create custom scan tasks from the Endpoint Security Client in the Common settings.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 From the **Action** menu, select **Settings**.

3 Click **Show Advanced**.

4 From **Common**, click **Tasks**.

5 Configure scan task settings on the page.

To...	Follow these steps
Create a custom scan task.	1 Click **Add**. 2 Enter the name, select **Custom scan** from the drop-down list, then click **Next**. 3 Configure the scan task settings and schedule, then click **OK** to save the task.
Change a scan task.	• Double-click the task, make your changes, then click **OK** to save the task.
Remove a custom scan task.	• Select the task, then click **Delete**.
Create a copy of a scan task.	1 Select the task, then click **Duplicate**. 2 Enter the name, configure the settings, then click **OK** to save the task.

To...	Follow these steps
Change the schedule for a **Full Scan** or **Quick Scan** task.	1 Double-click **Full Scan** or **Quick Scan**. 2 Click the **Schedule** tab, change the schedule, then click **OK** to save the task. You can configure **Full Scan** and **Quick Scan** task settings on self-managed systems only. By default, the **Full Scan** is scheduled to run every Wednesday at 12 midnight. The **Quick Scan** is scheduled to run every day at 7 p.m. The schedules are enabled.
Run a scan task.	• Select the task, then click **Run Now**. If the task is already running, including paused or deferred, the button changes to **View**. If you run a task before applying changes, Endpoint Security Client prompts you to save the settings.

6 Click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26
Configure On-Demand Scan settings on page 86
Run a Full Scan or Quick Scan on page 56

Endpoint Security Client interface reference — Threat Prevention

Provide context-sensitive help for pages in the Endpoint Security Client interface.

Contents

Quarantine page

Manage items in the Quarantine.

Table 3-3 Options

Option	Definition
Delete	Deletes selected items from the Quarantine. Deleted items can't be restored.
Restore	Restores items from the Quarantine. Endpoint Security restores items to the original location and removes them from the Quarantine. If an item is still a valid threat, Endpoint Security immediately returns it to the Quarantine.
Rescan	Rescans selected items in the Quarantine. If the item is no longer a threat, Endpoint Security restores the item to its original location and removes it from the Quarantine.

Column heading	Sorts the quarantine list by...
Detection Name	Name of the detection.
Type	Type of threat, for example, **Trojan** or **Adware**.
Time quarantined	The length of time the item has been quarantined.
Number of objects	The number of objects in the detection.
AMCore content version	The version number of AMCore content that identified the threat.
Rescan status	The status of the rescan, if the item has been rescanned: • **Clean** — The rescan resulted in no threat detections. • **Infected** — Endpoint Security detected a threat during the rescan.

See also

Manage quarantined items on page 59
Detection names on page 61
Rescanning quarantined items on page 62

Threat Prevention — Access Protection

Protect your system's access points based on configured rules. Access Protection compares a requested action against the list of configured rules and acts according to the rule.

Best practice: For information about creating Access Protection rules to protect against ransomware, see PD25203.

Table 3-4 Options

Section	Option	Definition
ACCESS PROTECTION	**Enable Access Protection**	Enables the Access Protection feature.

Table 3-5 Advanced options

Section	Option	Description
Exclusions		Allows access to the specified processes, also called executables, for all rules. • **Add** — Adds a process to the exclusion list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. • **Duplicate** — Creates a copy of the selected item.
Rules		Configures Access Protection rules. You can enable, disable, and change McAfee-defined rules, but you can't delete these rules. • **Add** — Creates a custom rule and adds it to the list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. • **Duplicate** — Creates a copy of the selected item. • **Block** (only) — Blocks access attempts without logging. • **Report** (only) — Logs without blocking access attempts. • **Block** and **Report** — Blocks and logs access attempts. **Best practice:** When the full impact of a rule is not known, select **Report** but not **Block** to receive a warning without blocking access attempts. To determine whether to block access, monitor the logs and reports. To block or report all, select **Block** or **Report** in the first row. To disable the rule, deselect both **Block** and **Report**.

See also

Configure McAfee-defined Access Protection rules on page 66
Configure user-defined Access Protection rules on page 70
Add Exclusion or Edit Exclusion on page 103
Add Rule or Edit Rule on page 94
McAfee-defined Access Protection rules on page 67

Add Rule or Edit Rule

Add or edit user-defined Access Protection rules.

Table 3-6 Options

Section	Option	Definition
Options	Name	Specifies or indicates the name of the rule. (Required)
	Action	Specifies actions for the rule. • **Block** (only) — Blocks access attempts without logging. • **Report** (only) — Warns without blocking access attempts. • **Block** and **Report** — Blocks and logs access attempts. **Best practice:** When the full impact of a rule is not known, select **Report** but not **Block** to receive a warning without blocking access attempts. To determine whether to block access, monitor the logs and reports. To block or report all, select **Block** or **Report** in the first row. To disable the rule, deselect both **Block** and **Report**.
	Executables	Specifies executables for the rule. • **Add** — Creates an executable and adds it to the list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. • **Duplicate** — Creates a copy of the selected item. • **Toggle Inclusion Status** — Changes the inclusion status of the item between **Include** and **Exclude**.
	User Names	Specifies user names that the rule applies to (for user-defined rules only). • **Add** — Selects a user name and adds it to the list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. • **Duplicate** — Creates a copy of the selected item. • **Toggle Inclusion Status** — Changes the inclusion status of the item between **Include** and **Exclude**.
	Subrules	Configures subrules (for user-defined rules only). • **Add** — Creates a subrule and adds it to the list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. • **Duplicate** — Creates a copy of the selected item.
	Notes	Provides more information about the item.

See also

Add Exclusion or Edit Exclusion on page 103
Add User Name or Edit User Name on page 96
Add Subrule or Edit Subrule on page 96

Add User Name or Edit User Name

Add or edit the user that the rule applies to (for user-defined rules only).

Table 3-7 Options

Option	Definition
Name	Specifies the name of the user that the rule applies to. Use this format to specify the user: • **Local user** — Valid entries include: <machine_name>\<local_user_name> .\<local_user_name> .\administrator (for the local administrator) • **Domain user** — <domain name>\<domain user_name> • **Local system** — Local\System specifies the NT AUTHORITY\System account on the system.
Inclusion status	Specifies the inclusion status for the user. • **Include** — Triggers the rule if the specified user runs the executable that violates a subrule. • **Exclude** — Doesn't trigger the rule if the specified user runs the executable that violates a subrule.

See also

Add Rule or Edit Rule on page 94

Add Subrule or Edit Subrule

Add or edit user-defined Access Protection subrules.

Table 3-8 Options

Option	Definition
Name	Specifies the name of the subrule.
Subrule type	Specifies the subrule type. Changing the subrule type removes any previously defined entries in the **Targets** table. • **Files** — Protects a file or directory. For example, create a custom rule to block or report attempts to delete an Excel spreadsheet that contains sensitive information. • **Registry key** — Protects the specified key. A registry key is the container for the registry value. For example, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Run. • **Registry value** — Protects the specified value. Registry values are stored in registry keys and are referenced separately from registry keys. For example, HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Autorun. • **Processes** — Protects the specified process. For example, create a custom rule to block or report attempted operations on a process. • **Services** — Protects the specified service. For example, create a custom rule to prevent a service from being stopped or started.

Table 3-8 Options *(continued)*

Option	Definition
Operations	Indicates the operations permitted with the subrule type. You must specify at least one operation to apply to the subrule. **Best practice:** To avoid impacting performance, don't select the **Read** operation. **Files:** • **Change read-only or hidden attributes** — Blocks or reports changing these attributes of files in the specified folder. • **Create** — Blocks or reports creation of files in the specified folder. • **Delete** — Blocks or reports deletion of files in the specified folder. • **Execute** — Blocks or reports execution of files in the specified folder. • **Change permissions** — Blocks or reports changing permissions settings of files in the specified folder. • **Read** — Blocks or reports read access to the specified files. • **Rename** — Blocks or reports rename access to the specified files.

Table 3-8 Options *(continued)*

Option	Definition
	If the **Destination File** target is specified, **Rename** is the only valid operation. • **Write** — Blocks or reports write access to the specified files. **Registry key:** • **Write** — Blocks or reports write access to the specified key. • **Create** — Blocks or reports creation of the specified key. • **Delete** — Blocks or reports deletion of the specified key. • **Read** — Blocks or reports read access to the specified key. • **Enumerate** — Blocks or reports enumeration of the subkeys for the specified registry key. • **Load** — Blocks or reports the ability to unload the specified registry key and its subkeys from the registry. • **Replace** — Blocks or reports replacement of the specified registry key and its subkeys with another file. • **Restore** — Blocks or reports the ability to save registry information in a specified file and copies over the specified key. • **Change permissions** — Blocks or reports changing permissions settings of specified registry key and its subkeys. **Registry value:** • **Write** — Blocks or reports write access to the specified value. • **Create** — Blocks or reports creation of the specified value. • **Delete** — Blocks or reports deletion of the specified value. • **Read** — Blocks or reports read access to the specified value. **Processes:** • **Any access** — Blocks or reports opening the process with any access. • **Create thread** — Blocks or reports opening the process with access to create a thread. • **Modify** — Blocks or reports opening the process with access to modify. • **Terminate** — Blocks or reports opening the process with access to terminate. • **Run** — Blocks or reports running the specified target executable. You must add at least one target executable to the rule.

Table 3-8 Options *(continued)*

Option	Definition
	For the **Run** operation, an event is generated when an attempt is made to run the target process. For all other operations, an event is generated when the target is opened. **Services:** • **Start** — Blocks or reports starting the service. • **Stop** — Blocks or reports stopping the service. • **Pause** — Blocks or reports pausing the service. • **Continue** — Blocks or reports continuing the service after a pause. • **Create** — Blocks or reports creating the service. • **Delete** — Blocks or reports deleting the service. • **Enable hardware profile** — Blocks or reports enabling the hardware profile of the service. • **Disable hardware profile** — Blocks or reports disabling the hardware profile of the service. • **Modify startup mode** — Blocks or reports modifying the startup mode (Boot, System, Automatic, Manual, Disabled) of the service. • **Modify logon information** — Blocks or reports modifying the logon information of the service.
Targets	• **Add** — Specifies the targets for the rule. Targets vary depending on the rule type selection. You must add at least one target to the subrule. Click **Add**, select the inclusion status, then enter or select the target to include or exclude. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item.

See also

Add Rule or Edit Rule on page 94
Targets on page 100
Add Exclusion or Edit Exclusion on page 103

Targets

Specify the inclusion status and definition for a target.

Table 3-9 Options

Section	Option	Definition
Targets		Determines whether the target is a positive match for the subrule. Also specifies the status of the inclusion for the target. • **Include** — Indicates that the subrule can match the specified target. • **Exclude** — Indicates that the subrule must not match the specified target. Add a target with either an **Include** or **Exclude** directive.
	*If you selected the **Files** subrule type...*	Specifies the file name, folder name, path, or drive type target for a **Files** subrule. • **File path** — Browse to select the file. • **Destination file** — Browse to select the target file name or path for a **Rename** operation. If the **Destination file** target is selected, the **Rename** operation (only) must be selected. • **Drive type** — Select the drive type target from the drop-down list: • **Removable** — Files on a USB drive or other removable drive connected to a USB port, including those with Windows To Go installed. This drive type doesn't include files on a CD, DVD, or floppy disk. Blocking this drive type also blocks drives with Windows To Go installed. • **Network** — Files on a network share • **Fixed** — Files on the local hard drive or other fixed hard disk • **CD/DVD** — Files on a CD or DVD • **Floppy** — Files on a floppy disk You can use `?`, `*`, and `**` as wildcards. **Files subrule target best practices** For example, to protect: • A file or folder named c:\testap, use a target of c:\testap or c:\testap\ • The contents of a folder, use the asterisk wildcard — c:\testap* • The contents of a folder and its subfolders, use 2 asterisks — c:\testap** System environment variables are supported. Environment variables can be specified in one of the following formats: • `$(EnvVar) - $(SystemDrive), $(SystemRoot)` • `%EnvVar% - %SystemRoot%, %SystemDrive%` Not all system-defined environment variables can be accessed using the `$(var)` syntax, specifically those containing the `or` characters. You can use the `%var%` syntax to avoid this issue. User environment variables are not supported.

Table 3-9 Options *(continued)*

Section	Option	Definition
	If you selected the ***Registry key*** *subrule type...*	Defines registry keys using root keys. These root keys are supported: • HKLM or HKEY_LOCAL_MACHINE • HKCU or HKEY_CURRENT_USER • HKCR or HKEY_CLASSES_ROOT • HKCCS matches HKLM/SYSTEM/CurrentControlSet and HKLM/SYSTEM/ControlSet00X • HKLMS matches HKLM/Software on 32-bit and 64-bit systems, and HKLM/Software/Wow6432Node on 64-bit systems only • HKCUS matches HKCU/Software on 32-bit and 64-bit systems, and HKCU/Software/Wow6432Node on 64-bit systems only • HKULM treated as both HKLM and HKCU • HKULMS treated as both HKLMS and HKCUS • HKALL treated as both HKLM and HKU You can use `?`, `*`, and `**` as wildcards, and `|` (pipe) as an escape character. **Registry key subrule target best practices** For example, to protect: • A registry key named HKLM\SOFTWARE\testap, use a target of HKLM\SOFTWARE\testap or HKLM\SOFTWARE\testap\ • The contents of a registry key, use the asterisk wildcard — HKLM\SOFTWARE\testap* • The contents of a registry key and its subkeys, use 2 asterisks — HKLM\SOFTWARE\testap** • Registry keys and values under a registry key, enable the **Write** operation

Table 3-9 Options *(continued)*

Section	Option	Definition
	If you selected the ***Registry value*** *subrule type...*	Defines registry values using root keys. These root keys are supported: • HKLM or HKEY_LOCAL_MACHINE • HKCU or HKEY_CURRENT_USER • HKCR or HKEY_CLASSES_ROOT • HKCCS matches HKLM/SYSTEM/CurrentControlSet and HKLM/SYSTEM/ControlSet00X • HKLMS matches HKLM/Software on 32-bit and 64-bit systems, and HKLM/Software/Wow6432Node on 64-bit systems only • HKCUS matches HKCU/Software on 32-bit and 64-bit systems, and HKCU/Software/Wow6432Node on 64-bit systems only • HKULM treated as both HKLM and HKCU • HKULMS treated as both HKLMS and HKCUS • HKALL treated as both HKLM and HKU You can use `?`, `*`, and `**` as wildcards, and `|` (pipe) as an escape character. **Registry value subrule target best practices** For example, to protect: • A registry value named HKLM\SOFTWARE\testap, use a target of HKLM\SOFTWARE\testap • The registry values under a registry key, use the asterisk wildcard — HKLM\SOFTWARE\testap* • The registry values under a registry key and its subkeys, use 2 asterisks — HKLM\SOFTWARE\testap**

Table 3-9 Options *(continued)*

Section	Option	Definition
	If you selected the **Processes** *subrule type...*	Specifies the process file name or path, MD5 hash, or signer target for a **Processes** subrule. You can use `?`, `*`, and `**` as wildcards for all except MD5 hash. **Processes subrule target best practices** For example, to protect: • A process named c:\testap.exe, use a target file name or path of c:\testap.exe • All processes in a folder, use the asterisk wildcard — c:\testap* • All processes in a folder and its subfolders, use 2 asterisks — c:\testap**
	If you selected the **Services** *subrule type...*	Specifies the service name or display name for a **Services** subrule. • **Service registered name** — Contains the name of the service in the corresponding registry key under HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\. • **Service display name** — Contains the display name of the service from the DisplayName registry value under HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<service_name>\ . This is the name that appears in the Services manager. For example, "Adobe Acrobat Update Service" is the display name for the "AdobeARMservice" service name. You can use `?` and `*` as wildcards. **Services subrule target best practices** For example, to protect all Adobe services by display name, use the asterisk wildcard — Adobe*

See also

Add Subrule or Edit Subrule on page 96

Add Exclusion or Edit Exclusion

Add or edit an executable to exclude at the policy level, or include or exclude at the rule level.

When specifying exclusions and inclusions, consider the following:

- You must specify at least one identifier: File name or path, MD5 hash, or Signer.
- If you specify more than one identifier, all identifiers apply.
- If you specify more than one identifier and they don't match (for example, the file name and MD5 hash don't apply to the same file), the exclusion or inclusion is invalid.
- Exclusions and inclusions are case insensitive.
- Wildcards are allowed for all except MD5 hash.

Table 3-10 Options

Option	Definition
Name	Specifies the name that you call the executable. This field is required with at least one other field: **File name or path**, **MD5 hash**, or **Signer**.
Inclusion status	Determines the inclusion status for the executable. • **Include** — Triggers the rule if the executable violates a subrule. • **Exclude** — Doesn't trigger the rule if the executable violates a subrule. **Inclusion status** only appears when adding an executable to a rule or the target for the Processes subrule.
File name or path	Specifies the file name or path of the executable to add or edit. Click **Browse** to select the executable. The file path can include wildcards.
MD5 hash	Indicates the (32-digit hexadecimal number) MD5 hash of the process.
Signer	**Enable digital signature check** — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify: • **Allow any signature** — Allows files signed by any process signer. • **Signed by** — Allows only files signed by the specified process signer. A signer distinguished name (SDN) for the executable is required and it must match exactly the entries in the accompanying field, including commas and spaces. The process signer appears in the correct format in the events in the Endpoint Security Client Event Log and McAfee ePO Threat Event Log. For example: C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS To obtain the SDN of an executable: 1 Right-click an executable and select **Properties**. 2 On the **Digital Signatures** tab, select a signer and click **Details**. 3 On the **General** tab, click **View Certificate**. 4 On the **Details** tab, select the **Subject** field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: • CN = Mozilla Corporation • OU = Release Engineering • O = Mozilla Corporation • L = Mountain View • S = California • C = US
Notes	Provides more information about the item.

See also

Add Rule or Edit Rule on page 94

Threat Prevention — Exploit Prevention

Enable and configure Exploit Prevention to keep buffer overflow exploits from executing arbitrary code on your computer.

For the list of processes protected by Exploit Prevention, see KB58007.

Host Intrusion Prevention 8.0 can be installed on the same system as Endpoint Security version 10.5. If McAfee Host IPS is enabled, Exploit Prevention is disabled even if enabled in the policy settings.

Table 3-11 Options

Section	Option	Definition
EXPLOIT PREVENTION	Enable Exploit Prevention	Enables the Exploit Prevention feature. Failure to enable this option leaves your system unprotected from malware attacks.

Table 3-12 Advanced options

Section	Option	Definition
Generic Privilege Escalation Prevention	Enable Generic Privilege Escalation Prevention	Enables Generic Privilege Escalation Prevention (GPEP) support. (Disabled by default) GPEP uses GPEP signatures in the Exploit Prevention Content to provide coverage for privilege escalation exploits in kernel mode and user mode. Enabling this option raises the severity of GPEP buffer overflow signature 6052 to High, so that it is blocked or reported, depending on the specified action. Because GPEP might generate false positive reports, this option is disabled by default.
Windows Data Execution Prevention	Enable Windows Data Execution Prevention	Enables Windows Data Execution Prevention (DEP) integration. (Disabled by default) Select this option to: • Enable DEP for 32-bit applications in the McAfee application protection list, if not already enabled, and use it instead of Generic Buffer Overflow Protection (GBOP). Caller validation and Targeted API Monitoring are still enforced. • Monitor for DEP detections in the DEP-enabled 32-bit applications. • Monitor for DEP detections in 64-bit applications in the McAfee application protection list. • Log any DEP detections and send an event to McAfee ePO. Disabling this option doesn't affect any processes that have DEP enabled as a result of the Windows DEP policy.
Exclusions		Specifies the process, caller module, API, or signature to exclude. Exclusions with Caller Module or API don't apply to DEP. • **Add** — Creates an exclusion and adds it to the list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. • **Duplicate** — Creates a copy of the selected item.

