



Product Guide

McAfee Endpoint Security 10.2

## **COPYRIGHT**

© 2016 Intel Corporation

## **TRADEMARK ATTRIBUTIONS**

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

## **LICENSE INFORMATION**

### **License Agreement**

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents

<b>McAfee Endpoint Security</b>	<b>7</b>
<b>1 Introduction</b>	<b>9</b>
Endpoint Security modules . . . . .	9
How Endpoint Security protects your computer . . . . .	10
How your protection stays up to date . . . . .	10
Interacting with Endpoint Security . . . . .	11
Accessing Endpoint Security tasks from the McAfee system tray icon . . . . .	12
About notification messages . . . . .	13
About the Endpoint Security Client . . . . .	14
<b>2 Using the Endpoint Security Client</b>	<b>19</b>
Open the Endpoint Security Client . . . . .	19
Get help . . . . .	20
Respond to prompts . . . . .	20
Respond to a threat-detection prompt . . . . .	20
Respond to a scan prompt . . . . .	21
Respond to a file-reputation prompt . . . . .	21
Get information about your protection . . . . .	22
Management types . . . . .	22
Update protection and software manually . . . . .	23
What gets updated . . . . .	23
View the Event Log . . . . .	24
Endpoint Security log file names and locations . . . . .	25
Managing Endpoint Security . . . . .	27
Log on as administrator . . . . .	27
Unlock the client interface . . . . .	27
Disable and enable features . . . . .	28
Change the AMCore content version . . . . .	28
Use Extra.DAT files . . . . .	29
Configure common settings . . . . .	30
Configure update behavior . . . . .	34
Client Interface Reference — Common . . . . .	39
Event Log page . . . . .	40
Common — Options . . . . .	41
Common — Tasks . . . . .	48
<b>3 Using Threat Prevention</b>	<b>55</b>
Scan your computer for malware . . . . .	55
Types of scans . . . . .	55
Run a Full Scan or Quick Scan . . . . .	56
Scan a file or folder . . . . .	58
Manage threat detections . . . . .	59
Manage quarantined items . . . . .	59
Detection names . . . . .	61

Rescanning quarantined items . . . . .	62
Managing Threat Prevention . . . . .	62
Configuring exclusions . . . . .	63
Protecting your system access points . . . . .	64
Blocking buffer overflow exploits . . . . .	72
Detecting potentially unwanted programs . . . . .	74
Configure common scan settings . . . . .	76
How McAfee GTI works . . . . .	76
Configure On-Access Scan settings . . . . .	77
Configure On-Demand Scan settings . . . . .	81
Configure, schedule, and run scan tasks . . . . .	85
Client Interface Reference — Threat Prevention . . . . .	86
Quarantine page . . . . .	87
Threat Prevention — Access Protection . . . . .	87
Threat Prevention — Exploit Prevention . . . . .	97
Threat Prevention — On-Access Scan . . . . .	101
Threat Prevention — On-Demand Scan . . . . .	105
Scan Locations . . . . .	108
McAfee GTI . . . . .	109
Actions . . . . .	110
Add Exclusion or Edit Exclusion . . . . .	112
Threat Prevention — Options . . . . .	112
Roll Back AMCore Content . . . . .	114
<b>4 Using Firewall . . . . .</b>	<b>115</b>
How Firewall works . . . . .	115
Enable and disable Firewall from the McAfee system tray icon . . . . .	115
Enable or view Firewall timed groups from the McAfee system tray icon . . . . .	116
About timed groups . . . . .	116
Managing Firewall . . . . .	116
Modify Firewall options . . . . .	117
Configure Firewall rules and groups . . . . .	121
Client Interface Reference — Firewall . . . . .	129
Firewall — Options . . . . .	130
Firewall — Rules . . . . .	133
<b>5 Using Web Control . . . . .</b>	<b>141</b>
About Web Control features . . . . .	141
How Web Control blocks or warns a site or download . . . . .	142
Web Control button identifies threats while browsing . . . . .	142
Safety icons identify threats while searching . . . . .	143
Site reports provide details . . . . .	144
How safety ratings are compiled . . . . .	144
Access Web Control features . . . . .	145
Enable the Web Control plug-in from the browser . . . . .	145
View information about a site while browsing . . . . .	146
View site report while searching . . . . .	147
Managing Web Control . . . . .	147
Configure Web Control options . . . . .	147
Specify rating actions and block site access based on web category . . . . .	150
Client Interface Reference — Web Control . . . . .	151
Web Control — Options . . . . .	151
Web Control — Content Actions . . . . .	153
<b>6 Using Threat Intelligence . . . . .</b>	<b>155</b>
How Threat Intelligence works . . . . .	155

Managing Threat Intelligence . . . . .	156
About Threat Intelligence . . . . .	156
Containing applications dynamically . . . . .	162
Configure Threat Intelligence options . . . . .	169
Client Interface Reference — Threat Intelligence . . . . .	170
Threat Intelligence — Dynamic Application Containment . . . . .	170
Threat Intelligence — Options . . . . .	172
<b>Index</b>	<b>177</b>



# 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.

## Getting started

- [Endpoint Security modules on page 9](#)
- [How Endpoint Security protects your computer on page 10](#)
- [Interacting with Endpoint Security on page 11](#)

## Frequently performed tasks

- [Open the Endpoint Security Client on page 19](#)
- [Update protection and software manually on page 23](#)
- [Scan your computer for malware on page 55](#)
- [Unlock the client interface on page 27](#)

## 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 Threat Intelligence 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](#).



Threat Intelligence isn't supported on McAfee ePO Cloud-managed systems.

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

### Contents

- [Endpoint Security modules](#)
- [How Endpoint Security protects your computer](#)
- [Interacting with Endpoint Security](#)

---

## 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.
- **Threat Intelligence** — Provides context-aware adaptive security for your network environment.

Endpoint Security Threat Intelligence 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.



Threat Intelligence isn't supported on McAfee ePO Cloud-managed systems.

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 22](#)

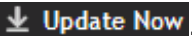
## How your protection stays up to date

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 protection and software manually on page 23](#)

## 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.

### AMCore content

McAfee Labs finds and adds known threat information (*signatures*) to the content files. With the signatures, content files include information on cleaning and counteracting damage that the detected virus can cause.



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

New threats appear regularly. McAfee Labs releases engine updates and new content files that incorporate the results of ongoing threat research daily by 7:00 p.m. (GMT/UTC). If a new threat warrants it, daily AMCore content files might be released earlier and, under some circumstances, releases might be delayed. To receive alerts regarding delays or important notifications, subscribe to the Support Notification Service (SNS). See KnowledgeBase article [KB67828](#).

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. For information about installing Extra.DAT files, see the Threat Prevention Help.

### Exploit Prevention content

The Exploit Prevention content 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.

McAfee releases new Exploit Prevention content files once a month.

### Threat Intelligence content

Threat Intelligence content contains rules to dynamically compute the reputation of files and processes on the endpoints. McAfee releases new Threat Intelligence content files every two months.

Endpoint Security Threat Intelligence 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.

---

## 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 <b>View Security Status</b> to display the <b>McAfee Security Status</b> page.   |
| Open Endpoint Security Client.                  | Select <b>McAfee Endpoint Security</b> .  |
| Update protection and software manually.        | Select <b>Update Security</b> .   |
| Disable or re-enable Firewall.                  | Select <b>Disable Endpoint Security Firewall</b> from the <b>Quick Settings</b> menu.<br>When Firewall is disabled, the option is <b>Enable Endpoint Security Firewall</b> .  |
| Enable, disable, or view Firewall timed groups. | Select an option from the <b>Quick Settings</b> menu: <ul style="list-style-type: none"> <li>• <b>Enable Firewall Timed Groups</b> — 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 <b>Disable Firewall Timed Groups</b>.<br/>Each time you select this option, you reset the time for the groups.<br/>Depending on settings, you might be prompted to provide the administrator with a reason for enabling timed groups.</li> <li>• <b>View Firewall Timed Groups</b> — Displays the names of the timed groups and the amount of time remaining for each group to be active.</li> </ul> |



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.
	<p>Endpoint Security detects an issue with your security, such as a module or technology is disabled.</p> <ul style="list-style-type: none"><li>• Firewall is disabled.</li><li>• Threat Prevention — Exploit Prevention, On-Access Scan, or ScriptScan is disabled.</li></ul> <p>Endpoint Security reports issues differently, depending on the management type.</p> <ul style="list-style-type: none"><li>• Self-managed:<ul style="list-style-type: none"><li>• One or more technologies is disabled.</li><li>• One or more technologies is not responding.</li></ul></li><li>• Managed:<ul style="list-style-type: none"><li>• One or more technologies is disabled, not as a result of a policy enforcement from the management server or from the Endpoint Security Client.</li><li>• One or more technologies is not responding.</li></ul></li></ul> <p>When an issue is detected, the <b>McAfee Security Status</b> page indicates which module or technology is disabled.</p>

**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 Threat Intelligence 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](#)

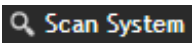

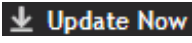

[Respond to a file-reputation prompt on page 21](#)


## 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.
 

<b>Settings</b>	Configures feature settings. This menu option is available if either of the following is true: <ul style="list-style-type: none"> <li>The Client Interface Mode is set to <b>Full access</b>.</li> <li>You are logged on as administrator.</li> </ul>
<b>Load Extra.DAT</b>	Enables you to install a downloaded Extra.DAT file.
<b>Roll Back AMCore Content</b>	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: <ul style="list-style-type: none"> <li>The Client Interface Mode is set to <b>Full access</b>.</li> <li>You are logged on as administrator.</li> </ul>
<b>Help</b>	Displays Help.
<b>Support Links</b>	Displays a page with links to helpful pages, such as the McAfee ServicePortal and Knowledge Center.
<b>Administrator Logon</b>	Logs on as the site administrator. (Requires administrator credentials.) This menu option is available if the Client Interface Mode isn't set to <b>Full access</b> . If you are already logged on as administrator, this option is <b>Administrator Logoff</b> .
<b>About</b>	Displays information about Endpoint Security.
<b>Exit</b>	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.
 

<b>Status</b>	Returns you to the main Status page.
<b>Event Log</b>	Displays the log of all protection and threat events on this computer.
<b>Quarantine</b>	Opens the <b>Quarantine Manager</b> .   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 30](#)  
[Log on as administrator on page 27](#)  
[Scan your computer for malware on page 55](#)  
[Update protection and software manually on page 23](#)  
[View the Event Log on page 24](#)  
[Manage quarantined items on page 59](#)  
[Managing Endpoint Security on page 27](#)  
[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:

<b>Web</b>	Threats from webpages or downloads.
<b>External Device or Media</b>	Threats from external devices, such as USB, 1394 firewire, eSATA, tape, CD, DVD, or disk.
<b>Network</b>	Threats from the network (not network file share).
<b>Local System</b>	Threats from the local boot file system drive (usually C:) or drives other than those classified as External Device or Media.
<b>File Share</b>	Threats from a network file share.
<b>Email</b>	Threats from email messages.
<b>Instant Message</b>	Threats from instant messaging.
<b>Unknown</b>	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.

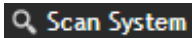
**See also**

[Controlling access to the client interface on page 32](#)

**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:

-  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.

<b>Common</b>	Appears if any module is installed.
<b>Threat Prevention</b>	Appears only if Threat Prevention is installed.
<b>Firewall</b>	Appears only if Firewall is installed.
<b>Web Control</b>	Appears only if Web Control is installed.
<b>Threat Intelligence</b>	Appears only if Threat Intelligence and Threat Prevention are installed.



Threat Intelligence isn't supported on McAfee ePO Cloud-managed systems.



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 15](#)*



# 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*
- ▶ *Get help*
- ▶ *Respond to prompts*
- ▶ *Get information about your protection*
- ▶ *Update protection and software manually*
- ▶ *View the Event Log*
- ▶ *Managing Endpoint Security*
- ▶ *Client Interface Reference — Common*

---

## 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 27*


## 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, 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 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 file-reputation prompt on page 21](#)  
When a file with a specific reputation attempts to run on your system, Endpoint Security might prompt you for input to continue. The prompt appears only if Threat Intelligence is configured to prompt.