Table 3-12 Advanced options *(continued)*

Section	Option	Definition
Signatures		Changes the action (**Block** or **Report**) for McAfee-defined Exploit Prevention signatures. You can't change the severity or create signatures. To disable the signature, deselect **Block** and **Report**.
	Show signatures with a severity of	Filters the **Signatures** list by severity or disabled status: • **High** • **Medium** • **Low** • **Informational** • **Disabled** You can't enable signatures with a severity of Disabled.
	Block (only)	Blocks behavior that matches the signature without logging.
	Report (only)	Logs behavior that matches the signature without blocking. Selecting **Report** only for Signature ID 9990 is not permitted.
	Block and **Report**	Blocks and logs behavior that matches the signature.
Application Protection Rules		Configures application protection rules. • **Add** — Creates an application protection rule and adds it to the list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. (User-defined rules only) • **Duplicate** — Creates a copy of the selected item. (User-defined rules only)

See also

Configure Exploit Prevention settings on page 75
Add Exclusion or Edit Exclusion on page 106

Add Exclusion or Edit Exclusion

Add or edit an Exploit Prevention exclusion.

When specifying exclusions, consider the following:

- You must specify at least one of Process, Caller Module, API, or Signature.
- Exclusions with Caller Module or API don't apply to DEP.
- For Process exclusions, you must specify at least one identifier: File name or path, MD5 hash, or Signer.
- If you specify more than one identifier, all identifiers apply.
- If you specify more than one identifier and they don't match (for example, the file name and MD5 hash don't apply to the same file), the exclusion is invalid.
- Exclusions are case insensitive.

- Wildcards are allowed for all except MD5 hash and Signature IDs.
- If you include signature IDs in an exclusion, the exclusion only applies to the process in the specified signatures. If no signature IDs are specified, the exclusion applies to the process in all signatures.

Table 3-13 Options

Section	Option	Definition
Process	**Name**	Specifies the process name to exclude. Exploit Prevention excludes the process wherever it is located. This field is required with at least one other field: **File name or path**, **MD5 hash**, or **Signer**.
	File name or path	Specifies the file name or path of the executable to add or edit. Click **Browse** to select the executable.
	MD5 hash	Indicates the (32-digit hexadecimal number) MD5 hash of the process.
	Signer	**Enable digital signature check** — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify: • **Allow any signature** — Allows files signed by any process signer. • **Signed by** — Allows only files signed by the specified process signer. A signer distinguished name (SDN) for the executable is required and it must match exactly the entries in the accompanying field, including commas and spaces. The process signer appears in the correct format in the events in the Endpoint Security Client Event Log and McAfee ePO Threat Event Log. For example: C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS To obtain the SDN of an executable: 1 Right-click an executable and select **Properties**. 2 On the **Digital Signatures** tab, select a signer and click **Details**. 3 On the **General** tab, click **View Certificate**. 4 On the **Details** tab, select the **Subject** field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: • CN = Mozilla Corporation • OU = Release Engineering • O = Mozilla Corporation • L = Mountain View • S = California • C = US
Caller Module	**Name**	Specifies the name of the module (a DLL) loaded by an executable that owns the writable memory that makes the call. This field is required with at least one other field: **File name or path**, **MD5 hash**, or **Signer**.
	File name or path	Specifies the file name or path of the executable to add or edit. Click **Browse** to select the executable.

Table 3-13 Options *(continued)*

Section	Option	Definition
	MD5 hash	Indicates the (32-digit hexadecimal number) MD5 hash of the process.
	Signer	**Enable digital signature check** — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify: • **Allow any signature** — Allows files signed by any process signer. • **Signed by** — Allows only files signed by the specified process signer. A signer distinguished name (SDN) for the executable is required and it must match exactly the entries in the accompanying field, including commas and spaces. The process signer appears in the correct format in the events in the Endpoint Security Client Event Log and McAfee ePO Threat Event Log. For example: C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS To obtain the SDN of an executable: 1 Right-click an executable and select **Properties**. 2 On the **Digital Signatures** tab, select a signer and click **Details**. 3 On the **General** tab, click **View Certificate**. 4 On the **Details** tab, select the **Subject** field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: • CN = Mozilla Corporation • OU = Release Engineering • O = Mozilla Corporation • L = Mountain View • S = California • C = US
API	**Name**	Specifies the name of the API (application programming interface) being called.
Signatures	**Signature IDs**	Specifies (comma-separated) Exploit Prevention signature identifiers.
Notes		Provides more information about the item.

See also

Exclude processes from Exploit Prevention on page 75

Add Rule or Edit Rule

Add or edit user-defined Application Protection rules.

Table 3-14 Options

Section	Option	Definition
	Name	Specifies or indicates the name of the rule. (Required)
	Status	Enables or disables the item.

Table 3-14 Options *(continued)*

Section	Option	Definition
	Inclusion status	Specifies the inclusion status for the executable. • **Include** — Triggers the rule if an executable in the Executables list runs. • **Exclude** — Doesn't trigger the rule if an executable in the Executables list runs.
Executables		Specifies executables for the rule. • **Add** — Adds an executable to the list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. • **Duplicate** — Creates a copy of the selected item.
Notes		Provides more information about the item. For McAfee-defined Application Protection rules, this field contains the name of the executable being protected.

Add Executable or Edit Executable

Add or edit an executable in an Application Protection rule.

When configuring executables, consider the following:

- You must specify at least one identifier: File name or path, MD5 hash, or Signer.
- If you specify more than one identifier, all identifiers apply.
- If you specify more than one identifier and they don't match (for example, the file name and MD5 hash don't apply to the same file), the executable definition is invalid.

Table 3-15 Options

Section	Option	Definition
Properties	**Name**	Specifies the process name. This field is required with at least one other field: **File name or path**, **MD5 hash**, or **Signer**.
	File name or path	Specifies the file name or path of the executable to add or edit. Click **Browse** to select the executable.
	MD5 hash	Indicates the (32-digit hexadecimal number) MD5 hash of the process.

Table 3-15 Options *(continued)*

Section	Option	Definition
	Signer	**Enable digital signature check** — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify: • **Allow any signature** — Allows files signed by any process signer. • **Signed by** — Allows only files signed by the specified process signer. A signer distinguished name (SDN) for the executable is required and it must match exactly the entries in the accompanying field, including commas and spaces. The process signer appears in the correct format in the events in the Endpoint Security Client Event Log and McAfee ePO Threat Event Log. For example: C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS To obtain the SDN of an executable: 1 Right-click an executable and select **Properties**. 2 On the **Digital Signatures** tab, select a signer and click **Details**. 3 On the **General** tab, click **View Certificate**. 4 On the **Details** tab, select the **Subject** field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: • CN = Mozilla Corporation • OU = Release Engineering • O = Mozilla Corporation • L = Mountain View • S = California • C = US
Notes		Provides more information about the item.

Threat Prevention — On-Access Scan

Enable and configure the on-access scan settings.

Table 3-16 Options

Section	Option	Definition
ON-ACCESS SCAN	**Enable On-Access Scan**	Enables the On-Access Scan feature. (Enabled by default)
	Enable On-Access Scan on system startup	Enables the On-Access Scan feature each time you start the computer. (Enabled by default)
	Specify maximum number of seconds for each file scan	Limits each file scan to the specified number of seconds. (Enabled by default) The default value is 45 seconds. If a scan exceeds the time limit, the scan stops cleanly and logs a message.

Table 3-16 Options *(continued)*

Section	Option	Definition
	Scan boot sectors	Examines the disk boot sector. (Enabled by default) **Best practice:** Deselect boot sector scanning when a disk contains a unique or abnormal boot sector that can't be scanned.
	Scan processes on service startup and content update	Rescans all processes that are currently in memory each time: • You re-enable on-access scans. • Content files are updated. • The system starts. • The McShield.exe process starts. (Disabled by default) **Best practice:** Because some programs or executables start automatically when you start your system, deselect this option to improve system startup time. When the on-access scanner is enabled, it always scans all processes when they are executed.
	Scan trusted installers	Scans MSI files (installed by msiexec.exe and signed by McAfee or Microsoft) or Windows Trusted Installer service files. (Disabled by default) **Best practice:** Deselect this option to improve the performance of large Microsoft application installers.
	Scan when copying between local folders	Scans files when the user copies from one local folder to another. If this option is: • **Disabled** — Only items in the destination folder are scanned. • **Enabled** — Items in both source (read) and destination (write) folders are scanned. (Disabled by default)
	Scan when copying from network folders and removable drives	Scans files when the user copies from a network folder or removable USB drive. Failure to select this option leaves your system vulnerable to malware attacks. (Enabled by default)
McAfee GTI		Enables and configures McAfee GTI settings.

Table 3-16 Options *(continued)*

Section	Option	Definition
ScriptScan	Enable ScriptScan	Enables scanning JavaScript and VBScript scripts in Internet Explorer to prevent unwanted scripts from executing. (Disabled by default) If ScriptScan is disabled when Internet Explorer is launched and then is enabled, it doesn't detect malicious scripts in that instance of Internet Explorer. You must restart Internet Explorer after enabling ScriptScan for it to detect malicious scripts.
	Exclude these URLs or partial URLs	Specifies ScriptScan exclusions by URL. **Add** — Adds a URL to the exclusion list. **Delete** — Removes a URL from the exclusion list. URLs can't include wildcard characters. But, any URL with a string from an excluded URL is also excluded. For example, if the URL msn.com is excluded, the following URLs are also excluded: • http://weather.msn.com • http://music.msn.com

Table 3-17 Advanced options

Section	Option	Definition
Threat Detection User Messaging	Display the On-Access Scan window to users when a threat is detected	Displays the **On-Access Scan** page with the specified message to client users when a detection occurs. (Enabled by default) When this option is selected, users can open this page from the **Scan Now** page at any time the detection list includes at least one threat. The on-access scan detection list is cleared when the Endpoint Security service restarts or the system reboots.
	Message	Specifies the message to display to client users when a detection occurs. The default message is: McAfee Endpoint Security detected a threat.
Process Settings	Use Standard settings for all processes	Applies the same configured settings to all processes when performing an on-access scan.
	Configure different settings for High Risk and Low Risk processes	Configures different scanning settings for each process type that you identify.
	Standard	Configures settings for processes that aren't identified as either high risk or low risk. (Enabled by default)
	High Risk	Configures settings for processes that are high risk.
	Low Risk	Configures settings for processes that are low risk.
	Add	Adds a process to the **High Risk** or **Low Risk** list.
	Delete	Removes a process from the **High Risk** or **Low Risk** list.
Scanning	When to scan	
	When writing to disk	Attempts to scan all files as they are written to or changed on the computer or other data storage device.

Table 3-17 Advanced options *(continued)*

Section	Option	Definition
	When reading from disk	Scans all files as they are read from the computer or other data storage device.
	Let McAfee decide	Allows McAfee to decide whether a file must be scanned, using trust logic to optimize scanning. Trust logic improves your security and boosts performance by avoiding unnecessary scans.  **Best practice:** Enable this option for the best protection and performance.
	Do not scan when reading from or writing to disk	Specifies to not scan **Low Risk** processes only.
	What to scan	
	All files	Scans all files, regardless of extension.  Failure to select this option leaves your system vulnerable to malware attacks.
	Default and specified file types	Scans: • Default list of file extensions defined in the current AMCore content file, including files with no extension • Any additional file extensions that you specify Separate extensions with a comma. • (Optional) Known macro threats in the list of default and specified file extensions
	Specified file types only	Scans either or both: • Only files with the (comma-separated) extensions that you specify • All files with no extension
	On network drives	Scans resources on mapped network drives.  **Best practice:** Deselect this option to improve performance.
	Opened for backups	Scans files when accessed by backup software.  **Best practice:** For most environments, you don't need to select this setting.
	Compressed archive files	Examines the contents of archive (compressed) files, including .jar files.  **Best practice:** Because scanning compressed archive files can negatively affect system performance, deselect this option to improve system performance.
	Compressed MIME-encoded files	Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
	Additional scan options	

Table 3-17 Advanced options *(continued)*

Section	Option	Definition
	Detect unwanted programs	Enables the scanner to detect potentially unwanted programs. The scanner uses the information you configured in the Threat Prevention Options settings to detect potentially unwanted programs.
	Detect unknown program threats	Uses McAfee GTI to detect executable files that have code resembling malware.
	Detect unknown macro threats	Uses McAfee GTI to detect unknown macro viruses.
Actions		Specifies how the scanner responds when it detects a threat.
Exclusions		Specifies files, folders, and drives to exclude from scanning.
	Add	Adds an item to the exclusion list.
	Delete	Removes an item from the exclusion list.

See also

Configure On-Access Scan settings on page 80
McAfee GTI on page 118
Actions on page 119
Add Exclusion or Edit Exclusion on page 121

Threat Prevention — On-Demand Scan

Configure the On-Demand Scan settings for the preconfigured and custom scans that run on your system.

See the settings in the Common module for logging configuration.

These settings specify the scanner behavior when you:

- Select **Full Scan** or **Quick Scan** from the **Scan Now** page in the Endpoint Security Client.
- As an administrator, run a custom on-demand scan task from **Settings** | **Common** | **Tasks** in the Endpoint Security Client.
- Right-click a file or folder and select **Scan for threats** from the pop-up menu.

Table 3-18 Options

Section	Option	Definition
What to Scan	**Boot sectors**	Examines the disk boot sector. **Best practice:** Deselect boot sector scanning when a disk contains a unique or abnormal boot sector that can't be scanned.
	Files that have been migrated to storage	Scans files that Remote Storage manages. Some offline data storage solutions replace files with a *stub* file. When the scanner encounters a stub file, which indicates that the file has been migrated, the scanner restores the file to the local system before scanning. The restore process can negatively impact system performance. **Best practice:** Deselect this option unless you have a specific need to scan files in storage.
	Compressed MIME-encoded files	Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.

Table 3-18 Options *(continued)*

Section	Option	Definition
	Compressed archive files	Examines the contents of archive (compressed) files, including .jar files. **Best practice:** Select this option only in scans scheduled during off hours when the system isn't being used because scanning compressed archive files can negatively affect system performance.
	Subfolders (**Right-Click Scan** only)	Examines all subfolders of the specified folder.
Additional Scan Options	**Detect unwanted programs**	Enables the scanner to detect potentially unwanted programs. The scanner uses the information you configured in the Threat Prevention Options settings to detect potentially unwanted programs.
	Detect unknown program threats	Uses McAfee GTI to detect executable files that have code resembling malware.
	Detect unknown macro threats	Uses McAfee GTI to detect unknown macro viruses.
Scan Locations	(**Full Scan** and **Quick Scan** only)	Specifies the locations to scan. These options apply to **Full Scan**, **Quick Scan**, and custom scans only.
File Types to Scan	**All files**	Scans all files, regardless of extension. McAfee strongly recommends enabling **All files**. Failure to select this option leaves your system vulnerable to malware attacks.
	Default and specified file types	Scans: • Default list of file extensions defined in the current AMCore content file, including files with no extension • Any additional file extensions that you specify Separate extensions with a comma. • (Optional) Known macro threats in the list of default and specified file extensions
	Specified file types only	Scans either or both: • Only files with the (comma-separated) extensions that you specify • All files with no extension
McAfee GTI		Enables and configures McAfee GTI settings.
Exclusions		Specifies files, folders, and drives to exclude from scanning.
	Add	Adds an item to the exclusion list.
	Delete	Removes an item from the exclusion list.
Actions		Specifies how the scanner responds when it detects a threat.
Performance	**Use the scan cache**	Enables the scanner to use the existing clean scan results. **Best practice:** Select this option to reduce duplicate scanning and improve performance.

Table 3-18 Options *(continued)*

Section	Option	Definition
	System utilization	Enables the operating system to specify the amount of CPU time that the scanner receives during the scan. Each task runs independently, unaware of the limits for other tasks. • **Low** — Provides improved performance for other running applications. **Best practice:** Select this option for systems with end-user activity. • **Below normal** — Sets the system utilization for the scan to the McAfee ePO default. • **Normal** (Default) — Enables the scan to complete faster. **Best practice:** Select this option for systems that have large volumes and little end-user activity.
Scheduled Scan Options		These options apply to **Full Scan**, **Quick Scan**, and custom scans only.
	Scan only when the system is idle	Runs the scan only when the system is idle. Threat Prevention pauses the scan when the user accesses the system using the keyboard or mouse. Threat Prevention resumes the scan when the user (and CPU) is idle for five minutes. Disable this option only on server systems and systems that users access using Remote Desktop Connection (RDP). Threat Prevention depends on McTray to determine if the system is idle. On systems accessed only by RDP, McTray doesn't start and the on-demand scanner never runs. To work around this issue, users can start McTray (in C:\Program Files\McAfee\Agent\mctray.exe, by default) manually when they log on using RDP.
	Scan anytime	Runs the scan even if the user is active and specifies options for the scan.
		User can defer scans — Allows the user to defer scheduled scans, and specifies options for scan deferral. • **Maximum number of times user can defer for one hour** — Specifies the number of times (1–23) that the user can defer the scan for one hour. • **User message** — Specifies the message to display when a scan is about to start. The default message is: *McAfee Endpoint Security is about to scan your system.* • **Message duration (seconds)** — Specifies how long (in seconds that the user message appears when a scan is about to start. The valid range for the duration is 30–300; the default is 45 seconds.
		Do not scan when the system is in presentation mode — Postpones the scan while the system is presentation mode.
	Do not scan when the system is on battery power	Postpones the scan when the system is using battery power.

See also

Configure On-Demand Scan settings on page 86
Configure, schedule, and run scan tasks on page 91
Run a Full Scan or Quick Scan on page 56
Scan a file or folder on page 58
Scan Locations on page 117
McAfee GTI on page 118
Actions on page 119
Add Exclusion or Edit Exclusion on page 121

Scan Locations

Specify the locations to scan.

These options apply to **Full Scan**, **Quick Scan**, and custom scans only.

Table 3-19 Options

Section	Option	Definition
Scan Locations	**Scan subfolders**	Examines all subfolders in the specified volumes when any of these options are selected: • **Home folder** • **User profile folder** • **Program files folder** • **Temp folder** • **File or folder** Deselect this option to scan only the root level of the volumes.
	Specify locations	Specifies the locations to scan. • **Add** — Adds a location to the scan. Click **Add**, then select the location from the drop-down. • *Double-click an item* — Changes the selected item. • **Delete** — Removes a location from the scan. Select the location and click **Delete**.
	Memory for rootkits	Scans system memory for installed rootkits, hidden processes, and other behavior that suggests malware is attempting to hide itself. This scan occurs before all other scans. Failure to enable this option leaves your system unprotected from malware attacks.
	Running processes	Scans the memory of all running processes. Actions other than **Clean files** are treated as **Continue scanning**. Failure to enable this option leaves your system unprotected from malware attacks.
	Registered files	Scans files that the Windows Registry references. The scanner searches the registry for file names, determines whether the files exist, creates a list of files to scan, then scans the files.
	My computer	Scans all drives physically attached to your computer or logically mapped to a drive letter on your computer.
	All local drives	Scans all drives and their subfolders on the computer.
	All fixed drives	Scans all drives physically connected to the computer.