## 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.

<b>Scan Now</b>	Starts the scan immediately.
<b>View Scan</b>	Views detections for a scan in progress.
<b>Pause Scan</b>	Pauses the scan. Depending on the configuration, clicking <b>Pause Scan</b> might reset the scan to run only when you're idle. Click <b>Resume Scan</b> to resume the scan where it left off.
<b>Resume Scan</b>	Resumes a paused scan.
<b>Cancel Scan</b>	Cancels the scan.
<b>Defer Scan</b>	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.

## Respond to a file-reputation prompt

When a file with a specific reputation attempts to run on your system, Endpoint Security might prompt you for input to continue. The prompt appears only if Threat Intelligence is configured to prompt.



Threat Intelligence isn't supported on McAfee ePO Cloud-managed systems.

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, Threat Intelligence takes the default action configured by the administrator.



The prompt, timeout, and default action depend on how Threat Intelligence 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**.

<b>Allow</b>	Allows the file.
<b>Block</b>	Blocks the file on your system.


To instruct Threat Intelligence not to prompt for the file again, select **Remember this decision**.

Threat Intelligence acts, based on your choice or the default action, and closes the prompt window.

## 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 <a href="#">KB87057</a> .
Self-Managed	Endpoint Security is managed locally using Endpoint Security Client. This mode is also called <i>unmanaged</i> or <i>standalone</i> .

## Update protection and software manually

Depending on how settings are configured, you can manually check for and download updates to content files and software components from the Endpoint Security Client.

Manual updates are called *on-demand updates*.

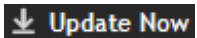
You can also run manual updates from the McAfee system tray icon.



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 .

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

Endpoint Security Client checks for updates.

- To cancel the update, click **Cancel**.
- If your system is up to date, the page displays **No Updates Available** and the date and time of the last update.
- If the update completes successfully, the page displays the current date and time for the last update.

Any messages or 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 25

[What gets updated](#) on page 23

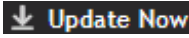

[Configure the default behavior for updates](#) on page 36


[Open the Endpoint Security Client](#) on page 19

## What gets updated

Endpoint Security updates security content, software (hotfixes and patches), and policy settings differently, depending on the management type.

The visibility and behavior of the  button is configurable.

Management type	Update method	Updates
McAfee ePO	<b>Update Security</b> option on the McAfee system tray icon menu	Content and software only, not policy settings.
	 button in the Endpoint Security Client	Content, software, and policy settings, if configured.
McAfee ePO Cloud	<b>Update Security</b> option on the McAfee system tray icon menu	Content, software, and policy settings.
	 button in the Endpoint Security Client	Content, software, and policy settings, if configured.

Management type	Update method	Updates
Self-managed	<b>Update Security</b> option on the McAfee system tray icon menu	Content and software only.
	 <b>Update Now</b> button in the Endpoint Security Client	Content, software, and policy settings, if configured.

**See also**

*Update protection and software manually on page 23*

## 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 <b>Search</b> field and press <b>Enter</b> , or click <b>Search</b> . 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 <b>Search</b> 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 <b>Show all events</b> from the drop-down list.
Refresh the <b>Event Log</b> display with any new events.	Click  .
Open the folder that contains the log files.	Click <b>View Logs Folder</b> .

- 5 Navigate within the Event Log.

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

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 25](#)

[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 in one of the following default locations, depending on the operating system.

Operating system	Default location
Microsoft Windows 10	%ProgramData%\McAfee\Endpoint Security\Logs
Microsoft Windows 8 and 8.1	
Microsoft Windows 7	
Microsoft Vista	C:\Documents and Settings\All Users\Application Data\McAfee\Endpoint Security\Logs

Each module, feature, or technology places activity or debug logging in a separate file. All modules place error logging in a single 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
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	OnDemandScan_Activity.log	
	• Quick Scan	OnDemandScan_Debug.log
	• Full Scan	
	• Right-Click Scan	
	Endpoint Security Client	MFConsole_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
Threat Intelligence		ThreatIntelligence_Activity.log
		ThreatIntelligence_Debug.log
	Dynamic Application Containment	DynamicApplicationContainment_Activity.log
		DynamicApplicationContainment_Debug.log

By default, installation log files are stored in the following locations:

<b>Self-managed</b>	%TEMP%\McAfeeLogs (Windows user TEMP folder)
<b>Managed</b>	TEMP\McAfeeLogs (Windows system 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 27](#)

[Unlock the client interface on page 27](#)

[Disable and enable features on page 28](#)

[Change the AMCore content version on page 28](#)

[Use Extra.DAT files on page 29](#)

[Configure common settings on page 30](#)

## 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 27](#)

**Change the AMCore content version**

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

### 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 27](#)

## 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 30](#)  
To download an Extra.DAT file, click the download link supplied by McAfee Labs.
- [Load an Extra.DAT file on page 30](#)  
To install the downloaded Extra.DAT file, use Endpoint Security Client.

### See also

[About Extra.DAT files on page 29](#)

## 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 27](#)

## 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 31](#)  
One of the first things that malware attempts to do during an attack is to disable your system security software. Configure Self Protection for Endpoint Security in the Common settings to prevent Endpoint Security services and files from being stopped or modified.
- [Configure logging settings on page 31](#)  
Configure Endpoint Security logging in the Common settings.
- [Allow certificate authentication on page 32](#)  
Certificates allow a vendor to run code within McAfee processes.
- [Controlling access to the client interface on page 32](#)  
Control access to the Endpoint Security Client by setting a password in the Common settings.
- [Configure proxy server settings for McAfee GTI on page 33](#)  
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 for Endpoint Security 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 modifying the McAfee database, binaries, safe search files, and configuration files.
  - **Registry** — Prevents users from modifying 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 27](#)

## 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 25*

*Log on as administrator on page 27*

**Allow certificate authentication**

Certificates allow a vendor 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.

**Controlling 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 a password to access Endpoint Security Client settings.

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

**See also**

*Effects of setting an administrator password on page 33*

*Log on as administrator on page 27*



## Effects of setting an administrator password

When you set the interface mode to Standard access, you must also set an administrator password. Setting an administrator password on the Endpoint Security Client affects the following users:

### Non-administrators

(users without administrator rights)

Non-administrators can:

- View some configuration parameters.
- Run scans.
- Check for updates (if enabled).
- View the Quarantine.
- View the Event Log.
- Access the Settings page to view or modify Firewall rules (if enabled).

Non-administrators can't:

- Change any configuration parameters.
  - View, create, delete, or modify settings.
- One exception is the ability to view or modify Firewall rules (if enabled).

### Administrators

(users with administrator rights)

Administrators must type the password to access the protected areas and modify settings.

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

### See also

[How McAfee GTI works on page 33](#)

[Log on as administrator on page 27](#)

### 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 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 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. However, allowing more detections can result in more false positive results.

- For Threat Prevention, the McAfee GTI sensitivity level is set to Medium by default. Configure the sensitivity level for each scanner in the Threat Prevention settings.
- For Web Control, 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** settings.

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

## 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 34](#)  
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 36](#)  
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 37](#)  
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 38](#)  
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.	<ol style="list-style-type: none"> <li>1 Click <b>Add</b>.</li> <li>2 Specify the site settings, then click <b>OK</b>.</li> </ol> <p>The site appears at the beginning of the list.</p>
Change an existing site.	<ol style="list-style-type: none"> <li>1 Double-click the site name.</li> <li>2 Change the settings, then click <b>OK</b>.</li> </ol>
Delete a site.	Select the site, then click <b>Delete</b> .
Import sites from a source site list file.	<ol style="list-style-type: none"> <li>1 Click <b>Import</b>.</li> <li>2 Select the file to import, then click <b>OK</b>.</li> </ol> <div style="text-align: center;">  The site list file replaces the existing source site list.         </div>
Export the source site list to a SiteList.xml file.	<ol style="list-style-type: none"> <li>1 Click <b>Export All</b>.</li> <li>2 Select the location to save the source site list file to, then click <b>OK</b>.</li> </ol>
Reorder sites in the list.	<p>To move elements:</p> <ol style="list-style-type: none"> <li>1 Select elements to move.</li> </ol> <p>The grip  appears to the left of elements that can be moved.</p> <ol style="list-style-type: none"> <li>2 Drag-and-drop the elements to the new location.</li> </ol> <p>A blue line appears between elements where you can drop the dragged elements.</p>

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

[What the repository list contains on page 35](#)

[How the Default Client Update task works on page 37](#)

[Log on as administrator on page 27](#)

[Configure, schedule, and run update tasks on page 37](#)

**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

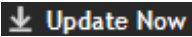
## Configure the default behavior for updates

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  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 27](#)

[Configure source sites for updates on page 34](#)

[Configure, schedule, and run update tasks on page 37](#)

## 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 34](#)

[Configure, schedule, and run update tasks on page 37](#)

[What the repository list contains on page 35](#)

## 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.	<ol style="list-style-type: none"> <li>1 Click <b>Add</b>.</li> <li>2 Enter the name, then from the <b>Select task type</b> drop-down list, select <b>Update</b>.</li> <li>3 Configure the settings, then click <b>OK</b> to save the task.</li> </ol>
Change an update task.	<ul style="list-style-type: none"> <li>• Double-click the task, make your changes, then click <b>OK</b> to save the task.</li> </ul>
Remove a custom update task.	<ul style="list-style-type: none"> <li>• Select the task, then click <b>Delete</b>.</li> </ul>
Create a copy of an update task.	<ol style="list-style-type: none"> <li>1 Select the task, then click <b>Duplicate</b>.</li> <li>2 Enter the name, configure the settings, then click <b>OK</b> to save the task.</li> </ol>
Change the schedule for a <b>Default Client Update</b> task.	<ol style="list-style-type: none"> <li>1 Double-click <b>Default Client Update</b>.</li> <li>2 Click the <b>Schedule</b> tab, change the schedule, then click <b>OK</b> to save the task.</li> </ol> <p>You can also configure the default behavior for client updates initiated from the Endpoint Security Client.</p>
Run an update task.	<ul style="list-style-type: none"> <li>• Select the task, then click <b>Run Now</b>.</li> </ul> <p>If the task is already running, including paused or deferred, the button changes to <b>View</b>.</p> <p>If you run a task before applying changes, Endpoint Security Client prompts you to save the settings.</p>

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

### See also

*How the Default Client Update task works on page 37*

*Configure source sites for updates on page 34*

*Configure the default behavior for updates on page 36*

## 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.	<ol style="list-style-type: none"> <li>1 Click <b>Add</b>.</li> <li>2 Enter the name, then from the <b>Select task type</b> drop-down list, select <b>Mirror</b>.</li> <li>3 Configure the settings, then click <b>OK</b>.</li> </ol>
Change a mirror task.	<ul style="list-style-type: none"> <li>• Double-click the mirror task, make your changes, then click <b>OK</b>.</li> </ul>
Remove a mirror task.	<ul style="list-style-type: none"> <li>• Select the task, then click <b>Delete</b>.</li> </ul>
Create a copy of a mirror task.	<ol style="list-style-type: none"> <li>1 Select the task, then click <b>Duplicate</b>.</li> <li>2 Enter the name, configure the settings, then click <b>OK</b>.</li> </ol>
Schedule a mirror task.	<ol style="list-style-type: none"> <li>1 Double-click the task.</li> <li>2 Click the <b>Schedule</b> tab, change the schedule, then click <b>OK</b> to save the task.</li> </ol>
Run a mirror task.	<ul style="list-style-type: none"> <li>• Select the task, then click <b>Run Now</b>.</li> </ul> <p>If the task is already running, including paused or deferred, the button changes to <b>View</b>.</p> <p>If you run a task before applying changes, Endpoint Security Client prompts you to save the settings.</p>

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.

---

## Client Interface Reference — Common

The interface reference help topics provide context-sensitive help for pages in the client interface.