Table 3-19 Options *(continued)*

Section	Option	Definition
	All removable drives	Scans all removable drives or other storage devices connected to the computer, except those drives with Windows To Go installed.
	All mapped drives	Scans network drives logically mapped to a network drive on the computer.
	Home folder	Scans the home folder of the user who starts the scan.
	User profile folder	Scans the profile of the user who starts the scan, including the user's My Documents folder.
	Windows folder	Scans the contents of the Windows folder.
	Program Files folder	Scans the contents of the Program Files folder.
	Temp folder	Scans the contents of the Temp folder.
	Recycle bin	Scans the contents of the Recycle Bin.
	File or folder	Scans the specified file or folder.
	Registry	Scans registry keys and values.

See also

Threat Prevention — On-Demand Scan on page 114

McAfee GTI

Enable and configure McAfee GTI (Global Threat Intelligence) settings.

Table 3-20 Options

Section	Option	Definition
Enable McAfee GTI		Enables and disables heuristic checks. • When enabled, fingerprints of samples, or *hashes*, are submitted to McAfee Labs to determine if they are malware. By submitting hashes, detection might be made available sooner than the next AMCore content file release, when McAfee Labs publishes the update. • When disabled, no fingerprints or data is submitted to McAfee Labs.
Sensitivity level		Configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. But, allowing more detections might result in more false positive results.
	Very low	The detections and risk of false positives are the same as with regular AMCore content files. A detection is made available to Threat Prevention when McAfee Labs publishes it instead of in the next AMCore content file update. Use this setting for desktops and servers with restricted user rights and strong security configurations. This setting results in an average of 10–15 queries per day, per computer.
	Low	This setting is the minimum recommendation for laptops, desktops, and servers with strong security configurations. This setting results in an average of 10–15 queries per day, per computer.

Table 3-20 Options *(continued)*

Section	Option	Definition
	Medium	Use this setting when the regular risk of exposure to malware is greater than the risk of a false positive. McAfee Labs proprietary, heuristic checks result in detections that are likely to be malware. But, some detections might result in a false positive. With this setting, McAfee Labs checks that popular applications and operating system files don't result in a false positive. This setting is the minimum recommendation for laptops, desktops, and servers. This setting results in an average of 20–25 queries per day, per computer.
	High	Use this setting for deployment to systems or areas which are regularly infected. This setting results in an average of 20–25 queries per day, per computer.
	Very high	Use this setting for non-operating system volumes. Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives. Use this setting only to scan volumes and directories that don't support executing programs or operating systems. This setting results in an average of 20–25 queries per day, per computer.

See also

Threat Prevention — On-Access Scan on page 110
Threat Prevention — On-Demand Scan on page 114
Web Control — Options on page 161

Actions

Specify how the scanner responds when it detects a threat.

Table 3-21 Options

Section	Option	Definition	Scan type	
			On-Access Scan	**On-Demand Scan**
Threat detection first response		Specifies the first action for the scanner to take when a threat is detected.		
	Deny access to files	Prevents users from accessing any files with potential threats.	✓	
	Continue scanning	Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.		✓
	Clean files	Removes the threat from the detected file, if possible.	✓	✓
	Delete files	Deletes files with potential threats.	✓	✓
If first response fails		Specifies the action for the scanner to take when a threat is detected if the first action fails.		
	Deny access to files	Prevents users from accessing files with potential threats.	✓	
	Continue scanning	Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.		✓

Table 3-21 Options *(continued)*

Section	Option	Definition	Scan type	
			On-Access Scan	On-Demand Scan
	Delete files	Deletes files with potential threats.	✓	✓
Unwanted program first response		Specifies the first action for the scanner to take when a potentially unwanted program is detected. This option is available only if **Detect unwanted programs** is selected.		
	Deny access to files	Prevents users from accessing files with potential threats.	✓	
	Allow access to files	Allows users to access files with potential threats.	✓	
	Continue scanning	Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.		✓
	Clean files	Removes the threat from the potentially unwanted program file, if possible.	✓	✓
	Delete files	Deletes potentially unwanted program files.	✓	✓
If first response fails		Specifies the action for the scanner to take when an unwanted program detection is detected if the first action fails. This option is available only if **Detect unwanted programs** is selected.		
	Deny access to files	Prevents users from accessing files with potential threats.	✓	
	Allow access to files	Allows users to access files with potential threats.	✓	
	Continue scanning	Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.		✓
	Delete files	Deletes potentially unwanted program files automatically.	✓	✓

See also

Threat Prevention — On-Access Scan on page 110
Threat Prevention — On-Demand Scan on page 114

Add Exclusion or Edit Exclusion

Add or edit an exclusion definition.

Table 3-22 Options

Section	Option	Definition	Scan type	
			On-Access	On-Demand
What to exclude		Specifies the type of exclusion and the details for the exclusion.		
	File name or path	Specifies the file name or path to exclude. The file path can include wildcards. To exclude a folder on Windows systems, append a backslash (\) character to the path. Select **Also exclude subfolders** if necessary.	✓	✓
	File type	Specifies file types (file extensions) to exclude.	✓	✓
	File age	Specifies the access type (**Modified**, **Accessed** (On-Demand Scan only), or **Created**) of files to exclude and the **Minimum age in days**.	✓	✓
When to exclude		Specifies when to exclude the selected item.		
	When writing to or reading from disk	Excludes from scanning when files are being written to or read from disk or other data storage device.	✓	
	When reading from disk	Excludes from scanning when files are being read from the computer or other data storage device.	✓	
	When writing to disk	Excludes from scanning when files are being written to or modified on the disk or other data storage device.	✓	

See also

Threat Prevention — On-Access Scan on page 110
Threat Prevention — On-Demand Scan on page 114
Wildcards in exclusions on page 64
Configuring exclusions on page 63

Threat Prevention — Options

Configure the settings that apply to the Threat Prevention feature, including quarantine, potentially unwanted programs, and exclusions.

This section includes only Advanced options.

Table 3-23 Advanced options

Section	Option	Definition
Quarantine Manager	**Quarantine folder**	Specifies the location for the quarantine folder or accepts the default location: c:\Quarantine The quarantine folder is limited to 190 characters.
	Specify the maximum number of days to keep quarantine data	Specifies the number of days (1–999) to keep the quarantined items before automatically deleting. The default is 30 days.
Exclusion by Detection Name	**Exclude these detection names**	Specifies detection exclusions by detection name. For example, to specify that the on-access scanner and on-demand scanner not detect **Installation Check** threats, enter `Installation Check`. **Add** — Adds a detection name to the exclusion list. Click **Add**, then enter the detection name. *Double-click an item* — Changes the selected item. **Delete** — Removes a detection name from the exclusion list. Select the name, then click **Delete**.
Potentially Unwanted Program Detections	**Exclude custom unwanted programs**	Specifies individual files or programs to treat as potentially unwanted programs. The scanners detect the programs you specify as well as programs specified in the AMCore content files. The scanner doesn't detect a zero-byte sized user-defined unwanted program. • **Add** — Defines a custom unwanted program. Click **Add**, enter the name, then press **Tab** to enter the description. • **Name** — Specifies the file name of the potentially unwanted program. • **Description** — Specifies the information to display as the detection name when a detection occurs. • *Double-click an item* — Changes the selected item. • **Delete** — Removes a potentially unwanted program from the list. Select the program in the table, then click **Delete**.
Proactive Data Analysis		Sends anonymous diagnostic and usage data to McAfee.
	McAfee GTI feedback	Enables McAfee GTI-based telemetry feedback to collect anonymized data on files and processes executing on the client system.

Table 3-23 Advanced options *(continued)*

Section	Option	Definition
	Safety pulse	Performs a health check on the client system before and after AMCore content file updates, and at regular intervals, and sends results to McAfee. The results are encrypted and sent to McAfee using SSL. McAfee then aggregates and analyzes the data from these reports to identify anomalies that might indicate potential content-related issues. Prompt identification of such issues is critical to providing timely containment and remediation. Safety pulse collects the following types of data: • Operating system version and locale • McAfee product version • AMCore content and engine version • McAfee and Microsoft running process information
	AMCore Content Reputation	Performs a McAfee GTI reputation lookup on the AMCore content file before updating the client system. • If McAfee GTI allows the file, Endpoint Security updates AMCore content. • If McAfee GTI doesn't allow the file, Endpoint Security doesn't update AMCore content.

See also

Configure common scan settings on page 79

Roll Back AMCore Content

Changes the AMCore content to a previous version.

Exploit Prevention content updates cannot be rolled back.

Option	Definition
Select version to load	Specifies the version number of a previous AMCore content file to load. Endpoint Security retains the previous two versions on the client system. When you change to a previous version, Endpoint Security removes the current version of AMCore content from the system.

See also

Change the AMCore content version on page 27

4 Using Firewall

The Firewall acts as a filter between your computer and the network or the Internet.

Contents

How Firewall works

The Firewall scans all incoming and outgoing traffic.

As it reviews arriving or departing traffic, the Firewall checks its list of rules, which is a set of criteria with associated actions. If the traffic matches all criteria in a rule, the Firewall acts according to the rule, blocking or allowing traffic through the Firewall.

Information about threat detections is saved for reports that notify the administrator of any security issues for your computer.

Firewall options and rules define how the Firewall works. Rule groups organize firewall rules for easy management.

If the Client Interface Mode is set to **Full access** or you are logged on as administrator, you can configure rules and groups using the Endpoint Security Client. For managed systems, rules and groups that you create might be overwritten when the administrator deploys an updated policy.

See also

Configure Firewall options on page 127
How firewall rules work on page 131
How firewall rule groups work on page 133

Enable and disable Firewall from the McAfee system tray icon

Depending on how settings are configured, you can enable and disable Firewall from the McAfee system tray icon.

These options might not be available, depending on how the settings are configured.

Task

- Right-click the McAfee system tray icon and select **Disable Endpoint Security Firewall** an option from the **Quick Settings** menu.

  When Firewall is enabled, the option is **Disable Endpoint Security Firewall**.

  Depending on settings, you might be prompted to provide your administrator with a reason for disabling Firewall.

Enable or view Firewall timed groups from the McAfee system tray icon

Enable, disable, or view Firewall timed groups from the McAfee system tray icon.

These options might not be available, depending on how the settings are configured.

Task

- Right-click the McAfee system tray icon and select an option from the **Quick Settings** menu.
  - **Enable Firewall Timed Groups** — Enables timed groups for a set amount of time to allow access to the Internet before rules restricting access are applied. When timed groups are enabled, the option is **Disable Firewall Timed Groups**.

    Each time you select this option, you reset the time for the groups.

    Depending on settings, you might be prompted to provide the administrator with a reason for enabling timed groups.

  - **View Firewall Timed Groups** — Displays the names of the timed groups and the amount of time remaining for each group to be active.

About timed groups

Timed groups are Firewall rule groups that are active for a set amount of time.

For example, a timed group can be enabled to allow a client system to connect to a public network and establish a VPN connection.

Depending on settings, groups can be activated either:

- On a specified schedule.
- Manually by selecting options from the McAfee system tray icon.

Managing Firewall

As administrator, you can configure Firewall options and create rules and groups on the Endpoint Security Client.

For managed systems, policy changes from McAfee ePO might overwrite changes from the Settings page.

Modify Firewall options

As administrator, you can modify Firewall options from the Endpoint Security Client.

Tasks

- *Configure Firewall options* on page 127
  Configure settings in Options to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options.
- *Block DNS traffic* on page 128
  To refine firewall protection, create a list of FQDNs to block. Firewall blocks connections to the IP addresses resolving to the domain names.
- *Define networks to use in rules and groups* on page 129
  Define network addresses, subnets, or ranges to use in rules and groups. Optionally, specify that those networks are trusted.
- *Configure trusted executables* on page 130
  Define or edit the list of trusted executables that are considered safe for your environment.

See also

FAQ — McAfee GTI and Firewall on page 128

Configure Firewall options

Configure settings in Options to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Select **Enable Firewall** to make the firewall active and modify its options.

Host Intrusion Prevention 8.0 can be installed on the same system as Endpoint Security version 10.5. If McAfee Host IPS Firewall is installed and enabled, Endpoint Security Firewall is disabled even if enabled in the policy settings.

4 Click **Show Advanced**.

5 Configure settings on the page, then click **Apply** to save your changes or click **Cancel**.

See also

Log on as administrator on page 26

Block DNS traffic

To refine firewall protection, create a list of FQDNs to block. Firewall blocks connections to the IP addresses resolving to the domain names.

> **Before you begin**
>
> The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Firewall** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Under **DNS Blocking**, click **Add**.
4. Enter the FQDN of the domains to block, then click **Save**.

   You can use the ***** and **?** wildcards. For example, *domain.com.

   Duplicate entries are removed automatically.
5. Click **Save**.
6. Click **Apply** to save your changes or click **Cancel**.

FAQ — McAfee GTI and Firewall

Here are answers to frequently asked questions.

Firewall Options settings enable you to block incoming and outgoing traffic from a network connection that McAfee GTI rated as high risk. This FAQ explains what McAfee GTI does and how it affects the firewall.

What is McAfee GTI?

McAfee GTI is a global Internet reputation intelligence system that determines what is good and bad behavior on the Internet. McAfee GTI uses real-time analysis of worldwide behavioral and sending patterns for email, web activity, malware, and system-to-system behavior. Using data obtained from the analysis, McAfee GTI dynamically calculates reputation scores that represent the level of risk to your network when you visit a webpage. The result is a database of reputation scores for IP addresses, domains, specific messages, URLs, and images.

For frequently asked questions about McAfee GTI, see KB53735.

How does McAfee GTI work with Firewall?

When the McAfee GTI options are selected, two firewall rules are created: **McAfee GTI — Allow Endpoint Security Firewall Service** and **McAfee GTI — Get Rating**. The first rule allows a connection to McAfee GTI and the second blocks or allows traffic based on the connection's reputation and the block threshold set.

What do you mean by "reputation"?

For each IP address on the Internet, McAfee GTI calculates a reputation value. McAfee GTI bases the value on sending or hosting behavior and various environmental data collected from customers and partners about the state of Internet threat landscape. The reputation is expressed in four classes, based on our analysis:

- **Do not block** (minimal risk) — This is a legitimate source or destination of content/traffic.
- **High Risk** — This source/destination sends or hosts potentially malicious content/traffic that McAfee considers risky.
- **Medium Risk** — This source/destination shows behavior that McAfee considers suspicious. Any content/traffic from the site requires special scrutiny.
- **Unverified** — This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is needed.

Does McAfee GTI introduce latency? How much?

When McAfee GTI is contacted to do a reputation lookup, some latency is inevitable. McAfee has done everything possible to minimize this latency. McAfee GTI:

- Checks reputations only when the options are selected.
- Uses an intelligent caching architecture. In normal network usage patterns, the cache resolves most wanted connections without a live reputation query.

If the firewall can't reach the McAfee GTI servers, does traffic stop?

If the firewall can't reach any of the McAfee GTI servers, it automatically assigns all applicable connections a default allowed reputation. The firewall then continues analyzing the rules that follow.

Define networks to use in rules and groups

Define network addresses, subnets, or ranges to use in rules and groups. Optionally, specify that those networks are trusted.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Firewall** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Click **Show Advanced**.

4 From **Defined Networks**, do any of the following:

To...	Steps
Define a new network.	Click **Add** and enter the details for the trusted network. Define the network as trusted by selecting **Yes** from the **Trusted** drop-down menu. If you select **No**, the network is defined for use in rules and groups, but incoming and outgoing traffic from the network is not automatically trusted.
Change a network definition.	For each column, double-click the item and enter the new information.
Delete a network.	Select a row, then click **Delete**.

5 Click **Apply** to save your changes or click **Cancel**.

About trusted networks

Trusted networks are IP addresses, IP address ranges, and subnets that your organization considers safe.

Defining a network as trusted creates a bi-directional Allow rule for that remote network at the top of the Firewall rules list.

Once defined, you can create firewall rules that apply to these trusted networks. Trusted networks also function as exceptions to McAfee GTI in the firewall.

Best practice: When adding networks to firewall rules and groups, select **Defined Networks** for the **Network type** to take advantage of this feature.

Configure trusted executables

Define or edit the list of trusted executables that are considered safe for your environment.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Click **Show Advanced**.

4 From **Trusted Executables**, do any of the following:

To...	Steps
Define a new trusted executable.	Click **Add** and enter the details for the trusted executable.
Change an executable definition.	For each column, double-click the item and enter the new information.
Delete an executable.	Select a row, then click **Delete**.

5 Click **Apply** to save your changes or click **Cancel**.

About trusted executables and applications

Trusted executables are executables that have no known vulnerabilities and are considered safe.

Configuring a trusted executable creates a bi-directional Allow rule for that executable at the top of the Firewall rules list.

Maintaining a list of safe executables for a system reduces or eliminates most false positives. For example, when you run a backup application, many false positive events might be triggered. To avoid triggering false positives, make the backup application as a trusted executable.

A trusted executable is susceptible to common vulnerabilities, such as buffer overflow and illegal use. Therefore, Firewall still monitors trusted executables and triggers events to prevent exploits.

The Firewall Catalog contains both executables and applications. Executables in the catalog can be associated with a container *application*. You can add executables and applications from the catalog to your list of trusted executables. Once defined, you can reference the executables in rules and groups.

Configure Firewall rules and groups

As administrator, you can configure Firewall rules and groups from the Endpoint Security Client.

Tasks

- *Create and manage Firewall rules and groups* on page 137
  For managed systems, rules and groups that you configure from the Endpoint Security Client might be overwritten when the administrator deploys an updated policy.
- *Create connection isolation groups* on page 139
  Create a connection isolation firewall rule group to establish a set of rules that apply only when connecting to a network with particular parameters.
- *Create timed groups* on page 139
  Create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

How firewall rules work

Firewall rules determine how to handle network traffic. Each rule provides a set of conditions that traffic must meet and an action to allow or block traffic.

When Firewall finds traffic that matches a rule's conditions, it performs the associated action.

You can define rules broadly (for example, all IP traffic) or narrowly (for example, identifying a specific application or service) and specify options. You can group rules according to a work function, service, or application for easier management. Like rules, you can define rule groups by network, transport, application, schedule, and location options.

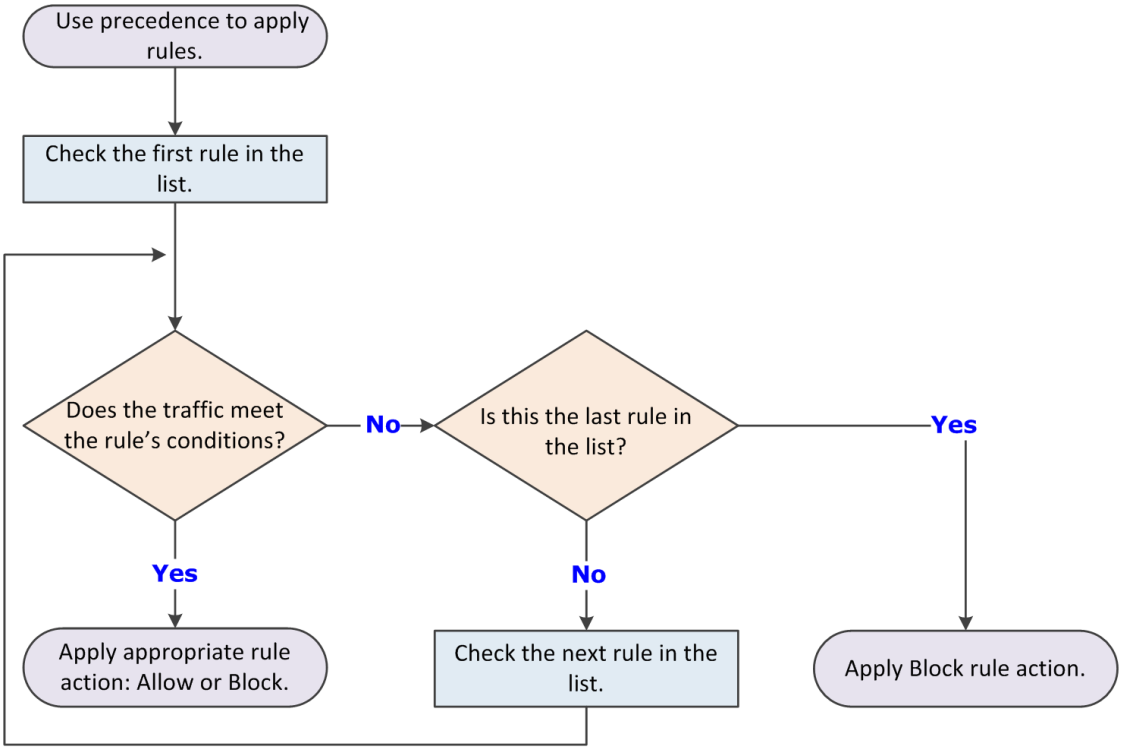
Firewall uses precedence to apply rules:

1 Firewall applies the rule at the top of the firewall rules list.

   If the traffic meets this rule's conditions, Firewall allows or blocks the traffic. It doesn't try to apply any other rules in the list.