### Contents

- ▶ [Event Log page](#)
- ▶ [Common — Options](#)
- ▶ [Common — Tasks](#)

## Event Log page

Displays the activity and debug events in the Event Log.

**Table 2-2 Options**

Option	Definition										
<b>Number of events</b>	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.										
<b>View Logs Folder</b>	Opens the folder that contains the log files in Windows Explorer.										
<b>Show all events</b>	Removes any filter.										
<b>Filter by Severity</b>	Filters events by a severity level: <table border="0" style="margin-left: 20px;"> <tr> <td><b>Alert</b></td> <td>Shows level 1 severity events only.</td> </tr> <tr> <td><b>Critical and greater</b></td> <td>Shows levels 1 and 2 severity events only.</td> </tr> <tr> <td><b>Warning and greater</b></td> <td>Shows levels 1, 2, and 3 severity events only.</td> </tr> <tr> <td><b>Notice and greater</b></td> <td>Shows levels 1, 2, 3, and 4 severity levels.</td> </tr> </table>	<b>Alert</b>	Shows level 1 severity events only.	<b>Critical and greater</b>	Shows levels 1 and 2 severity events only.	<b>Warning and greater</b>	Shows levels 1, 2, and 3 severity events only.	<b>Notice and greater</b>	Shows levels 1, 2, 3, and 4 severity levels.		
<b>Alert</b>	Shows level 1 severity events only.										
<b>Critical and greater</b>	Shows levels 1 and 2 severity events only.										
<b>Warning and greater</b>	Shows levels 1, 2, and 3 severity events only.										
<b>Notice and greater</b>	Shows levels 1, 2, 3, and 4 severity levels.										
<b>Filter by Module</b>	Filters events by module: <table border="0" style="margin-left: 20px;"> <tr> <td><b>Common</b></td> <td>Shows Common events only.</td> </tr> <tr> <td><b>Threat Prevention</b></td> <td>Shows Threat Prevention events only.</td> </tr> <tr> <td><b>Firewall</b></td> <td>Shows Firewall events only.</td> </tr> <tr> <td><b>Web Control</b></td> <td>Shows Web Control events only.</td> </tr> <tr> <td><b>Threat Intelligence</b></td> <td>Shows Threat Intelligence events only.</td> </tr> </table> <p>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.</p>	<b>Common</b>	Shows Common events only.	<b>Threat Prevention</b>	Shows Threat Prevention events only.	<b>Firewall</b>	Shows Firewall events only.	<b>Web Control</b>	Shows Web Control events only.	<b>Threat Intelligence</b>	Shows Threat Intelligence events only.
<b>Common</b>	Shows Common events only.										
<b>Threat Prevention</b>	Shows Threat Prevention events only.										
<b>Firewall</b>	Shows Firewall events only.										
<b>Web Control</b>	Shows Web Control events only.										
<b>Threat Intelligence</b>	Shows Threat Intelligence events only.										
<b>Search</b>	Searches the Event Log for a string.										
<b>Events per page</b>	Selects the number of events to display on a page. (By default, 20 events per page)										
<b>Previous page</b>	Displays the previous page in the Event Log.										
<b>Next page</b>	Displays the next page in the Event Log.										
<b>Page x of x</b>	Selects a page in the Event Log to navigate to. Enter a number in the <b>Page</b> field and press <b>Enter</b> or click <b>Go</b> to navigate to the page.										
Column heading	Sorts the event list by...										
<b>Date</b>	Date the event occurred.										
<b>Feature</b>	Feature that logged the event.										



Column heading	Sorts the event list by...
<b>Action taken</b>	<p>Action that Endpoint Security took, if any, in response to the event. The action is configured in the settings.</p> <p><b>Allowed</b> Allowed access to file.</p> <p><b>Access Denied</b> Prevented access to file.</p> <p><b>Deleted</b> Deleted file automatically.</p> <p><b>Continue</b></p> <p><b>Cleaned</b> Removed the threat from the file automatically.</p> <p><b>Moved</b> Moved the file into the Quarantine.</p> <p><b>Blocked</b> Blocked access to the file.</p> <p><b>Would Block</b> An Access Protection rule would have blocked access to the file if the rule was being enforced.</p>
<b>Severity</b>	<p>Severity level of the event.</p> <p><b>Critical</b> 1</p> <p><b>Major</b> 2</p> <p><b>Minor</b> 3</p> <p><b>Warning</b> 4</p> <p><b>Informational</b> 5</p>

**See also**

[View the Event Log on page 24](#)

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



**Table 2-3 Options** (continued)

Section	Option	Definition
	<b>Set Administrator password</b>	For <b>Standard access</b> and <b>Lock client interface</b> , specifies the administrator password for accessing all features of the Endpoint Security Client interface. <ul style="list-style-type: none"> <li>• <b>Password</b> — Specifies the password.</li> <li>• <b>Confirm password</b> — Confirms the password.</li> </ul>
Uninstallation	<b>Require password to uninstall the client</b>	Requires a password to uninstall Endpoint Security Client and specifies the password. The default password is <code>mcafee</code> . (Disabled by default) <ul style="list-style-type: none"> <li>• <b>Password</b> — Specifies the password.</li> <li>• <b>Confirm password</b> — Confirms the password.</li> </ul>

**Table 2-4 Advanced options**

Section	Option	Definition
Client Interface Language	<b>Automatic</b>	Automatically selects the language to use for Endpoint Security Client interface text based on the language on the client system.
	<i>Language</i>	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	<b>Enable Self Protection</b>	Protects Endpoint Security system resources from malicious activity.
	<b>Action</b>	Specifies the action to take when malicious activity occurs: <ul style="list-style-type: none"> <li>• <b>Block and report</b> — Blocks activity and reports to McAfee ePO. (Default)</li> <li>• <b>Block only</b> — Blocks activity but doesn't report to McAfee ePO.</li> <li>• <b>Report only</b> — Reports to McAfee ePO but doesn't block activity.</li> </ul>
	<b>Files and folders</b>	Prevents changing or deleting McAfee system files and folders.
	<b>Registry</b>	Prevents changing or deleting McAfee registry keys and values.
	<b>Processes</b>	Prevents stopping McAfee processes.
	<b>Exclude these processes</b>	Allows access for the specified processes. Wildcards are supported.  <b>Add</b> — Adds a process to the exclusion list. Click <b>Add</b> , then enter the exact resource name, such as <code>avtask.exe</code> .  <i>Double-click an item</i> — Changes the selected item.  <b>Delete</b> — Deletes the selected item. Select the resource, then click <b>Delete</b> .
	<b>Certificates</b>	Specifies certificate options.