2 If the traffic doesn't meet the first rule's conditions, Firewall continues to the next rule in the list until it finds a rule that the traffic matches.

3 If no rule matches, the firewall automatically blocks the traffic.



If Adaptive mode is activated, an Allow Rule is created for the traffic. Sometimes the intercepted traffic matches more than one rule in the list. In this case, precedence means that Firewall applies only the first matching rule in the list.

Best practices

Place the more specific rules at the top of the list, and the more general rules at the bottom. This order makes sure that Firewall filters traffic appropriately.

For example, to allow all HTTP requests except from a specific address (for example, IP address 10.10.10.1), create two rules:

- **Block Rule** — Block HTTP traffic from IP address 10.10.10.1. This rule is specific.
- **Allow Rule** — Allow all traffic using the HTTP service. This rule is general.

Place the Block Rule higher in the firewall rules list than the Allow Rule. When the firewall intercepts the HTTP request from address 10.10.10.1, the first matching rule it finds is the one that blocks this traffic through the firewall.

If the general Allow Rule is higher than the specific Block Rule, Firewall matches requests against the Allow Rule before finding the Block Rule. It allows the traffic, even though you wanted to block the HTTP request from a specific address.

How firewall rule groups work

Use Firewall rule groups to organize firewall rules for easy management. Firewall rule groups don't affect the way Firewall handles the rules within them; Firewall still processes rules from top to bottom.

Firewall processes the settings for the group before processing the settings for the rules it contains. If a conflict exists between these settings, the group settings take precedence.

Making groups location-aware

Firewall enables you to make a group and its rules location-aware and to create connection isolation. The Location and Network Options of the group enable you to make the groups network adapter-aware. Use network adapter groups to apply adapter-specific rules for computers with multiple network interfaces. After enabling location status and naming the location, parameters for allowed connections can include the following for each network adapter:

Location:

- Require that McAfee ePO is reachable
- Connection-specific DNS suffix
- Default gateway IP address
- DHCP server IP address
- DNS server queried to resolve URLs
- Primary WINS server IP address
- Secondary WINS server IP address
- Domain reachability (HTTPS)
- Registry key

Networks:

- Local network IP address
- Connection types

If two location-aware groups apply to a connection, Firewall uses normal precedence, processing the first applicable group in its rule list. If no rule in the first group matches, rule processing continues.

When Firewall matches a location-aware group’s parameters to an active connection, it applies the rules within the group. It treats the rules as a small rule set and uses normal precedence. If some rules don't match the intercepted traffic, the firewall ignores them.

If this option is selected...	Then...
Enable location awareness	A location name is required.
Require that McAfee ePO is reachable	The McAfee ePO is reachable and the FQDN of the server has been resolved.
Local Network	The IP address of the adapter must match one of the list entries.
Connection-specific DNS suffix	The DNS suffix of the adapter must match one of the list entries.
Default gateway	The default adapter gateway IP address must match at least one of the list entries.
DHCP server	The adapter DHCP server IP address must match at least one of the list entries.
DNS server	The adapter DNS server IP address must match any of the list entries.

If this option is selected...	Then...
Primary WINS server	The adapter primary WINS server IP address must match at least one of the list entries.
Secondary WINS server	The adapter secondary WINS server IP address must match at least one of the list entries.
Domain reachability (HTTPS)	The specified domain must be reachable using HTTPS.

Firewall rule groups and connection isolation

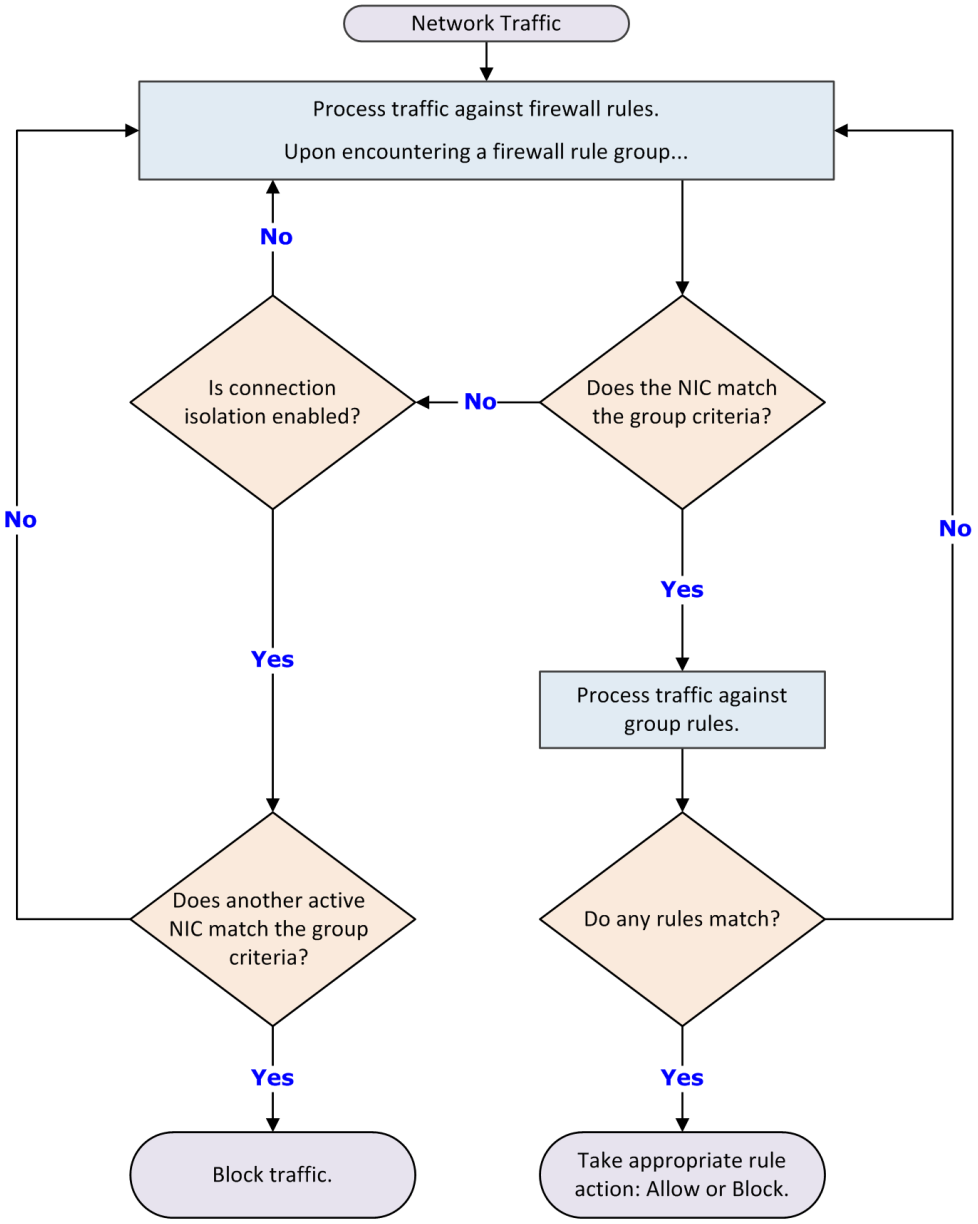
Use connection isolation for groups to prevent undesirable traffic from accessing a designated network.

When connection isolation is enabled for a group, and an active Network Interface Card (NIC) matches the group criteria, Firewall only processes traffic that matches:

- Allow rules above the group in the firewall rules list
- Group criteria

All other traffic is blocked.

Any group with connection isolation enabled can't have associated transport options or executables.



As examples of using connection isolation, consider two settings: a corporate environment and a hotel. The active firewall rules list contains rules and groups in this order:

1 Rules for basic connection

2 VPN connection rules

3 Group with corporate LAN connection rules

4 Group with VPN connection rules

Example: connection isolation on the corporate network

Connection rules are processed until the group with corporate LAN connection rules is encountered. This group contains these settings:

- Connection type = Wired
- Connection-specific DNS suffix = mycompany.com
- Default gateway
- Connection isolation = Enabled

The computer has both LAN and wireless network adapters. The computer connects to the corporate network with a wired connection. However, the wireless interface is still active, so it connects to a hotspot outside the office. The computer connects to both networks because the rules for basic access are at the top of the firewall rules list. The wired LAN connection is active and meets the criteria of the corporate LAN group. The firewall processes the traffic through the LAN but because connection isolation is enabled, all other traffic not through the LAN is blocked.

Example: connection isolation at a hotel

Connection rules are processed until the group with VPN connection rules is encountered. This group contains these settings:

- Connection type = Virtual
- Connection-specific DNS suffix = vpn.mycompany.com
- IP address = An address in a range specific to the VPN concentrator
- Connection isolation = Enabled

General connection rules allow the setup of a timed account at the hotel to gain Internet access. The VPN connection rules allow connection and use of the VPN tunnel. After the tunnel is established, the VPN client creates a virtual adapter that matches the criteria of the VPN group. The only traffic the firewall allows is inside the VPN tunnel and the basic traffic on the actual adapter. Attempts by other hotel guests to access the computer over the network, either wired or wireless, are blocked.

Predefined firewall rule groups

Firewall includes several predefined firewall groups.

Firewall group	Description
McAfee core networking	Contains the core networking rules provided by McAfee and includes rules to allow McAfee applications and DNS. You can't change or delete these rules. You can disable the group in the Firewall Options, but doing so might disrupt network communications on the client.
Admin added	Contains rules defined by the administrator at the management server. These rules can't be changed or deleted on the Endpoint Security Client.
User added	Contains rules defined on the Endpoint Security Client. Depending on policy settings, these rules might be overwritten when the policy is enforced.

Firewall group	Description
Adaptive	Contains client exception rules that are created automatically when the system is in Adaptive mode. Depending on policy settings, these rules might be overwritten when the policy is enforced.
Default	Contains default rules provided by McAfee. These rules can't be changed or deleted.

Create and manage Firewall rules and groups

For managed systems, rules and groups that you configure from the Endpoint Security Client might be overwritten when the administrator deploys an updated policy.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

The groups and rules appear in priority order in the **Firewall Rules** table. You can't sort rules by column.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Firewall** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Use these tasks to manage firewall rules and groups.

To do this...	Follow these steps
View the rules in a firewall group.	Click >.
Collapse a firewall group.	Click v.
Modify an existing rule. You can modify rules in the **User added** group only.	1 Expand the **User added** group. 2 Double-click the rule. 3 Change the rule settings. 4 Click **OK** to save your changes.
View an existing rule in any group.	1 Expand the group. 2 Select the rule to view its details in the bottom pane.
Create a rule.	1 Click **Add Rule**. 2 Specify the rule settings. 3 Click **OK** to save your changes. The rule appears at the end of the **User added** group.

To do this...	Follow these steps
Create copies of rules.	1 Select the rule or rules and click **Duplicate**. Copied rules appear with the same name at the end of the **User added** group. 2 Modify the rules to change the name and settings.
Delete rules. You can delete rules from the **User added** and **Adaptive** groups only.	1 Expand the group. 2 Select the rule or rules and click **Delete**.
Create a group.	1 Click **Add Group**. 2 Specify the group settings. 3 Click **OK** to save your changes. The group appears in the **User added** group.
Move rules and groups within and between groups. You can move rules and groups in the **User added** group only.	To move elements: 1 Select elements to move. The grip appears to the left of elements that can be moved. 2 Drag-and-drop the elements to the new location. A blue line appears between elements where you can drop the dragged elements.

4 Click **Apply** to save your changes or click **Cancel**.

See also

Wildcards in firewall rules on page 138
Log on as administrator on page 26
Create connection isolation groups on page 139

Wildcards in firewall rules

You can use wildcards to represent characters for some values in firewall rules.

Wildcards in path and address values

For paths of files, registry keys, executables, and URLs, use these wildcards.

Registry key paths for firewall group locations don't recognize wildcard values.

?	Question mark	A single character.
*	Asterisk	Multiple characters, excluding slash (/) and backslash (\). Use this character to match the root-level contents of a folder with no subfolders.
**	Double asterisk	Multiple characters, including slash (/) and backslash (\).
|	Pipe	Wildcard escape.

For the double asterisk (**), the escape is |*|*.

Wildcards in all other values

For values that normally don't contain path information with slashes, use these wildcards.

?	Question mark	A single character.
*	Asterisk	Multiple characters, including slash (/) and backslash (\).
|	Pipe	Wildcard escape.

Create connection isolation groups

Create a connection isolation firewall rule group to establish a set of rules that apply only when connecting to a network with particular parameters.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Firewall** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.
3. Under **RULES**, click **Add Group**.
4. Under **Description**, specify options for the group.
5. Under **Location**, select **Enable location awareness** and **Enable connection isolation**. Then, select the location criteria for matching.
6. Under **Networks**, for **Connection types**, select the type of connection (**Wired**, **Wireless**, or **Virtual**) to apply to the rules in this group.

   Settings for **Transport** and **Executables** aren't available for connection isolation groups.
7. Click **OK**.
8. Create new rules within this group, or move existing rules into it from the firewall rule list.
9. Click **Apply** to save your changes or click **Cancel**.

See also

Firewall rule groups and connection isolation on page 134
How firewall rule groups work on page 133

Create timed groups

Create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Firewall** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Firewall** on the **Settings** page.

3 Create a Firewall group with default settings that allow Internet connectivity.

For example, allow port 80 HTTP traffic.

4 In the **Schedule** section, select how to enable the group.

- **Enable schedule** — Specifies a start and end time for the group to be enabled.
- **Disable schedule and enable the group from the McAfee system tray icon** — Allows users to enable the group from the McAfee system tray icon and keeps the group enabled for the specified number of minutes.

  If you allow users to manage the timed group, you can optionally require that they provide a justification before enabling the group.

5 Click **OK** to save your changes.

6 Create a connection isolation group that matches the VPN network to allow necessary traffic.

Best practice: To allow outbound traffic from only the connection isolation group on the client system, don't place any Firewall rules below this group.

7 Click **Apply** to save your changes or click **Cancel**.

See also

Create connection isolation groups on page 139

Endpoint Security Client interface reference — Firewall

Provide context-sensitive help for pages in the Endpoint Security Client interface.

Contents

Firewall — Options

Enable and disable the Firewall module, set protection options, and define networks and trusted executables.

To reset the settings to the McAfee default settings and cancel your changes, click **Reset to Default**.

See the settings in the Common module for logging configuration.

Host Intrusion Prevention 8.0 can be installed on the same system as Endpoint Security version 10.5. If McAfee Host IPS Firewall is installed and enabled, Endpoint Security Firewall is disabled even if enabled in the policy settings.

Table 4-1 Options

Section	Option	Definition
	Enable Firewall	Enables and disables the Firewall module.
Protection Options	**Allow traffic for unsupported protocols**	Allows all traffic that uses unsupported protocols. When disabled, all traffic using unsupported protocols is blocked.

Table 4-1 Options *(continued)*

Section	Option	Definition
	Allow only outgoing traffic until firewall services have started	Allows outgoing traffic but no incoming traffic until the Firewall service starts. If this option is disabled, Firewall allows all traffic before services are started, potentially leaving the system vulnerable.
	Allow bridged traffic	Allows: • **Incoming packets** if the destination MAC address is in the supported VM MAC address range and is not a local MAC address on the system. • **Outgoing packets** if the source MAC address is in the supported MAC address range and is not a local MAC address on the system.
	Enable firewall intrusion alerts	Displays alerts automatically when Firewall detects a potential attack.
DNS Blocking	**Domain name**	Defines domain names to block. When applied, this setting adds a rule near the top of the firewall rules that blocks connections to the IP addresses resolving to the domain names. • **Add** — Adds a domain name to the blocked list. Separate multiple domains with a comma (,) or a carriage return. You can use the ***** and **?** wildcards. For example, *domain.com. Duplicate entries are removed automatically. • *Double-click an item* — Changes the selected item. • **Delete** — Removes the selected domain name from the blocked list.

Table 4-2 Advanced options

Section	Option	Definition
Tuning Options	**Enable Adaptive mode**	Creates rules automatically to allow traffic. **Best practice:** Enable Adaptive mode temporarily on a few systems only while tuning Firewall. Enabling this mode might generate many client rules, which the McAfee ePO server must process, negatively affecting performance.
	Disable McAfee core networking rules	Disables the built-in McAfee networking rules (in the **McAfee core networking** rule group). (Disabled by default) Enabling this option might disrupt network communications on the client.
	Log all blocked traffic	Logs all blocked traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client. (Enabled by default)

Table 4-2 Advanced options *(continued)*

Section	Option	Definition
	Log all allowed traffic	Logs all allowed traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client. (Disabled by default) Enabling this option might negatively affect performance.
McAfee GTI Network Reputation	**Treat McAfee GTI match as intrusion**	Treats traffic that matches the McAfee GTI block threshold setting as an *intrusion*. Enabling this option displays an alert, sends an event to the management server, and adds it Endpoint Security Client log file. Any IP address for a trusted network is excluded from McAfee GTI lookup. (Enabled by default)
	Log matching traffic	Treats traffic that matches the McAfee GTI block threshold setting as a *detection*. Enabling this option sends an event to the management server and adds it to the Endpoint Security Client log file. (Enabled by default) Any IP address for a trusted network is excluded from McAfee GTI lookup.
	Block all untrusted executables	Blocks all executables that are not signed or have an unknown McAfee GTI reputation.
	Incoming network-reputation threshold **Outgoing network-reputation threshold**	Specifies the McAfee GTI rating threshold for blocking incoming or outgoing traffic from a network connection. • **Do not block** — This site is a legitimate source or destination of content/traffic. • **High Risk** — This source/destination sends or hosts potentially malicious content/traffic that McAfee considers risky. • **Medium Risk** — This source/destination shows behavior that McAfee considers suspicious. Any content/traffic from the site requires special scrutiny. • **Unverified** — This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary.
Stateful Firewall	**Use FTP protocol inspection**	Allows FTP connections to be tracked so that they require only one firewall rule for outgoing FTP client traffic and incoming FTP server traffic. If not selected, FTP connections require a separate rule for incoming FTP client traffic and outgoing FTP server traffic.
	Number of seconds (1-240) before TCP connections time out	Specifies the time, in seconds, that an unestablished TCP connection remains active if no more packets matching the connection are sent or received. The valid range is 1–240.
	Number of seconds (1-300) before UDP and ICMP echo virtual connections time out	Specifies the time, in seconds, that a UDP or ICMP Echo virtual connection remains active if no more packets matching the connection are sent or received. This option resets to its configured value every time a packet that matches the virtual connection is sent or received. The valid range is 1–300.

Table 4-2 Advanced options *(continued)*

Section	Option	Definition
Defined Networks		Defines network addresses, subnets, or ranges to use in rules and groups. • **Add** — Adds a network address, subnet, or range to the defined networks list. Click **Add**, then complete fields in the row define the network. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected address from the defined networks list.
	Address type	Specifies the address type of the network to define.
	Trusted	• **Yes** — Allows all traffic from the network. Defining a network as trusted creates a bi-directional Allow rule for that remote network at the top of the Firewall rules list. • **No** — Adds the network to the list of defined networks for creating rules.
	Owner	
Trusted Executables		Specifies executables that are safe in any environment and have no known vulnerabilities. These executables are allowed to perform all operations except operations that suggest that the executables have been compromised. Configuring a trusted executable creates a bi-directional Allow rule for that executable at the top of the Firewall rules list. • **Add** — Adds a trusted executable. • *Double-click an item* — Changes the selected item. • **Delete** — Removes the executable from the trusted list.

See also

Configure Firewall options on page 127
Define networks to use in rules and groups on page 129
Configure trusted executables on page 130
Add Executable or Edit Executable on page 149

Firewall — Rules

Manage firewall rules and groups.

You can add and delete rules and groups in the User added group only. Firewall automatically moves newly added rules to this group.

To reset the settings to the factory default settings and cancel your changes, click **Reset to Default**.

Table 4-3 Options

Section	Option	Definition	Rule	Group
RULES	**Add Rule**	Creates a firewall rule.	✓	
	Add Group	Creates a firewall group.		✓
	Double-click an item	Changes the selected item.	✓	✓
	Duplicate	Creates a copy of the selected item.	✓	✓

Table 4-3 Options *(continued)*

Section	Option	Definition	Rule	Group
	Delete	Removes a selected firewall item.	✓	✓
		Indicates elements that can be moved in the list. Select elements, then drag and drop to the new location. A blue line appears between elements where you can drop the dragged elements.	✓	✓

See also

Create and manage Firewall rules and groups on page 137
Add Rule or Edit Rule, Add Group or Edit Group on page 144

Add Rule or Edit Rule, Add Group or Edit Group

Add or edit firewall rules and groups.

Table 4-4 Options

Section	Option	Definition	Rule	Group
Description	**Name**	Specifies the descriptive name of the item (required).	✓	✓
	Status	Enables or disables the item.	✓	✓
	Specify actions	**Allow** — Allows traffic through the firewall if the item is matched.	✓	
		Block — Stops traffic from passing through the firewall if the item is matched.	✓	
		Treat match as intrusion — Treats traffic that matches the rule as an *intrusion*. Enabling this option displays an alert, sends an event to the management server, and adds it Endpoint Security Client log file. **Best practice:** Don't enable this option for an **Allow** rule because it results in many events.		
		Log matching traffic — Treats traffic that matches the rule as a *detection*. Enabling this option sends an event to the management server and adds it to the Endpoint Security Client log file.	✓	
	Direction	Specifies the direction: • **Either** — Monitors both incoming and outgoing traffic. • **In** — Monitors incoming traffic. • **Out** — Monitors outgoing traffic.	✓	✓
	Notes	Provides more information about the item.	✓	✓
Location	**Enable location awareness**	Enables or disables location information for the group.		✓
	Name	Specifies the name of the location (required).		✓

Table 4-4 Options *(continued)*

Section	Option	Definition	Rule	Group
	Enable connection isolation	Blocks traffic on network adapters that don't match the group when an adapter is present that does match the group. Settings for **Transport** and **Executables** aren't available for connection isolation groups. One use of this option is to block traffic generated by potentially undesirable sources outside the corporate network from entering the corporate network. Blocking traffic in this way is possible only if a rule preceding the group in the firewall hasn't already allowed it. When connection isolation is enabled, and a NIC matches the group, traffic is allowed only when one of the following applies: • Traffic matches an **Allow Rule** before the group. • Traffic traversing a NIC matches the group and there is a rule in or below the group that allows the traffic. If no NIC matches the group, the group is ignored and rule matching continues.		✓
	Require that McAfee ePO is reachable	Enables the group to match only if there is communication with the McAfee ePO server and the FQDN of the server has been resolved.		✓

Table 4-4 Options *(continued)*

Section	Option	Definition	Rule	Group
	Location criteria	• **Connection-specific DNS suffix** — Specifies a connection-specific DNS suffix in the format: `example.com`. • **Default gateway** — Specifies a single IP address for a default gateway in IPv4 or IPv6 format. • **DHCP server** — Specifies a single IP address for a DHCP server in IPv4 or IPv6 format. • **DNS server** — Specifies a single IP address for a domain name server in IPv4 or IPv6 format. • **Primary WINS server** — Specifies a single IP address for a primary WINS server in IPv4 or IPv6 format. • **Secondary WINS server** — Specifies a single IP address for a secondary WINS server in IPv4 or IPv6 format. • **Domain reachability (HTTPS)** — Requires that the specified domain is reachable using HTTPS. • **Registry key** — Specifies the registry key and key value. 1 Click **Add**. 2 In the **Value** column, specify the registry key in the format: `<ROOT>\<KEY>\[VALUE_NAME]` • **<ROOT>** — Must use the full root name, such as HKEY_LOCAL_MACHINE, and not the shortened HKLM. • **<KEY>** — Is the key name under the root. • **[VALUE_NAME]** — is the name of the key value. If no value name is included, it is assumed to be the default value. Example formats: • **IPv4** — `123.123.123.123` • **IPv6** — `2001:db8:c0fa:f340:9219: bd20:9832:0ac7`		
Networks		Specifies the network host options that apply to the item.	✓	✓
	Network protocol	Specifies the network protocol that applies to the item.	✓	✓
	Any protocol	Allows both IP and non-IP protocols. If a transport protocol or an application is specified, only IP protocols are allowed.	✓	✓
	IP protocol	Excludes non-IP protocols. • **IPv4 protocol** • **IPv6 protocol** If neither checkbox is selected, any IP protocol applies. Both IPv4 and IPv6 can be selected.	✓	✓

Table 4-4 Options *(continued)*

Section	Option	Definition	Rule	Group
	Non-IP protocol	Includes non-IP protocols only. • **Select EtherType from list** — Specifies an EtherType. • **Specify custom EtherType** — Specifies the four-characters of the hexadecimal EtherType value of the non-IP protocol. See Ethernet Numbers for EtherType values. For example, enter 809B for AppleTalk, 8191 for NetBEUI, or 8037 for IPX.	✓	✓
	Connection types	Indicates if one or all connection types apply: • **Wired** • **Wireless** • **Virtual** A **Virtual** connection type is an adapter presented by a VPN or a virtual machine application, such as VMware, rather than a physical adapter.	✓	✓
	Specify networks	Specifies the networks that apply to the item. • **Add** — Creates and adds a network. • *Double-click an item* — Changes the selected item. • **Delete** — Removes the network from the list.	✓	✓
Transport		Specifies transport options that apply to the item.		

	Transport protocol	Specifies the transport protocol associated with the item.
		Select the protocol, then click **Add** to add ports.
		• **All protocols** — Allows IP, non-IP, and unsupported protocols.
		• **TCP** and **UDP** — Select from the drop-down:
		  • **Local port** — Specifies the local traffic service or port to which the item applies.
		  • **Remote port** — Specifies the traffic service or port on another computer to which the item applies.
		Local port and **Remote port** can be:
		  • A single service. For example, 23.
		  • A range. For example, 1–1024.
		  • A comma-separated list of single ports and ranges. For example, 80, 8080, 1–10, 8443 (up to 4 items).
		By default, rules apply to all services and ports.
		• **ICMP** — In the **Message type** drop-down, specify an ICMP message type. See ICMP.
		• **ICMPv6** — In the **Message type** drop-down, specify an ICMP message type. See ICMPv6.
		• **Other** — Selects from a list of less common protocols.
			✓	✓

Table 4-4 Options *(continued)*

Section	Option	Definition	Rule	Group
Executables		Specifies the executables that apply to the rule. • **Add** — Creates and adds an executable. • *Double-click an item* — Changes the selected item. • **Delete** — Removes an executable from the list.	✓	✓
Schedule		Specifies schedule settings for the rule or group.	✓	✓
	Enable schedule	Enables the schedule for the timed rule or group. When the schedule is disabled, the rule or rules in the group, don't apply. • **Start time** — Specifies the start time to enable the schedule. • **End time** — Specifies the time to disable the schedule. • *Days of the week* — Specifies the days of the week to enable the schedule. For start and end times, use a 24-hour clock style. For example, 13:00 = 1:00 p.m. You can either schedule Firewall timed groups or allow the user to enable them from the McAfee system tray icon.	✓	✓
	Disable schedule and enable the group from the McAfee system tray icon	Specifies that the user can enable the timed group for a set number of minutes from the McAfee system tray icon instead of using the schedule. **Best practice:** Use this option to allow broad network access, for example at a hotel, before a VPN connection can be established. Selecting this option displays more menu options under **Quick Settings** in the McAfee system tray icon: • **Enable Firewall Timed Groups** — Enables timed groups for a set amount of time to allow access to the Internet before rules restricting access are applied. When timed groups are enabled, the option is **Disable Firewall Timed Groups**. Each time you select this option, you reset the time for the groups. Depending on settings, you might be prompted to provide the administrator with a reason for enabling timed groups. • **View Firewall Timed Groups** — Displays the names of the timed groups and the amount of time remaining for each group to be active.		✓
	Number of minutes (1-60) to enable the group	Specifies the number of minutes (1–60) that the timed group is enabled after selecting **Enable Firewall Timed Groups** from the McAfee system tray icon.		✓

See also

Create and manage Firewall rules and groups on page 137
Create timed groups on page 139
Enable or view Firewall timed groups from the McAfee system tray icon on page 126
Add Network or Edit Network on page 150
Add Executable or Edit Executable on page 149

Add Executable or Edit Executable

Add or edit an executable associated with a rule or group.

Table 4-5 Options

Option	Definition
Name	Specifies the name that you call the executable. This field is required with at least one other field: **File name or path**, **File description**, **MD5 hash**, or signer.
File name or path	Specifies the file name or path of the executable to add or edit. Click **Browse** to select the executable. The file path can include wildcards.
File description	Indicates the description of the file.
MD5 hash	Indicates the (32-digit hexadecimal number) MD5 hash of the process.
Signer	**Enable digital signature check** — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify: • **Allow any signature** — Allows files signed by any process signer. • **Signed by** — Allows only files signed by the specified process signer. A signer distinguished name (SDN) for the executable is required and it must match exactly the entries in the accompanying field, including commas and spaces. The process signer appears in the correct format in the events in the Endpoint Security Client Event Log and McAfee ePO Threat Event Log. For example: C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS To obtain the SDN of an executable: 1 Right-click an executable and select **Properties**. 2 On the **Digital Signatures** tab, select a signer and click **Details**. 3 On the **General** tab, click **View Certificate**. 4 On the **Details** tab, select the **Subject** field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: • CN = Mozilla Corporation • OU = Release Engineering • O = Mozilla Corporation • L = Mountain View • S = California • C = US
Notes	Provides more information about the item.

Add Network or Edit Network

Adds or edits a network associated with a rule or group.

Table 4-6 Options

Option	Definition	Rule	Group
Name	Specifies the network address name (required).	✓	✓
Type	Selects either: • **Local network** — Creates and adds a local network. • **Remote network** — Creates and adds a remote network.	✓	✓
Add	Adds a network type to the network list.	✓	✓
Double-click an item	Changes the selected item.		
Delete	Deletes the selected item.	✓	✓
Address type	Specifies the origin or destination of traffic. Select from the **Address type** drop-down list.	✓	✓
Address	Specifies the IP address to add to the network. Wildcards are valid.	✓	✓

See also

Address type on page 150

Address type

Specify the address type for a defined network.

Table 4-7 Options

Option	Definition
Single IP address	Specifies a particular IP address. For example: • **IPv4** — `123.123.123.123` • **IPv6** — `2001:db8::c0fa:f340:9219:bd20:9832:0ac7*`
Subnet	Specifies the subnet address of any adapter on the network. For example: • **IPv4** — `123.123.123.0/24` • **IPv6** — `2001:db8::0/32`
Local subnet	Specifies the subnet address of the local adapter.
Range	Specifies a range of IP addresses. Enter the starting point and ending point of the range. For example: • **IPv4** — `123.123.1.0 - 123.123.255.255` • **IPv6** — `2001:db8::0000:0000:0000:0000 - 2001:db8::ffff:ffff:ffff:ffff`
Fully qualified domain name	Specifies the FQDN. For example, www.example.com.
Any local IP address	Specifies any local IP address.
Any IPv4 address	Specifies any IPv4 address.
Any IPv6 address	Specifies any IPv6 address.

5 Using Web Control

Web Control protection features appear in your browser while browsing or searching.

Contents

About Web Control features

As Web Control runs on each managed system, it notifies users about threats while they search or browse websites.

A McAfee team analyzes each website and assigns a color-coded safety rating based on test results. The color indicates the level of safety for the site.

The software uses the test results to notify users about web-based threats that they might encounter.

On search results pages — An icon appears next to each site listed. The color of the icon indicates the safety rating for the site. Users can access more information with the icons.

In the browser window — A button appears in the browser. The color of the button indicates the safety rating for the site. Users can access more information by clicking the button.

The button also notifies users when communication problems occur and provides quick access to tests that help identify common issues.

In safety reports — Details show how the safety rating was calculated based on types of threats detected, test results, and other data.

For managed systems, administrators create policies to:

- Enable and disable Web Control on the system, and prevent or allow disabling the browser plug-in.
- Control access to sites, pages, and downloads, based on their safety rating or type of content.

  For example, block red sites and warn users trying to access yellow sites.
- Identify sites as blocked or allowed, based on URLs and domains.
- Prevent users from uninstalling or changing Web Control files, registry keys, registry values, services, and processes.
- Customize the notification that appears when users try to access a blocked website.
- Monitor and regulate browser activity on network computers, and create detailed reports about websites.

For self-managed systems, you can configure settings to:

- Enable and disable Web Control on your system.
- Control access to sites, pages, and downloads, based on their safety rating or type of content.
  For example, block red sites and warn users trying to access yellow sites.

Supported and unsupported browsers

Web Control supports these browsers:

- Microsoft Internet Explorer 11
- Google Chrome — current version

  Chrome doesn't support the **Show Balloon** option.
- Mozilla Firefox — current version
- Mozilla Firefox ESR (Extended Support Release) — current version and previous version

As Google and Mozilla release new versions frequently, Web Control might not work with a new update. A Web Control patch is released as soon as possible to support the changes from Google or Mozilla.

Web Control doesn't support Microsoft Edge.

For the latest information about browsers that Web Control supports, see KB82761.

On self-managed systems, all browsers — supported and unsupported — are allowed by default.

See also

Web Control button identifies threats while browsing on page 153
Safety icons identify threats while searching on page 154
Site reports provide details on page 154
How safety ratings are compiled on page 155

How Web Control blocks or warns a site or download

When a user visits or accesses a resource from a site that has been blocked or warned, Web Control displays a page or pop-up message indicating the reason.

If rating actions for a site are set to:

- **Warn** — Web Control displays a warning to notify users of potential dangers associated with the site.

  Cancel returns to the previously browsed site.

  If the browser tab has no previously viewed site, **Cancel** is unavailable.

  Continue proceeds to the site.
- **Block** — Web Control displays a message that the site is blocked and prevents users from accessing the site.

  OK returns to the previously browsed site.

  If the browser tab has no previously viewed site, **OK** is unavailable.

If rating actions for downloads from a site are set to:

- **Warn** — Web Control displays a warning to notify users of potential dangers associated with the download file.

  Block prevents the download and returns to the site.

  Continue proceeds with the download.

- **Block** — Web Control displays a message that the site is blocked and prevents the download.

  OK returns to the site.

Web Control button identifies threats while browsing

When browsing to a website, a color-coded button 

appears in the browser. The color of the button corresponds to the safety rating for the site.

The safety rating applies to HTTP and HTTPS protocol URLs only.

Internet Explorer and Safari (Macintosh)	Firefox and Chrome	Description
		This site is tested daily and certified safe by McAfee SECURE™. (Windows only)
		This site is safe.
		This site might have some issues.
		This site has some serious issues.
		No rating is available for this site. This button appears for FILE (file:///) protocol URLs.
		A communication error occurred with the McAfee GTI server that contains rating information.
		Web Control didn't query McAfee GTI for this site, which indicates that the site is internal or in a private IP address range.
		This site is a phishing site. Phishing is an attempt to acquire sensitive information such as user names, passwords, and credit card details. Phishing sites masquerade as trustworthy entities in electronic communication.
		A setting allows this site.
		A setting disabled Web Control.

The location of the button depends on the browser:

- **Internet Explorer** — Web Control toolbar
- **Firefox** — Right corner of the Firefox toolbar
- **Chrome** — Address bar

See also

View information about a site while browsing on page 156

Safety icons identify threats while searching

When you type keywords into a search engine such as Google, Yahoo, Bing, or Ask, safety icons appear next to sites in the search results page. The color of the button corresponds to the site's safety rating.


Tests revealed no significant problems.


Tests revealed some issues that you might need to know about. For example, the site tried to change the testers' browser defaults, displayed pop-ups, or sent testers a significant amount of non-spam email.


Tests revealed some serious issues that you must consider carefully before accessing this site. For example, the site sent testers spam email or bundled adware with a download.


A setting blocked this site.


This site is unrated.

See also

View site report while searching on page 157

Site reports provide details

You can view the site report for a website for details about specific threats.

Site reports are delivered from the McAfee GTI ratings server and provide the following information.

This item...	Indicates...
Overview	The overall rating for the website, determined from these tests: • Evaluation of a website's email and download practices using proprietary data collection and analysis techniques. • Examination of the website itself to see if it engages in annoying practices such as excessive pop-ups or requests to change your home page. • Analysis of the website's online affiliations to see if it associates with other suspicious sites. • Combination of the McAfee review of suspicious sites with feedback from our Threat Intelligence services.
Online Affiliations	How aggressively the site tries to get you to go to other sites that McAfee flagged with a red rating. Suspicious sites often associate with other suspicious sites. The primary purpose of *feeder* sites is to get you to visit the suspicious site. A site can receive a red rating if, for example, it links too aggressively to other red sites. In this case, Web Control considers the site *red by association*.
Web Spam Tests	The overall rating for a website's email practices, based on the test results. McAfee rates sites based on how much email we receive after entering an address on the site, and how much the email looks like spam. If either measure is higher than what is considered acceptable, McAfee rates the site yellow. If both measures are high or one looks egregious, McAfee rates the site red.
Download Tests	The overall rating about the impact a site's downloadable software had on our test computer, based on the test results. McAfee gives red flags to sites with virus-infected downloads or to sites that add unrelated software considered by many to be adware or spyware. The rating also considers the network servers that a downloaded program contacts during operation, and any modifications to browser settings or computer registry files.

See also

View site report while searching on page 157
View information about a site while browsing on page 156

How safety ratings are compiled

A McAfee team develops safety ratings by testing criteria for each site and evaluating the results to detect common threats.

Automated tests compile safety ratings for a website by:

- Downloading files to check for viruses and potentially unwanted programs bundled with the download.
- Entering contact information into sign-up forms and checking for resulting spam or a high volume of non-spam email sent by the site or its affiliates.
- Checking for excessive pop-up windows.
- Checking for attempts by the site to exploit browser vulnerabilities.
- Checking for deceptive or fraudulent practices employed by a site.

The team compiles test results into a safety report that can also include:

- Feedback submitted by site owners, which might include descriptions of safety precautions used by the site or responses to user feedback about the site.
- Feedback submitted by site users, which might include reports of phishing scams or bad shopping experiences.
- More analysis by McAfee experts.