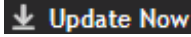
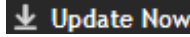

**Table 2-4 Advanced options** (continued)

Section	Option	Definition
	Allow	Allows a vendor to run code within 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: <ul style="list-style-type: none"> <li>• <b>CN</b> — Common Name</li> <li>• <b>OU</b> — Organization Unit</li> <li>• <b>O</b> — Organization</li> <li>• <b>L</b> — Locality</li> <li>• <b>ST</b> — State or province</li> <li>• <b>C</b> — Country Code</li> </ul>
	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:  <code>&lt;SYSTEM_DRIVE&gt;:\ProgramData\McAfee\Endpoint\Logs</code>  Enter or click <b>Browse</b> 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. Disable this option to allow log files to grow to any size.
Debug Logging		Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.   <b>Best practice:</b> 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.
	Enable for Threat Prevention	Enables verbose logging for Threat Prevention and individual technologies: <b>Enable for Access Protection</b> — Logs to AccessProtection_Debug.log. <b>Enable for Exploit Prevention</b> — Logs to ExploitPrevention_Debug.log. <b>Enable for On-Access Scan</b> — Logs to OnAccessScan_Debug.log. <b>Enable for On-Demand Scan</b> — 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 Firewall activity.


**Table 2-4 Advanced options** (continued)

Section	Option	Definition
	Enable for Web Control	Enables verbose logging of Web Control activity.
	Enable for Threat Intelligence	Enables verbose logging of Threat Intelligence activity.
	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. Disable this option to allow log files to grow to any size.
Event Logging	Send events to McAfee ePO	Sends all events logged to the <b>Event Log</b> 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 <b>Event Log</b> on the Endpoint Security Client to the Windows Application log. The Windows Application log is accessible from the Windows <b>Event Viewer</b>   <b>Windows Logs</b>   <b>Application</b> .
	Severity levels	Specifies the severity level of events to log to the <b>Event Log</b> on the Endpoint Security Client: <ul style="list-style-type: none"> <li>• <b>None</b> — Sends no alerts</li> <li>• <b>Alert only</b> — Sends alert level 1 only.</li> <li>• <b>Critical and Alert</b> — Sends alert levels 1 and 2.</li> <li>• <b>Warning, Critical, and Alert</b> — Sends alert levels 1–3.</li> <li>• <b>All except Informational</b> — Sends alert levels 1–4.</li> <li>• <b>All</b> — Sends alert levels 1–5.</li> <li>• 1 — Alert</li> <li>• 2 — Critical</li> <li>• 3 — Warning</li> <li>• 4 — Notice</li> <li>• 5 — Informational</li> </ul>
	Threat Prevention events to log	Specifies the severity level of events for each Threat Prevention feature to log: <p><b>Access Protection</b> — Logs to AccessProtection_Activity.log. Enabling event logging for Access Protection also enables event logging for Self Protection.</p> <p><b>Exploit Prevention</b> — Logs to ExploitPrevention_Activity.log.</p> <p><b>On-Access Scan</b> — Logs to OnAccessScan_Activity.log.</p> <p><b>On-Demand Scan</b> — Logs to OnDemandScan_Activity.log.</p>
	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.
	Threat Intelligence events to log	Specifies the severity level of Threat Intelligence events to log.

**Table 2-4 Advanced options** *(continued)*

Section	Option	Definition
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. <ul style="list-style-type: none"> <li>• <b>Address</b> — Specifies the IP address or fully qualified domain name of the HTTP proxy server.</li> <li>• <b>Port</b> — Limits access through the specified port.</li> <li>• <b>Exclude these addresses</b> — Don't use the HTTP proxy server for websites or IP addresses that begin with the specified entries. Click <b>Add</b>, then enter the address name to exclude.</li> </ul>
	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: <ul style="list-style-type: none"> <li>• <b>User name</b> — Specifies the user account with permissions to access the HTTP proxy server.</li> <li>• <b>Password</b> — Specifies the password for <b>User name</b>.</li> <li>• <b>Confirm password</b> — Confirms the specified password.</li> </ul>
Default Client Update	Enable the Update Now button in the client	Displays or hides the  <b>Update Now</b> 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.
	What to update	Specifies what to update when the  <b>Update Now</b> button is clicked. <ul style="list-style-type: none"> <li>• <b>Security content, hotfixes, and patches</b> — Updates all security content (including engine and AMCore and Exploit Prevention content), as well as any hotfixes and patches, to the latest versions.</li> <li>• <b>Security content</b> — Updates security content only. (Default)</li> <li>• <b>Hotfixes and patches</b> — Updates hotfixes and patches only.</li> </ul>
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, <b>McAfeeHttp</b> , 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.

**Table 2-4 Advanced options** *(continued)*

Section	Option	Definition
	Import	Imports sites from a source site list file. Select the file to import, then click <b>OK</b> .   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 <b>OK</b> .
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.
	Configure proxy server	Customizes proxy settings. <ul style="list-style-type: none"> <li>• <b>HTTP/FTP address</b> — Specifies the DNS, IPv4, or IPv6 address of the HTTP or FTP proxy server.</li> <li>• <b>Port</b> — Limits access through the specified port.</li> <li>• <b>Exclude these addresses</b> — Specifies the addresses for Endpoint Security Client systems that you don't want to use the proxy server for obtaining McAfee GTI ratings. Click <b>Add</b>, then enter the address name to exclude.</li> </ul>
	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: <ul style="list-style-type: none"> <li>• <b>User name</b> — Specifies the user account with permissions to access the proxy server.</li> <li>• <b>Password</b> — Specifies the password for the specified <b>User name</b>.</li> <li>• <b>Confirm password</b> — Confirms the specified password.</li> </ul>