The McAfee GTI server stores site ratings and reports.

Access Web Control features

Access Web Control features from the browser.

Tasks

- *Enable the Web Control plug-in from the browser* on page 155
  Depending on settings, you must manually enable the Web Control plug-in to be notified about web-based threats when browsing and searching.
- *View information about a site while browsing* on page 156
  Use the Web Control button on the browser to view information about a site. The button works differently depending on the browser.
- *View site report while searching* on page 157
  Use the safety icon on a search results page to view more information about the site.

Enable the Web Control plug-in from the browser

Depending on settings, you must manually enable the Web Control plug-in to be notified about web-based threats when browsing and searching.

Before you begin
The Web Control module must be enabled.

Plug-ins are also called *add-ons* in Internet Explorer and *extensions* in Firefox and Chrome.

When you first start Internet Explorer or Chrome, you might be prompted to enable plug-ins. For the latest information, see KnowledgeBase article KB87568.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- Depending on the browser, enable the plug-in.

Internet Explorer	• Click **Enable**. • If more than one plug-in is available, click **Choose add-ons**, then click **Enable** for the Web Control toolbar.
Chrome	Click **Enable extension**. If you aren't prompted to enable the Web Control plug-in, you can enable it manually. 1 Click **Settings** | **Extensions**. 2 Click **Enable** to activate Endpoint Security Web Control. 3 Restart Firefox.
Firefox	1 From the Mozilla Firefox Start Page, **Add-ons** | **Extensions**. 2 Select **Enable** to activate Endpoint Security Web Control.

In Internet Explorer, if you disable the Web Control toolbar, you are prompted to also disable the Web Control plug-in. For managed systems, if policy settings prevent uninstalling or disabling the plug-in, the Web Control plug-in remains enabled even though the toolbar isn't visible.

View information about a site while browsing

Use the Web Control button on the browser to view information about a site. The button works differently depending on the browser.

Before you begin

- The Web Control module must be enabled.
- The Web Control plug-in must be enabled in the browser.
- The **Hide the toolbar on the client browser** option in the **Options** settings must be disabled.

When Internet Explorer is in full-screen mode, the Web Control toolbar doesn't appear.

To display the Web Control menu:

Internet Explorer and Firefox	Click the ▼ button in the toolbar.
Chrome	Click the button in the address bar.

Task

1 Display a balloon with a summary of the safety rating for the site: hold the cursor over the button in the Web Control toolbar.

(Internet Explorer and Firefox only)

2 Display the detailed site report, including more information about the site's safety rating:
   - Click the Web Control button.
   - Select **View Site Report** from the Web Control menu.
   - Click the **Read site report** link in the site balloon. (Internet Explorer and Firefox only)

See also
Web Control button identifies threats while browsing on page 153
Site reports provide details on page 154

View site report while searching

Use the safety icon on a search results page to view more information about the site.

Task

1 Place the cursor over the safety icon. Balloon text displays a high-level summary of the safety report for the site.

2 Click **Read site report** (in the balloon) to open a detailed site safety report in another browser window.

See also
Safety icons identify threats while searching on page 154
Site reports provide details on page 154

Managing Web Control

As administrator, you can specify Web Control settings to enable and customize protection, block based on web categories, and configure logging.

For managed systems, policy changes from McAfee ePO might overwrite changes from the Settings page.

Configure Web Control options

You can enable Web Control and configure options from the Endpoint Security Client.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Web Control** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Web Control** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **Options**.

5 Select **Enable Web Control** to make Web Control active and modify its options.

To...	Do this...	Notes
Hide the Web Control toolbar on the browser without disabling protection.	Select **Hide the toolbar on the client browser**.	
Track browser events to use for reports.	Configure settings in the **Event Logging** section.	Configure Web Control events sent from client systems to the management server to use for queries and reports.
Block or warn unknown URLs.	In **Action Enforcement**, select the action (**Block**, **Allow**, or **Warn**) for sites not yet verified by McAfee GTI.	
Scan files before downloading.	In **Action Enforcement**, select **Enable file scanning for file downloads**, then select the McAfee GTI risk level to block.	
Add external sites to the local private network.	In **Action Enforcement**, under **Specify additional IP addresses and ranges to allow**, click **Add**, then enter an external IP address or range.	
Block risky sites from appearing in search results.	In **Secure Search**, select **Enable Secure Search**, select the search engine, then specify whether to block links to risky sites.	Secure Search automatically filters the malicious sites in the search result based on their safety rating. Web Control uses Yahoo as the default search engine and supports Secure Search on Internet Explorer only. If you change the default search engine, restart the browser for the changes to take effect. The next time the user opens Internet Explorer, Web Control displays a pop-up prompting the user to change to McAfee Secure Search with the specified search engine. For Internet Explorer versions where the search engine is locked, the Secure Search pop-up doesn't appear.

6 Configure other options as needed.

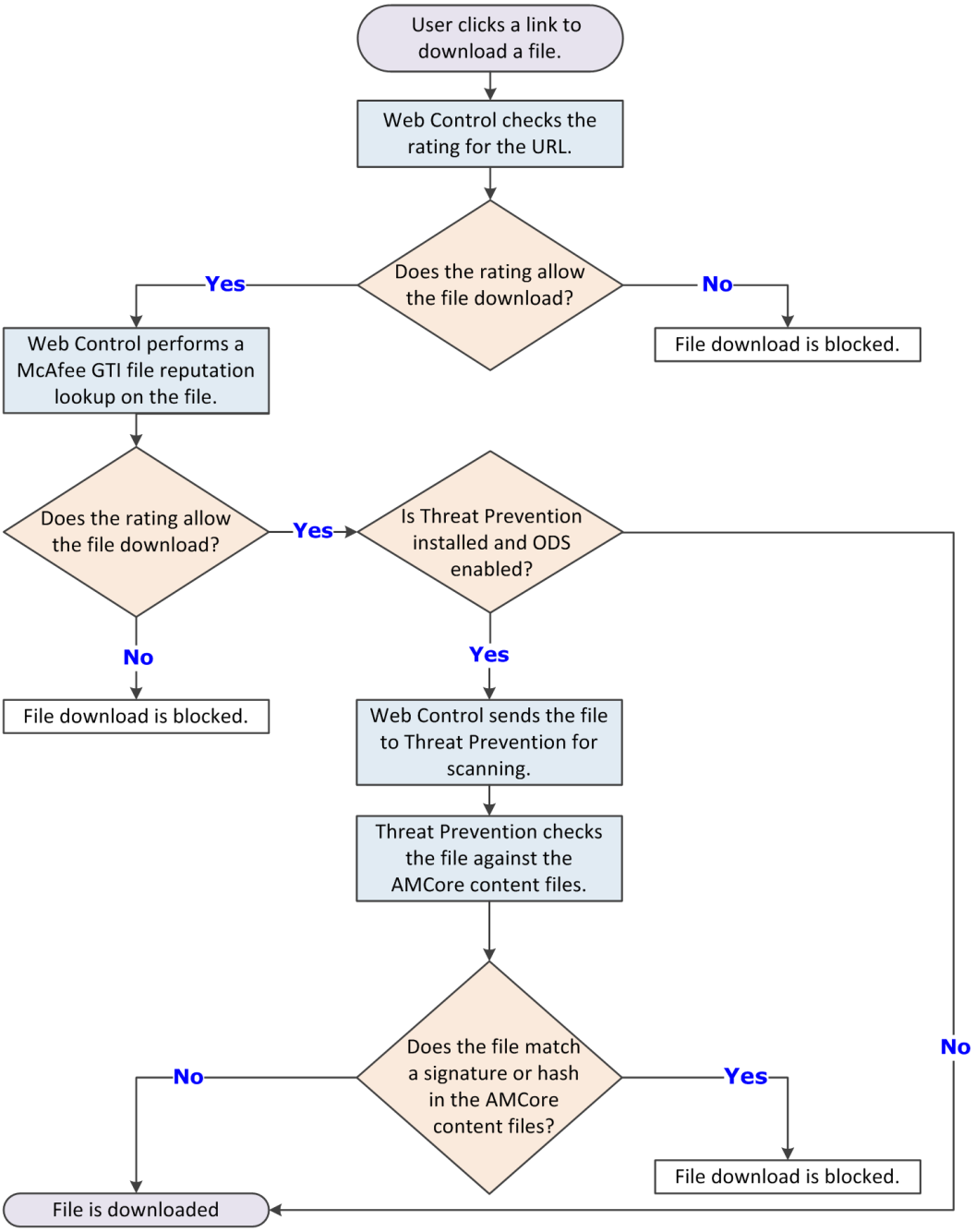
7 Click **Apply** to save your changes or click **Cancel**.

See also

How file downloads are scanned on page 159
Log on as administrator on page 26

How file downloads are scanned

Web Control sends file download requests to Threat Prevention for scanning before downloading.



How McAfee GTI works

The McAfee GTI server stores site ratings and reports for Web Control. If you configure Web Control to scan downloaded files, the scanner uses file reputation provided by McAfee GTI to check for suspicious files.

The scanner submits fingerprints of samples, or *hashes*, to a central database server hosted by McAfee Labs to determine if they are malware. By submitting hashes, detection might be available sooner than the next content file update, when McAfee Labs publishes the update.

You can configure the sensitivity level that McAfee GTI uses when it determines if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. But, allowing more detections can result in more false positive results. The McAfee GTI sensitivity level is set to Very High by default. Configure the sensitivity level for scanning file downloads in the Web Control **Options** policy settings.

You can configure Endpoint Security to use a proxy server to retrieve McAfee GTI reputation information in the Common settings.

For frequently asked questions about McAfee GTI, see KB53735.

Specify rating actions and block site access based on web category

Configure **Content Actions** settings to specify the actions to apply to sites and file downloads, based on safety ratings. Optionally, specify to block or allow sites in each web category.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Web Control** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Web Control** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **Content Actions**.

5 In the **Web Category Blocking** section, for each **Web Category**, enable or disable the **Block** option.

For sites in the unblocked categories, Web Control also applies the rating actions.

6 In the **Rating Actions** section, specify the actions to apply to any sites and file downloads, based on safety ratings defined by McAfee.

These actions also apply to sites that aren't blocked by web category blocking.

7 Click **Apply** to save your changes or click **Cancel**.

See also

Using web categories to control access on page 160
Using safety ratings to control access on page 161
Log on as administrator on page 26

Using web categories to control access

Web categories enable you to control access to sites, based on categories that McAfee defines. You can specify options to allow or block access to sites, based on the category of content they contain.

When you enable web category blocking in the Content Actions settings, the software blocks or allows categories of websites. These web categories include Gambling, Games, and Instant Messaging. McAfee defines and maintains the list of approximately 105 web categories.

When a client user accesses a site, the software checks the web category for the site. If the site belongs to a defined category, access is blocked or allowed, based on the settings in the Content Actions settings. For sites and file downloads in the unblocked categories, the software applies the specified Rating Actions.

Using safety ratings to control access

Configure actions based on safety ratings to determine whether users can access a site, or resources on a site.

In the Content Actions settings, specify whether to allow, warn, or block sites and file downloads, based on the safety rating. This setting enables a greater level of granularity in protecting users against files that might pose a threat on sites with an overall green rating.

Endpoint Security Client interface reference — Web Control

Provide context-sensitive help for pages in the Endpoint Security Client interface.

Contents

Web Control — Options

Configure Web Control options, which include action enforcement, Secure Search, and email annotations.

See the settings in the Common module for logging configuration.

Table 5-1 Options

Section	Option	Definition
OPTIONS	Enable Web Control	Disables or enables Web Control. (Enabled by default)
	Hide the toolbar on the client browser	Hides the Web Control toolbar on the browser without disabling its functionality. (Disabled by default)
Event Logging	Log web categories for green rated sites	Logs content categories for all green-rated sites. Enabling this feature might negatively affect McAfee ePO server performance.
	Log Web Control iFrame events	Logs when malicious (Red) and warn (Yellow) sites that appear in an HTML iframe are blocked.
Action Enforcement	Apply this action to sites not yet verified by McAfee GTI	Specifies the default action to apply to sites that McAfee GTI hasn't yet rated. • **Allow** (Default) — Permits users to access the site. • **Warn** — Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before continuing. • **Block** — Prevents users from accessing the site and displays a message that the site download is blocked.
	Enable HTML iFrames support	Blocks access to malicious (Red) and warn (Yellow) sites that appear in an HTML iframe. (Enabled by default)

Table 5-1 Options *(continued)*

Section	Option	Definition
	Block sites by default if McAfee GTI ratings server is not reachable	Blocks access to websites by default if Web Control can't reach the McAfee GTI server.
	Block phishing pages for all sites	Blocks all phishing pages, overriding content ratings actions. (Enabled by default)
	Enable file scanning for file downloads	Scans all (.zip, .exe, .ecx, .cab, .msi, .rar, .scr, and .com) files before downloading. (Enabled by default) This option prevents users from accessing a downloaded file until Web Control and Threat Prevention mark the file as clean. Web Control performs a McAfee GTI lookup on the file. If McAfee GTI allows the file, Web Control sends the file to Threat Prevention for scanning. If a downloaded file is detected as a threat, Endpoint Security takes action on the file and alerts the user.
	McAfee GTI sensitivity level	Specifies the McAfee GTI sensitivity level that Web Control uses for file downloads.
Exclusions	**Specify IP addresses or ranges to exclude from Web Control rating or blocking**	Adds specified IP addresses and ranges to the local private network, excluding them from rating or blocking. Private IP addresses are excluded by default. **Best practice:** Use this option to treat external sites as if they belong to the local network. • **Add** — Adds an IP address to the list of private addresses in the local network. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes an IP address from the list of private addresses in the local network.
Secure Search	**Enable Secure Search**	Enables Secure Search, automatically blocking malicious sites in search results based on safety rating.
	Set the default search engine in supported browsers	Specifies the default search engine to use for supported browsers: • **Yahoo** • **Google** • **Bing** • **Ask**
	Block links to risky sites in search results	Prevents users from clicking links to risky sites in search results.

Table 5-2 Advanced options

Section	Option	Definition
Email Annotations	**Enable annotations in browser-based email**	Annotates URLs in browser-based email clients, such as Yahoo Mail and Gmail.
	Enable annotations in non browser-based email	Annotates URLs in 32-bit email management tools, such as Microsoft Outlook or Outlook Express.

See also

Configure Web Control options on page 157
How file downloads are scanned on page 159
McAfee GTI on page 163

McAfee GTI

Enable and configure McAfee GTI (Global Threat Intelligence) settings.

Table 5-4 Options

Section	Option	Definition
Sensitivity level		Configures the sensitivity level to use when determining if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. But, allowing more detections might result in more false positive results.
	Very low	The detections and risk of false positives are the same as with regular AMCore content files. A detection is made available to Threat Prevention when McAfee Labs publishes it instead of in the next AMCore content file update. Use this setting for desktops and servers with restricted user rights and strong security configurations.
	Low	This setting is the minimum recommendation for laptops, desktops, and servers with strong security configurations.
	Medium	Use this setting when the regular risk of exposure to malware is greater than the risk of a false positive. McAfee Labs proprietary, heuristic checks result in detections that are likely to be malware. But, some detections might result in a false positive. With this setting, McAfee Labs checks that popular applications and operating system files don't result in a false positive. This setting is the minimum recommendation for laptops, desktops, and servers.
	High	Use this setting for deployment to systems or areas which are regularly infected.
	Very high	Use this setting for non-operating system volumes. Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives. Use this setting only to scan volumes and directories that don't support executing programs or operating systems.

See also

Web Control — Options on page 161

Web Control — Content Actions

Define actions for Web Control to take for rated sites and web content categories.

For sites and file downloads, Web Control applies the rating actions.

Table 5-5 Options

Section	Option	Definition
Rating Actions	Rating actions for sites	Specifies actions for sites that are rated Red or Yellow, or that are unrated. Green-rated sites and downloads are allowed automatically. • **Allow** — Permits users to access the site. (Default for **Unrated** sites) • **Warn** — Displays a warning to notify users of potential dangers associated with the site. Users must click **Cancel** to return to the previously viewed site or **Continue** to proceed to the site. If browser tab has no previously viewed site, **Cancel** is unavailable. (Default for **Yellow** sites) • **Block** — Prevents users from accessing the site and displays a message that the site is blocked. Users must click **OK** to return to the previously viewed site. If browser tab has no previously viewed site, **OK** is unavailable. (Default for **Red** sites)
	Rating actions for file downloads	Specifies actions for file downloads that are rated Red or Yellow, or that are unrated. These Rating Actions are applicable only when **Enable file scanning for file downloads** is enabled in the **Options** settings. • **Allow** — Permits users to proceed with the download. (Default for **Unrated** sites) • **Warn** — Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download. (Default for **Yellow** sites) • **Block** — Displays a message that the download is blocked and prevents users from downloading the file. (Default for **Red** sites)

Table 5-6 Advanced options

Section	Option	Definition
Web Category Blocking	Enable web category blocking	Enables blocking sites based on content category.
	Block	Prevents users from accessing any site in this category and displays a message that the site is blocked.
	Web Category	Lists the web categories.

See also

Specify rating actions and block site access based on web category on page 160
Using safety ratings to control access on page 161
Using web categories to control access on page 160

6 Using Adaptive Threat Protection

Adaptive Threat Protection is an optional Endpoint Security module that analyzes content from your enterprise and decides what to do based on file reputation, rules, and reputation thresholds.

Adaptive Threat Protection isn't supported on systems managed by McAfee ePO Cloud.

Contents

About Adaptive Threat Protection

Adaptive Threat Protection analyzes content from your enterprise and decides what to do based on file reputation, rules, and reputation thresholds.

Adaptive Threat Protection includes the ability to contain, block, or clean files, based on reputation. Adaptive Threat Protection integrates with Real Protect scanning to perform automated reputation analysis in the cloud and on client systems.

Adaptive Threat Protection is an optional Endpoint Security module. For additional threat intelligence sources and functionality, deploy the Threat Intelligence Exchange server. For information, contact your reseller or sales representative.

Adaptive Threat Protection isn't supported on systems managed by McAfee ePO Cloud.

Benefits of Adaptive Threat Protection

Adaptive Threat Protection enables you to determine what happens when a file with a malicious or unknown reputation is detected in your environment. You can also view threat history information and the actions taken.

Adaptive Threat Protection provides these benefits:

- Fast detection and protection against security threats and malware.
- The ability to know which systems or devices are compromised, and how the threat spread through your environment.
- The ability to immediately contain, block, or clean specific files and certificates based on their threat reputations and your risk criteria.

- Integration with Real Protect scanning to perform automated reputation analysis in the cloud and on client systems.
- Real-time integration with McAfee® Advanced Threat Defense and McAfee GTI to provide detailed assessment and data on malware classification. This integration allows you to respond to threats and share the information throughout your environment.

Adaptive Threat Protection components

Adaptive Threat Protection can include the optional components: TIE server and Data Exchange Layer.

Adaptive Threat Protection is an optional Endpoint Security module that enables you to create policies to contain, block, or clean files or certificates based on reputation. In addition, Adaptive Threat Protection integrates with Real Protect scanning to perform automated reputation analysis in the cloud and on client systems.

Adaptive Threat Protection also integrates with:

- **TIE server** — A server that stores information about file and certificate reputations, then passes that information to other systems.

  TIE server is optional. For information about the server, see the *Threat Intelligence Exchange Product Guide*.

- **Data Exchange Layer** — Clients and brokers that enable bidirectional communication between the Adaptive Threat Protection module on the managed system and the TIE server.

  Data Exchange Layer is optional, but it is required for communication with TIE server. See *McAfee Data Exchange Layer Product Guide* for details.