**See also**[Protect Endpoint Security resources on page 31](#)[Configure logging settings on page 31](#)[Controlling access to the client interface on page 32](#)[Configure proxy server settings for McAfee GTI on page 33](#)[Configure the default behavior for updates on page 36](#)[Configure source sites for updates on page 34](#)[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	<p>Retrieves files from the designated HTTP repository location.</p> <p> HTTP offers updating independent of network security, but supports higher levels of concurrent connections than FTP.</p> <p><b>URL</b></p> <ul style="list-style-type: none"><li>• <b>DNS name</b> — Indicates that the URL is a domain name.</li><li>• <b>IPv4</b> — Indicates that the URL is an IPv4 address.</li><li>• <b>IPv6</b> — Indicates that the URL is an IPv6 address.</li></ul> <p><b>http://</b> — Specifies the address of the HTTP server and folder where the update files are located.</p> <p><b>Port</b> — Specifies the port number for the HTTP server.</p> <p><b>Use authentication</b></p> <p>Selects to use authentication and specifies the credentials for accessing the update file folder.</p> <ul style="list-style-type: none"><li>• <b>User name</b> — Specifies the user account with read permissions to the update file folder.</li><li>• <b>Password</b> — Specifies the password for the specified <b>User name</b>.</li><li>• <b>Confirm password</b> — Confirms the specified password.</li></ul>

**Table 2-5 Option definitions** *(continued)*

Option	Definition
<b>FTP repository</b>	Retrieves files from the designated FTP repository location. <p> 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.</p> <p><b>URL</b></p> <ul style="list-style-type: none"> <li>• <b>DNS name</b> — Indicates that the URL is a domain name.</li> <li>• <b>IPv4</b> — Indicates that the URL is an IPv4 address.</li> <li>• <b>IPv6</b> — Indicates that the URL is an IPv6 address.</li> </ul> <p><b>ftp://</b> — Specifies the address of the FTP server and folder where the update files are located.</p> <p><b>Port</b> — Specifies the port number for the FTP server.</p> <p><b>Use anonymous login</b></p> <p>Selects to use anonymous FTP to access the update file folder. Deselect this option to specify access credentials.</p> <ul style="list-style-type: none"> <li>• <b>User name</b> — Specifies the user account with read permissions to the update file folder.</li> <li>• <b>Password</b> — Specifies the password for the specified <b>User name</b>.</li> <li>• <b>Confirm password</b> — Confirms the specified password.</li> </ul>
<b>UNC path or Local path</b>	Retrieves files from the designated UNC or local path location. <p> 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.</p> <p><b>Path</b></p> <ul style="list-style-type: none"> <li>• <b>UNC path</b> — Specifies the path using UNC notation (\\servername\path\).</li> <li>• <b>Local path</b> — Specifies the path of a folder on a local or network drive.</li> </ul> <p><b>Use logged on account</b></p> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>Domain</b> — Specifies the domain for the user account.</li> <li>• <b>User name</b> — Specifies the user account with read permissions to the update file folder.</li> <li>• <b>Password</b> — Specifies the password for the specified <b>User name</b>.</li> <li>• <b>Confirm password</b> — Confirms the specified password.</li> </ul>

## 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	<p>Indicates the currently defined and scheduled tasks.</p> <ul style="list-style-type: none"> <li>• <b>Name</b> — Name of the scheduled task.</li> <li>• <b>Feature</b> — Module or feature that the task is associated with.</li> <li>• <b>Schedule</b> — 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.</li> <li>• <b>Status</b> — Status of the last time the task ran: <ul style="list-style-type: none"> <li>• (no status) — Never run</li> <li>• <b>Running</b> — Current running or resumed</li> <li>• <b>Paused</b> — Paused by the user (such as a scan)</li> <li>• <b>Deferred</b> — Deferred by the user (such as a scan)</li> <li>• <b>Finished</b> — Completed running without errors</li> <li>• <b>Finished (errors)</b> — Finished running with errors</li> <li>• <b>Failed</b> — Failed to complete</li> </ul> </li> <li>• <b>Last Run</b> — Date and time the task last ran.</li> <li>• <b>Origin</b> — Origin of the task: <ul style="list-style-type: none"> <li>• <b>McAfee</b> — Provided by McAfee.</li> <li>• <b>Admin</b> — (Managed systems only) Defined by the administrator.</li> <li>• <b>User</b> — Defined on the Endpoint Security Client.</li> </ul> </li> </ul> <p>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. <b>Admin</b> tasks, defined by the administrator on managed systems, can't be changed or deleted on the Endpoint Security Client.</p>
<i>Double-click an item</i>	Changes the selected item.
<b>Add</b>	Creates a scan, update, or mirror task.
<b>Delete</b>	Deletes the selected task.
<b>Duplicate</b>	Creates a copy of the selected task.
<b>Run Now</b>	<p>Runs the selected task.</p> <p>If the task is already running, including paused or deferred, the button changes to <b>View</b>.</p> <ul style="list-style-type: none"> <li>• <b>Quick Scan</b> — Opens the <b>Quick Scan</b> dialog box and starts the scan.</li> <li>• <b>Full Scan</b> — Opens the <b>Full Scan</b> dialog box and starts the scan.</li> <li>• <b>Custom Scan</b> — Opens the <b>Custom Scan</b> dialog box and starts the scan.</li> <li>• <b>Default Client Update</b> — Opens the <b>Update</b> dialog box and starts the update.</li> <li>• <b>Update</b> — Opens the <b>Custom Update</b> dialog box and starts the update.</li> <li>• <b>Mirror</b> — Opens the <b>Mirror</b> dialog box and starts the repository replication.</li> </ul> <p>If you run a task before applying changes, Endpoint Security Client prompts you to save the settings.</p>

**See also**

*Run a Full Scan or Quick Scan on page 56*  
*Update protection and software manually on page 23*  
*Configure, schedule, and run mirror tasks on page 38*  
*Add Task on page 50*

**Add Task**

Adds custom scan, mirror, or update tasks.