These components include McAfee ePO extensions that add several new features and reports.

If TIE server and Data Exchange Layer are present, Adaptive Threat Protection and the server communicate file reputation information. The Data Exchange Layer framework immediately passes that information to managed endpoints. It also shares information with other McAfee products that access the Data Exchange Layer, such as McAfee® Enterprise Security Manager (McAfee ESM) and McAfee® Network Security Platform.

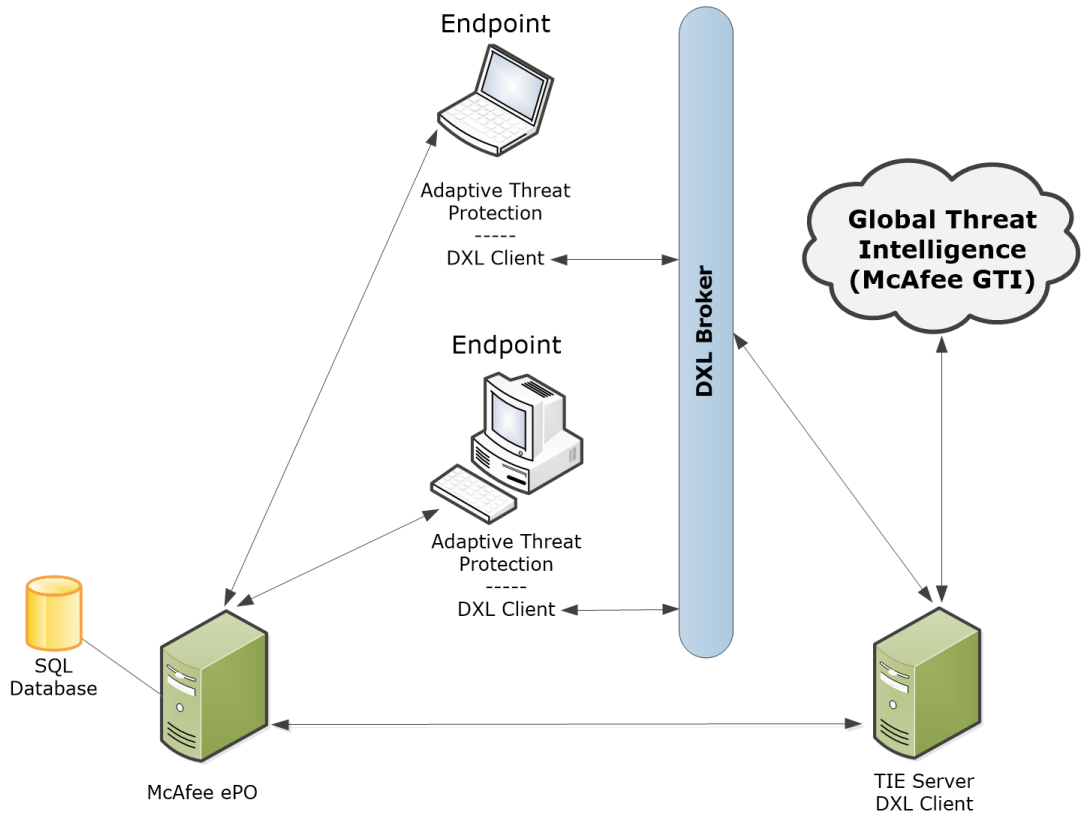


Figure 6-1 Adaptive Threat Protection with TIE server and Data Exchange Layer

If TIE server and Data Exchange Layer are not present, Adaptive Threat Protection communicates with McAfee GTI for file reputation information.

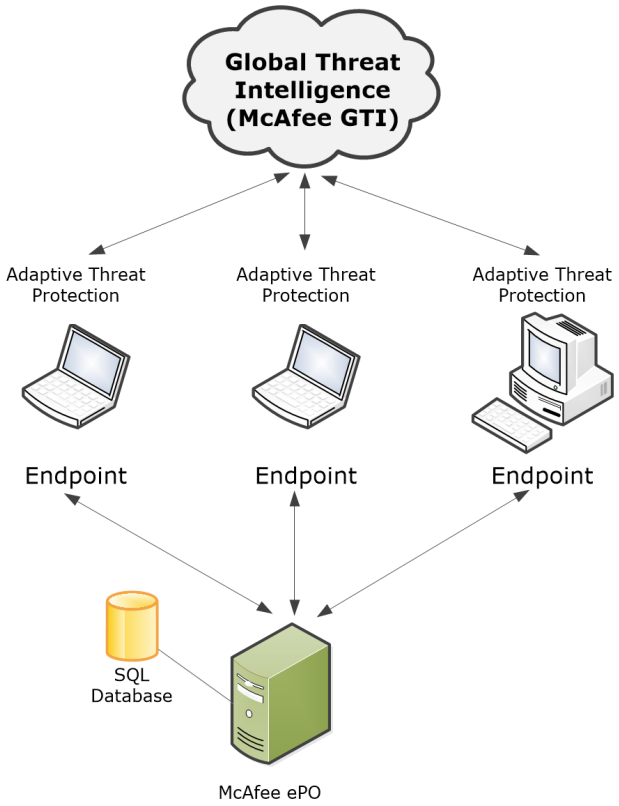


Figure 6-2 Adaptive Threat Protection with McAfee GTI

How Adaptive Threat Protection works

Adaptive Threat Protection uses rules to determine which actions to take based on multiple datapoints such as reputations, local intelligence, and contextual information. You can manage the rules independently.

Adaptive Threat Protection functions differently, depending on whether it is communicating with TIE:

- If TIE server is available, Adaptive Threat Protection uses the Data Exchange Layer framework to share file and threat information instantly across the whole enterprise. You can see the specific system where a threat was first detected, where it went from there, and stop it immediately.

  Adaptive Threat Protection with TIE server enables you to control file reputation at a local level, in your environment. You decide which files can run and which are blocked, and the Data Exchange Layer shares the information immediately throughout your environment.

- If TIE server isn't available and the system is connected to the Internet, Adaptive Threat Protection uses McAfee GTI for reputation decisions.

- If TIE server isn't available and the system isn't connected to the Internet, Adaptive Threat Protection determines the file reputation using information about the local system.

Scenarios for using Adaptive Threat Protection

- **Immediately block a file** — Adaptive Threat Protection alerts the network administrator of an unknown file in the environment. Instead of sending the file information to McAfee for analysis, the administrator blocks the file immediately. The administrator can then use TIE server, if available, to learn how many systems ran the file and Advanced Threat Defense to determine whether the file is a threat.
- **Allow a custom file to run** — A company routinely uses a file whose default reputation is suspicious or malicious, for example a custom file created for the company. Because this file is allowed, instead of sending the file information to McAfee and receiving an updated DAT file, the administrator can change the file's reputation to trusted and allow it to run without warnings or prompts.
- **Allow a file to run in a container** — When a company first uses a file whose reputation is not known, the administrator can specify to allow it to run in a container. In this case, the administrator configures the containment rules in the Dynamic Application Containment settings. Containment rules define which actions the contained application is prevented from performing.

Check connection status

To determine whether Adaptive Threat Protection on the client system gets file reputations from TIE server or McAfee GTI, check the Endpoint Security Client About page.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. From the **Action** menu, select **About**.
3. Click Adaptive Threat Protection on the left.

   The **Connection status** field indicates one of the following for Adaptive Threat Protection:

   - **Threat Intelligence Connectivity** — Connected to TIE server for enterprise-level reputation information.
   - **McAfee GTI Connectivity only** — Connected to McAfee GTI for global-level reputation information.
   - **Disconnected** — Not connected to TIE server or McAfee GTI. Adaptive Threat Protection determines the file reputation using information on the local system.

How a reputation is determined

File and certificate reputation is determined when a file attempts to run on a managed system.

These steps occur in determining a file or certificate's reputation.

1. A user or system attempts to run a file.
2. Endpoint Security checks the exclusions to determine whether to inspect the file.
3. Endpoint Security inspects the file and can't determine its validity and reputation.
4. The Adaptive Threat Protection module inspects the file and gathers file and local system properties of interest.

5 The module checks the local reputation cache for the file hash. If the file hash is found, the module gets the enterprise prevalence and reputation data for the file from the cache.

- If the file hash is not found in the local reputation cache, the module queries the TIE server. If the hash is found, the module gets the enterprise prevalence data (and any available reputations) for that file hash.
- If the file hash is not found in the TIE server or database, the server queries McAfee GTI for the file hash reputation. McAfee GTI sends the information it has available, for example "unknown" or "malicious," and the server stores that information.

  The server sends the file for scanning if both of the following are true:

  - Advanced Threat Defense is available or activated as reputation provider, the server looks locally if the Advanced Threat Defense reputation is present; if not, it marks the file as candidate for submission.
  - The policy on the endpoint is configured to send the file to Advanced Threat Defense.

  See the additional steps under *If Advanced Threat Defense is present*.

6 The server returns the file Hash's enterprise age, prevalence data, and reputation to the module based on the data that was found. If the file is new to the environment, the server also sends a first instance flag to the Adaptive Threat Protection module. If McAfee Web Gateway is present and eventually sends a reputation score, TIE server returns the reputation of the file.

7 The module evaluates this metadata to determine the file's reputation:

- File and system properties
- Enterprise age and prevalence data
- Reputation

8 The module acts based on the policy assigned to the system that is running the file.

9 The module updates the server with the reputation information and whether the file is blocked, allowed, or contained. It also sends threat events to McAfee ePO through the McAfee Agent.

10 The server publishes the reputation change event for the file hash.

If Advanced Threat Defense is present

If Advanced Threat Defense is present, the following process occurs.

1 If the system is configured to send files to Advanced Threat Defense and the file is new to the environment, the system sends the file to the TIE server. The TIE server then sends it to Advanced Threat Defense for scanning.

2 Advanced Threat Defense scans the file and sends file reputation results to the TIE server using the Data Exchange Layer. The server also updates the database and sends the updated reputation information to all Adaptive Threat Protection-enabled systems to immediately protect your environment. Adaptive Threat Protection or any other McAfee product can initiate this process. In either case, Adaptive Threat Protection processes the reputation and saves it in the database.

For information about how Advanced Threat Defense is integrated with Adaptive Threat Protection, see *McAfee Advanced Threat Defense Product Guide*.

If McAfee Web Gateway is present

If McAfee Web Gateway is present, the following occurs.

- When downloading files, McAfee Web Gateway sends a report to the TIE server that saves the reputation score in the database. When the server receives a file reputation request from the module, it returns the reputation received from McAfee Web Gateway and other reputation providers, too.

  For information about how McAfee Web Gateway exchanges information using a TIE server, see the chapter on proxies in the *McAfee Web Gateway Product Guide*.

When is the cache flushed?

- The whole Adaptive Threat Protection cache is flushed when the rules configuration changes:
  - The state of one or more rules has changed, for example from enabled to disabled.
  - The rule set assignment has changed, such as from **Balanced** to **Security**.
- An individual file or certificate cache is flushed when:
  - The cache is over 30 days old.
  - The file has changed on the disk.
  - The TIE server publishes a reputation change event.

  The next time Adaptive Threat Protection receives notice for the file, the reputation is recalculated.

Respond to a file-reputation prompt

When a file with a specific reputation attempts to run on your system, Adaptive Threat Protection might prompt you for input to continue. The prompt appears only if Adaptive Threat Protection is installed and configured to prompt.

The administrator configures the *reputation threshold*, at which point, a prompt is displayed. For example, if the reputation threshold is Unknown, Endpoint Security prompts you for all files with an unknown reputation and below.

If you don't select an option, Adaptive Threat Protection takes the default action configured by the administrator.

The prompt, timeout, and default action depend on how Adaptive Threat Protection is configured.

Windows 8 and 10 use *toast notifications* — messages that pop up to notify you of both alerts and prompts. Click the toast notification to display the notification in Desktop mode.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 (Optional) At the prompt, enter a message to send to the administrator.

  For example, use the message to describe the file or explain your decision to allow or block the file on your system.

2 Click **Allow** or **Block**.

Allow	Allows the file.
Block	Blocks the file on your system.

  To instruct Adaptive Threat Protection not to prompt for the file again, select **Remember this decision**.

Adaptive Threat Protection acts, based on your choice or the default action, and closes the prompt window.

Managing Adaptive Threat Protection

As administrator, you can specify Adaptive Threat Protection settings, such as selecting rule groups, setting reputation thresholds, enabling Real Protect, and configuring Dynamic Application Containment.

For managed systems, policy changes from McAfee ePO might overwrite changes from the Settings page.

Adaptive Threat Protection is an optional Endpoint Security module. For additional threat intelligence sources and functionality, deploy the Threat Intelligence Exchange server. For information, contact your reseller or sales representative.

Adaptive Threat Protection isn't supported on systems managed by McAfee ePO Cloud.

Getting started

After you install Adaptive Threat Protection, what do you do next?

To get started with Adaptive Threat Protection, do the following:

1. Create Adaptive Threat Protection policies to determine what is blocked, allowed, or contained.
2. Run Adaptive Threat Protection in Observe mode to build file prevalence and see what Adaptive Threat Protection detects in your environment. Adaptive Threat Protection generates Would Block, Would Clean, and Would Contain events to show what actions it would take. File prevalence indicates how often a file is seen in your environment.
3. Monitor and adjust the policies, or individual file or certificate reputations, to control what is allowed in your environment.

Building file prevalence and observing

After installation and deployment, start building file prevalence and current threat information.

You can see what is running in your environment and add file and certificate reputation information to the TIE server database. This information also populates the graphs and dashboards available in the module where you view detailed reputation information about files and certificates.

To get started, create one or more Adaptive Threat Protection policies to run on a few systems in your environment. The policies determine:

- When a file or certificate with a specific reputation is allowed to run on a system
- When a file or certificate is blocked
- When an application is contained
- When the user is prompted for what to do
- When a file is submitted to Advanced Threat Defense for further analysis

While building file prevalence, you can run the policies in Observe mode. File and certificate reputations are added to the database, Would Block, Would Clean, and Would Contain events are generated but no action is taken. You can see what Adaptive Threat Protection blocks, allows, or contains if the policy is enforced.

Monitoring and making adjustments

As the policies run in your environment, reputation data is added to the database.

Use the McAfee ePO dashboards and event views to see the files and certificates that are blocked, allowed, or contained based on the policies.

You can view detailed information by endpoint, file, rule, or certificate, and quickly see the number of items identified and the actions taken. You can drill down by clicking an item, and adjust the reputation settings for specific files or certificates so that the appropriate action is taken.

For example, if a file's default reputation is suspicious or unknown but you know it's a trusted file, you can change its reputation to trusted. The application is then allowed to run in your environment without being blocked or prompting the user for action. You might change the reputation for internal or custom files used in your environment.

- Use the TIE Reputations feature to search for a specific file or certificate name. You can view details about the file or certificate, including the company name, SHA-1 and SHA-256 hash values, MD5, description, and McAfee GTI information. For files, you can also access VirusTotal data directly from the TIE Reputations details page to see additional information.
- Use the Reporting Dashboard page to see several types of reputation information at once. You can view the number of new files seen in your environment in the last week, files by reputation, files whose reputations recently changed, systems that recently ran new files, and more. Clicking an item in the dashboard displays detailed information.
- If you identified a harmful or suspicious file, you can quickly see which systems ran the file and might be compromised.
- Change the reputation of a file or certificate as needed for your environment. The information is immediately updated in the database and sent to all devices managed by McAfee ePO. Files and certificates are blocked, allowed, or contained based on their reputation.

  If you're not sure what to do about a specific file or certificate, you can:

  - Block it from running while you learn more about it.

    Unlike a Threat Prevention Clean action, which might delete the file, blocking keeps the file in place but doesn't allow it to run. The file stays intact while you research it and decide what to do.

  - Allow it to run contained.

    Dynamic Application Containment runs applications with specific reputations in a container, blocking actions based on containment rules. The application is allowed to run, but some actions might fail, depending on the containment rules.
- Import file or certificate reputations into the database to allow or block specific files or certificates based on other reputation sources. This allows you to use the imported settings for specific files and certificates without having to set them individually on the server.
- The Composite Reputation column on TIE Reputations page shows the most prevalent reputation and its provider. (TIE server 2.0 and later)
- The Latest Applied Rule column on the TIE Reputations page shows and tracks reputation information based on the latest detection rule applied for each file at the endpoint.

You can customize this page by selecting **Actions** | **Choose Columns**.

Submitting files for further analysis

If a file's reputation is unknown, you can submit it to Advanced Threat Defense for further analysis. Specify in the TIE server policy which files you submit.

Advanced Threat Defense detects zero-day malware and combines anti-virus signatures, reputation, and real-time emulation defenses.You can send files automatically from Adaptive Threat Protection to Advanced Threat Defense based on their reputation level and file size. File reputation information sent from Advanced Threat Defense is added to the TIE server database.

McAfee GTI telemetry information

The file and certificate information sent to McAfee GTI is used to understand and enhance reputation information. See the table for details on the information provided by McAfee GTI for files and certificates, file-only, or certificate-only.

Category	Description
File and certificate	• TIE server and module versions • Reputation override settings made with the TIE server • External reputation information, for example from Advanced Threat Defense
File-only	• File name, type, path, size, product, publisher, and prevalence • SHA-1, SHA-256, and MD5 information • Operating system version of the reporting computer • Maximum, minimum, and average reputation set for the file • Whether the reporting module is in Observe mode • Whether the file was allowed to run, was blocked, contained, or cleaned • The product that detected the file, for example Advanced Threat Defense or Threat Prevention
Certificate-only	• SHA-1 information • The name of the certificate's issuer and its subject • The date the certificate was valid and its expiration date

McAfee does not collect personally identifiable information, and does not share information outside of McAfee.

Containing applications dynamically

Dynamic Application Containment enables you to specify that applications with specific reputations run in a container.

Based on the reputation threshold, Adaptive Threat Protection requests that Dynamic Application Containment run the application in a container. Contained applications aren't allowed to perform certain actions, as specified by containment rules.

This technology lets you evaluate unknown and potentially unsafe applications by allowing them to run in your environment, while limiting the actions they can take. Users can use the applications, but they might not work as expected if Dynamic Application Containment blocks certain actions. Once you determine that an application is safe, you can configure Endpoint Security Adaptive Threat Protection or TIE server to allow it to run normally.

To use Dynamic Application Containment:

1 Enable Adaptive Threat Protection and specify the reputation threshold for triggering Dynamic Application Containment in the **Options** settings.

2 Configure McAfee-defined containment rules and exclusions in the **Dynamic Application Containment** settings.

See also

Allowing contained applications to run normally on page 177
Configure McAfee-defined containment rules on page 178
Enable the Dynamic Application Containment trigger threshold on page 177

How Dynamic Application Containment works

Adaptive Threat Protection uses an application's reputation to determine whether to request that Dynamic Application Containment run the application with restrictions. When a file with the specified reputation runs in your environment, Dynamic Application Containment blocks or logs unsafe actions, based on containment rules.

As applications trigger containment block rules, Dynamic Application Containment uses this information to contribute to the overall reputation of contained applications.

Other technologies, such as McAfee Active Response, can request containment. If multiple technologies registered with Dynamic Application Containment request to contain an application, each request is cumulative. The application remains contained until all technologies release the application. If a technology that has requested containment is disabled or removed, Dynamic Application Containment releases those applications.

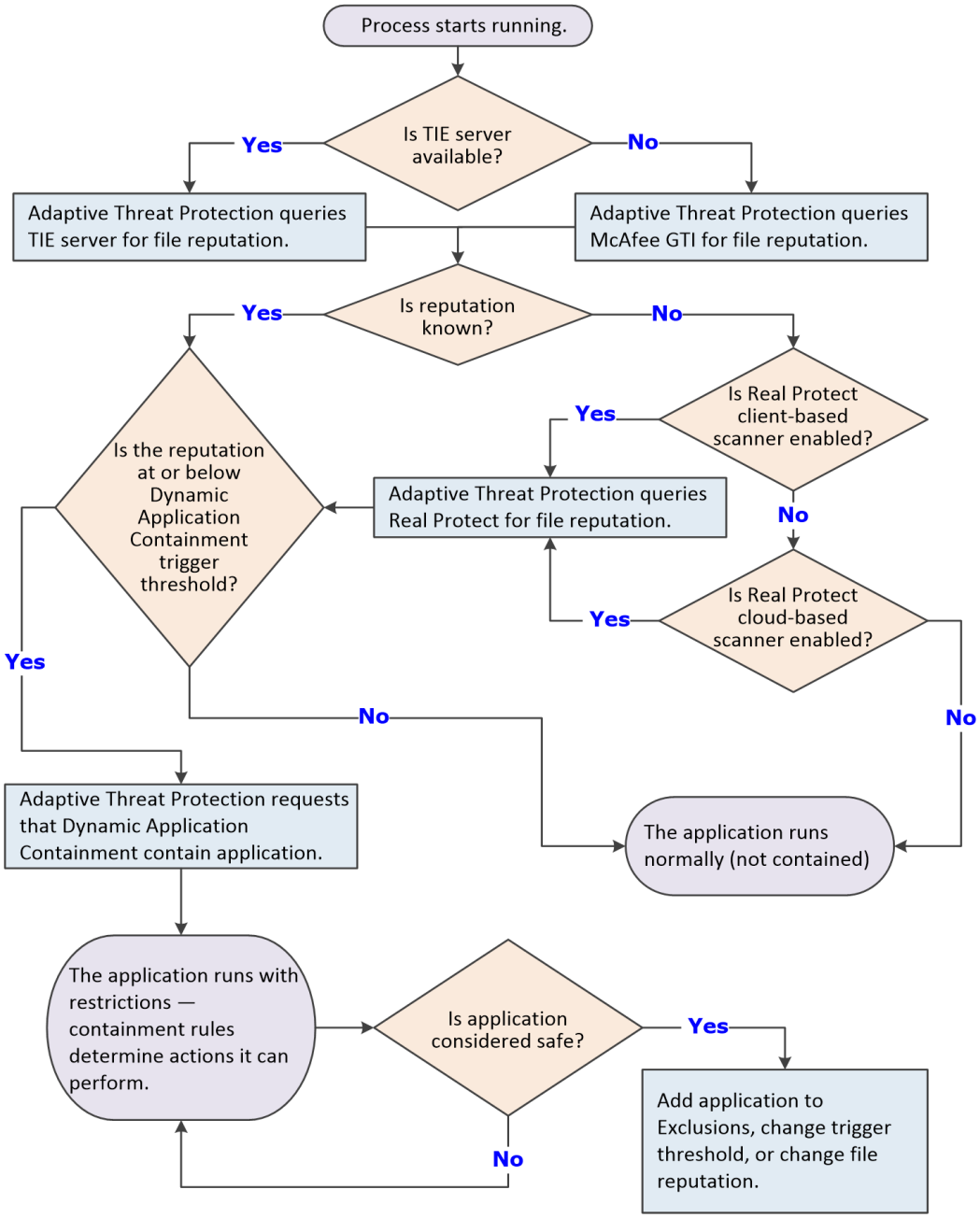
Dynamic Application Containment workflow

1. The process starts running.
2. Adaptive Threat Protection checks the file reputation.

   Adaptive Threat Protection uses TIE server, if it is available, for the application reputation. If TIE server isn't available, Adaptive Threat Protection uses McAfee GTI for reputation information.

   If the reputation isn't known and the Real Protect cloud-based and client-based scanners are enabled, Adaptive Threat Protection queries Real Protect for the reputation.
3. If the application reputation is at or below the containment reputation threshold, Adaptive Threat Protection notifies Dynamic Application Containment that the process has started and requests containment.
4. Dynamic Application Containment contains the process.

   You can view Dynamic Application Containment events in the Threat Event Log in McAfee ePO.
5. If the contained application is considered safe, you can allow it to run normally (not contained).



See also

Allowing contained applications to run normally on page 177

Allowing contained applications to run normally

Once you determine that a contained application is safe, you can allow it to run normally in your environment.

- Add the application to the global Exclusions list in the Dynamic Application Containment settings.

  In this case, the application is released from containment and runs normally, regardless of how many technologies have requested containment.

- Configure Adaptive Threat Protection to raise the reputation threshold and release it from containment.

  In this case, the application is released from containment and runs normally unless another technology has requested to contain the application.

- If TIE server is available, change the reputation of the file to a level that allows it to run, like **Known Trusted**.

  In this case, the application is released from containment and runs normally unless another technology has requested to contain the application.

  See the *McAfee Threat Intelligence Exchange Product Guide.*

See also

Exclude processes from Dynamic Application Containment on page 179

Enable the Dynamic Application Containment trigger threshold

With the *Dynamic Application Containment* technology, you can specify that applications with specific reputations run in a container, limiting the actions they can perform. Enable Dynamic Application Containment action enforcement and specify the reputation threshold at which to contain applications.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Options**.
5. Verify that Adaptive Threat Protection is enabled.
6. Select **Trigger Dynamic Application Containment when reputation threshold reaches**.
7. Specify the reputation threshold at which to contain applications.
   - **Might Be Trusted**
   - **Unknown** (Default for the **Security** rule group)
   - **Might Be Malicious** (Default for the **Balanced** rule group)

- **Most Likely Malicious** (Default for the **Productivity** rule group)
- **Known Malicious**

The Dynamic Application Containment reputation threshold must be higher than the block and clean thresholds. For example, if the block threshold is set to **Known Malicious**, the Dynamic Application Containment threshold must be set to **Most Likely Malicious** or higher.

8 Click **Apply** to save your changes or click **Cancel**.

Configure McAfee-defined containment rules

McAfee-defined *containment rules* block or log actions that contained applications can perform. You can change the block and report settings, but you can't otherwise change or delete these rules.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

For information about Dynamic Application Containment rules, including best practices for when to set a rule to report or block, see KB87843.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 Open the Endpoint Security Client.

2 Click **Adaptive Threat Protection** on the main **Status** page.

Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.

3 Click **Show Advanced**.

4 Click **Dynamic Application Containment**.

5 In the **Containment Rules** section, select **Block**, **Report**, or both for the rule.

- To block or report all, select **Block** or **Report** in the first row.
- To disable the rule, deselect both **Block** and **Report**.

6 In the **Exclusions** section, configure executables to exclude from Dynamic Application Containment.

Processes in the **Exclusions** list run normally (not contained).

7 Click **Apply** to save your changes or click **Cancel**.

See also

Exclude processes from Dynamic Application Containment on page 179

Manage contained applications

When Dynamic Application Containment contains a trusted application, you can *exclude* it from containment from the Endpoint Security Client. Excluding the application releases it, removes it from Contained Applications, and adds it to Exclusions, preventing it from being contained in the future.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Dynamic Application Containment**.
5. In the **Contained Applications** section, select the application and click **Exclude**.
6. On the **Add Executable** page, configure the executable properties, then click **Save**.

   The application appears in the **Exclusions** list. The application remains in the **Contained Applications** list until you click **Apply**. When you return to the **Settings** page, the application appears in the **Exclusions** list only.
7. Click **Apply** to save your changes or click **Cancel**.

Exclude processes from Dynamic Application Containment

If a trusted program is contained, exclude it by creating a Dynamic Application Containment exclusion.

Exclusions created using the Endpoint Security Client apply to the client system only. These exclusions aren't sent to McAfee ePO and don't appear in the Exclusions section in the Dynamic Application Containment settings.

For managed systems, create global exclusions in the Dynamic Application Containment settings in McAfee ePO.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Dynamic Application Containment**.
5. In the **Exclusions** section, click **Add** to add processes to exclude from all rules.
6. On the **Add Executable** page, configure the executable properties.
7. Click **Save**, then click **Apply** to save the settings.

Configure Adaptive Threat Protection options

Adaptive Threat Protection settings determine when a file or certificate is allowed to run, contained, cleaned, blocked, or if users are prompted what to do.

Before you begin

The interface mode for the Endpoint Security Client is set to **Full access** or you are logged on as administrator.

Policy changes from McAfee ePO overwrite changes from the Settings page.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1. Open the Endpoint Security Client.
2. Click **Adaptive Threat Protection** on the main **Status** page.

   Or, from the **Action** menu, select **Settings**, then click **Adaptive Threat Protection** on the **Settings** page.
3. Click **Show Advanced**.
4. Click **Options**.
5. Configure settings on the page, then click **Apply** to save your changes or click **Cancel**.

Blocking or allowing files and certificates

Files and certificates have threat reputations based on their content and properties. The Adaptive Threat Protection policies determine whether files and certificates are blocked or allowed on systems in your environment based on reputation levels.

There are three security levels depending on how you want to balance the rules for particular types of systems. Each level is associated with specific rules that identify malicious and suspicious files and certificates.

- **Productivity** — Systems that change frequently, often installing and uninstalling trusted programs and receiving frequent updates. Examples of these systems are computers used in development environments. Fewer rules are used with policies for this setting. Users see minimum blocking and prompting when new files are detected.
- **Balanced**— Typical business systems where new programs and changes are installed infrequently. More rules are used with policies for this setting. Users experience more blocking and prompting.
- **Security** — IT-managed systems with tight control and little change. Examples are systems that access critical or sensitive information in a financial or government environment. This setting is also used for servers. The maximum number of rules are used with policies for this setting. Users experience even more blocking and prompting.

To view the specific rules associated with each security level, select **Menu** | **Server Settings**. From the Setting Categories list, select **Adaptive Threat Protection**.

When determining which security level to assign a policy, consider the type of system where the policy is used, and how much blocking and prompting you want the user to encounter. After you create a policy, assign it to computers or devices to determine how much blocking and prompting occurs.

Using Real Protect scanning

The Real Protect scanner inspects suspicious files and activities on an endpoint to detect malicious patterns using machine-learning techniques. Using this information, the scanner can detect zero-day malware.

The Real Protect technology is not supported on some Windows operating systems. See KB82761 for information.

The Real Protect scanner provides two options for performing automated analysis:

- In the cloud

  Cloud-based Real Protect collects and sends file attributes and behavioral information to the machine-learning system in the cloud for malware analysis.

  This option requires Internet connectivity to mitigate false positives using McAfee GTI reputation.

  Best practice: Disable cloud-based Real Protect on systems that aren't connected to the Internet.

- On the client system

  Client-based Real Protect uses machine-learning on the client system to determine whether the file matches known malware. If the client system is connected to the Internet, Real Protect sends telemetry information to the cloud, but doesn't use the cloud for analysis.

  If the client system is using TIE for reputations, it doesn't require Internet connectivity to mitigate false positives.

Best practice: Enable both Real Protect options unless Support advises you to deselect one or both to mitigate false positives.

No personally identifiable information (PII) is sent to the cloud.

Endpoint Security Client interface reference — Adaptive Threat Protection

Provide context-sensitive help for pages in the Endpoint Security Client interface.

Contents

Adaptive Threat Protection — Dynamic Application Containment

Protect your system by limiting the actions that contained applications can perform based on configured rules.

Table 6-1 Options

Section	Option	Description
Containment Rules		Configures Dynamic Application Containment rules. You can change whether McAfee-defined containment rules block or report, but you can't otherwise change or delete these rules. • **Block** (only) — Blocks, without logging, contained applications from performing actions specified by the rule. • **Report** (only) — Logs when applications try to perform actions in the rule, but doesn't prevent applications from performing actions. • **Block** and **Report** — Blocks and logs access attempts. **Best practice:** When the full impact of a rule is not known, select **Report** but not **Block** to receive a warning without blocking access attempts. To determine whether to block access, monitor the logs and reports. To block or report all, select **Block** or **Report** in the first row. To disable the rule, deselect both **Block** and **Report**.
Contained Applications		Lists applications that are currently contained. • **Exclude** — Moves a contained application to the **Exclusions** list, releasing it from containment and allowing it to run normally.

Table 6-2 Advanced options

Section	Option	Description
Exclusions		Excludes processes from containment. • **Add** — Adds a process to the exclusion list. • *Double-click an item* — Changes the selected item. • **Delete** — Deletes the selected item. • **Duplicate** — Creates a copy of the selected item.

See also

How Dynamic Application Containment works on page 175
Add Exclusion or Edit Exclusion on page 182
Configure McAfee-defined containment rules on page 178
Exclude processes from Dynamic Application Containment on page 179

Add Exclusion or Edit Exclusion

Add or edit an executable to exclude from Dynamic Application Containment.

When specifying exclusions, consider the following:

- You must specify at least one identifier: File name or path, MD5 hash, or Signer.
- If you specify more than one identifier, all identifiers apply.
- If you specify more than one identifier and they don't match (for example, the file name and MD5 hash don't apply to the same file), the exclusion is invalid.
- Exclusions are case insensitive.
- Wildcards are allowed for all except MD5 hash.

Table 6-3 Options

Option	Definition
Name	Specifies the name that you call the executable. This field is required with at least one other field: **File name or path**, **MD5 hash**, or **Signer**.
File name or path	Specifies the file name or path of the executable to add or edit. Click **Browse** to select the executable. The file path can include wildcards.
MD5 hash	Indicates the (32-digit hexadecimal number) MD5 hash of the process.
Signer	**Enable digital signature check** — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify: • **Allow any signature** — Allows files signed by any process signer. • **Signed by** — Allows only files signed by the specified process signer. A signer distinguished name (SDN) for the executable is required and it must match exactly the entries in the accompanying field, including commas and spaces. The process signer appears in the correct format in the events in the Endpoint Security Client Event Log and McAfee ePO Threat Event Log. For example: C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS To obtain the SDN of an executable: 1 Right-click an executable and select **Properties**. 2 On the **Digital Signatures** tab, select a signer and click **Details**. 3 On the **General** tab, click **View Certificate**. 4 On the **Details** tab, select the **Subject** field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: • CN = Mozilla Corporation • OU = Release Engineering • O = Mozilla Corporation • L = Mountain View • S = California • C = US
Notes	Provides more information about the item.

Adaptive Threat Protection — Options

Configure settings for the Adaptive Threat Protection module.

Table 6-4 Options

Section	Option	Definition
Options	Enable Adaptive Threat Protection	Enables the Adaptive Threat Protection module. (Enabled by default)
	Allow the Threat Intelligence Exchange server to collect anonymous diagnostic and usage data	Allows the TIE server to send anonymous file information to McAfee.
	Use McAfee GTI file reputation if the Threat Intelligence Exchange server is not reachable	Gets file reputation information from the Global Threat Intelligence proxy if the TIE server is unavailable.
	Prevent users from changing settings (Threat Intelligence Exchange 1.0 clients only)	Prevents users on managed systems from changing Threat Intelligence Exchange 1.0 settings.
Rule Assignment	Productivity	Assigns the **Productivity** rule group. Use this group for high-change systems with frequent installations and updates of trusted software. This group uses the least number of rules. Users experience minimum prompts and blocks when new files are detected.
	Balanced	Assigns the **Balanced** rule group. Use this group for typical business systems with infrequent new software and changes. This group uses more rules — and users experience more prompts and blocks — than the **Productivity** group.
	Security	Assigns the **Security** rule group. Use this group for low-change systems, such as IT-managed systems and servers with tight control. Users experience more prompts and blocks than with the **Balanced** group.
Real Protect Scanning	Enable client-based scanning	Enables client-based Real Protect scanning, which uses machine learning on the client system to determine whether the file matches known malware. If the client system is connected to the Internet, Real Protect sends telemetry information to the cloud, but doesn't use the cloud for analysis. If the client system is using TIE for reputations, it doesn't require Internet connectivity to mitigate false positives.  **Best practice:** Select this option unless Support advises you to deselect it to mitigate false positives. The Real Protect technology is not supported on some Windows operating systems. See KB82761 for information.

Table 6-4 Options *(continued)*

Section	Option	Definition
	Enable cloud-based scanning	Enables cloud-based Real Protect scanning, which collects and sends the attributes of the file and its behavioral information to the machine-learning system in the cloud for analysis. This option requires Internet connectivity to mitigate false positives using McAfee GTI reputation.  **Best practice:** Disable cloud-based Real Protect on systems that aren't connected to the Internet. The Real Protect technology is not supported on some Windows operating systems. See KB82761 for information.
Action Enforcement	**Enable Observe mode**	Generates Adaptive Threat Protection events — Would Block, Would Clean, or Would Contain — and sends them to the server, but doesn't enforce actions. Enable Observe mode temporarily on a few systems only while tuning Adaptive Threat Protection.  Because enabling this mode causes Adaptive Threat Protection to generate events but not enforce actions, your systems might be vulnerable to threats.
	Trigger Dynamic Application Containment when reputation threshold reaches	Contains applications when the reputation reaches the specified threshold: • **Might Be Trusted** • **Unknown** (Default for the **Security** rule group) • **Might Be Malicious** (Default for the **Balanced** rule group) • **Most Likely Malicious** (Default for the **Productivity** rule group) • **Known Malicious** The Dynamic Application Containment reputation threshold must be higher than the block and clean thresholds. For example, if the block threshold is set to **Known Malicious**, the Dynamic Application Containment threshold must be set to **Most Likely Malicious** or higher. When an application with the specified reputation threshold tries to run in your environment, Dynamic Application Containment allows it to run in a container and blocks or logs unsafe actions, based on containment rules.

Table 6-4 Options *(continued)*

Section	Option	Definition
	Block when reputation threshold reaches	Blocks files when the file reputation reaches a specific threshold, and specifies the threshold: • **Might Be Trusted** • **Unknown** • **Might Be Malicious** (Default for the **Security** rule group) • **Most Likely Malicious** (Default for the **Balanced** rule group) • **Known Malicious** (Default for the **Productivity** rule group) When a file with the specified reputation threshold tries to run in your environment, it's prevented from running but remains in place. If a file is safe and you want it to run, change its reputation to a level that allows it to run, like Might be Trusted.
	Clean when reputation threshold reaches	Cleans files when the file reputation reaches a specific threshold, and specifies the threshold: • **Might Be Malicious** • **Most Likely Malicious** • **Known Malicious** (Default for the **Balanced** and **Security** rule groups) The default for the **Productivity** rule group is deselected.  **Best practice:** Use this option with Known Malicious file reputations because a file might be removed when cleaned.

Table 6-5 Advanced options

Section	Option	Description
Advanced Threat Defense	**Send files not yet verified to McAfee Advanced Threat Defense for analysis**	Sends executable files to McAfee Advanced Threat Defense for analysis. When enabled, Adaptive Threat Protection sends files securely over HTTPS using port 443 to Advanced Threat Defense when: • The TIE server doesn't have Advanced Threat Defense information about the file. • The file is at or below the specified reputation level. • The file is at or below the specified file size limit. If HTTPS fails, Adaptive Threat Protection sends files over HTTP. Specify information for the Advanced Threat Defense server in the management policy for the TIE server.
	Submit files when reputation threshold reaches	Submits files to Advanced Threat Defense when the file reputation reaches a specified threshold: • **Most Likely Trusted** • **Unknown** • **Most Likely Malicious** The default for all rule groups is **Unknown**.
	Limit size (MB) to	Limits the size of the files sent to Advanced Threat Defense to between 1 MB and 10 MB. The default is 5 MB.

See also

Configure Adaptive Threat Protection options on page 180
Enable the Dynamic Application Containment trigger threshold on page 177
Blocking or allowing files and certificates on page 180
Using Real Protect scanning on page 181

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z