Option	Definition
<b>Name</b>	Specifies the name of the task.
<b>Select task type</b>	Specifies the task type: <ul style="list-style-type: none"> <li>• <b>Custom scan</b> — Configures and schedules a custom scan, such as daily memory scans.</li> <li>• <b>Mirror</b> — Replicates the updated content and engine files from the first accessible repository to a mirror site on your network.</li> <li>• <b>Update</b> — Configures and schedules an update of the content files, scanning engine, or product.</li> </ul>

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

**See also**

*Configure, schedule, and run scan tasks on page 85*  
*Configure On-Demand Scan settings on page 81*  
*Run a Full Scan or Quick Scan on page 56*  
*Threat Prevention — On-Demand Scan on page 105*  
*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: <ul style="list-style-type: none"> <li>• Security content, hotfixes, and patches</li> <li>• Security content</li> <li>• Hotfixes and patches</li> </ul> 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 <b>Default Client Update</b> task runs every day at 12:00 midnight and repeats every four hours until 11:59 p.m.

### See also

*Common — Options on page 41*

*Configure the default behavior for updates on page 36*

*Configure, schedule, and run update tasks on page 37*

*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 38*

*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. <ul style="list-style-type: none"> <li>• <b>Daily</b> — Runs the task every day, at a specific time, on a recurring basis between two times of the day, or a combination of both.</li> <li>• <b>Weekly</b> — Runs the task weekly:               <ul style="list-style-type: none"> <li>• On a specific weekday, all weekdays, weekends, or a combination of days</li> <li>• At a specific time on the selected days, or on a recurring basis between two times of the selected days</li> </ul> </li> <li>• <b>Monthly</b> — Runs the task monthly on either:               <ul style="list-style-type: none"> <li>• The specified day of the month</li> <li>• The specified days of the week — first, second, third, fourth, or last</li> </ul> </li> <li>• <b>Once</b> — Starts the task on the time and date that you specify.</li> <li>• <b>At system startup</b> — Runs the task when the system starts.</li> <li>• <b>At login</b> — Starts the task the next time the user logs on to the system.</li> <li>• <b>Run immediately</b> — Starts the task immediately.</li> </ul>
	Frequency	Specifies the frequency for <b>Daily</b> and <b>Weekly</b> tasks.
	Run on	Specifies the days of the week for <b>Weekly</b> , and <b>Monthly</b> tasks.
	Run in	Specifies the months of the year for <b>Monthly</b> tasks.
	Only run this task once a day	Runs the task once a day for <b>At system startup</b> and <b>At login</b> tasks.
	Delay this task by	Specifies the number of minutes to delay before running <b>At system startup</b> and <b>At login</b> tasks.
	Start date	Specifies the start date for <b>Daily</b> , <b>Weekly</b> , <b>Monthly</b> , and <b>Once</b> tasks.
	End date	Specifies the end date for <b>Daily</b> , <b>Weekly</b> , and <b>Monthly</b> tasks.
	Start time	Specifies the time to start the task. <ul style="list-style-type: none"> <li>• <b>Run once at that time</b> — Runs the task once at the specified <b>Start time</b>.</li> <li>• <b>Run at that time, and then repeat until</b> — Runs the task at the specified <b>Start time</b>. Then, starts the task every number of hours/minutes specified by <b>Start task every</b> until the specified end time.</li> <li>• <b>Run at that time, and then repeat for</b> — Runs the task at the specified <b>Start time</b>. Then, starts the task every number of hours/minutes specified by <b>Start task every</b> until it has run for the specified amount of time.</li> </ul>
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
	<b>Stop this task if it runs longer than</b>	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.
	<b>Randomize the task start time by</b>	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.
	<b>Run missed task</b>	Runs the task after the number of minutes specified by <b>Delay start by</b> once the managed system restarts.
<b>Account</b>		Specifies the credentials to use for running the task. If no credentials are specified, the task runs as the local system Administrator account.
	<b>User name</b>	Specifies the user account.
	<b>Password</b>	Specifies the password for the specified user account.
	<b>Confirm password</b>	Confirms the password for the specified user account.
	<b>Domain</b>	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](#)
- ▶ [Manage threat detections](#)
- ▶ [Manage quarantined items](#)
- ▶ [Managing Threat Prevention](#)
- ▶ [Client Interface Reference — Threat Prevention](#)

---

## 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.

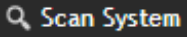
### See also

[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 , 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 85](#)  
[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.

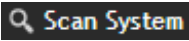
### Before you begin

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 .



- 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 protection and software manually on page 23](#)

[Manage threat detections on page 59](#)

[Configure On-Demand Scan settings on page 81](#)

[Configure, schedule, and run scan tasks on page 85](#)

## 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.

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

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

<b>Detection Name</b>	Identifies the name of the detected malware.
<b>Type</b>	Displays the threat type.
<b>File</b>	Identifies the infected file.
<b>Action Taken</b>	Describes the last security action taken on the infected file: <ul style="list-style-type: none"> <li>• Access Denied</li> <li>• Cleaned</li> <li>• Deleted</li> <li>• None</li> </ul>

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 81](#)

## 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.	<p>Select items, click <b>Delete</b>, then click <b>Delete</b> again to confirm.</p> <p> Deleted items can't be restored.</p>
Restore items from the quarantine.	<p>Select items, click <b>Restore</b>, then click <b>Restore</b> again to confirm.</p> <p>Endpoint Security restores items to the original location and removes them from the quarantine.</p> <p> If an item is still a valid threat, Endpoint Security returns it to the quarantine the next time the item is accessed.</p>
Rescan items.	<p>Select items, then click <b>Rescan</b>.</p> <p>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.</p>
View an item in the Event Log.	<p>Select an item, then click the <b>View in Event Log</b> link in the details pane.</p> <p>The <b>Event Log</b> page opens, with the event related to the selected item highlighted.</p>
Get more information about a threat.	<p>Select an item, then click the <b>Learn more about this threat</b> link in the details pane.</p> <p>A new browser window opens to the McAfee Labs website with more information about the threat that caused the item to be quarantined.</p>

**See also**

- [Detection names on page 61](#)
- [Rescanning quarantined items on page 62](#)
- [Open the Endpoint Security Client on page 19](#)
- [Update protection and software manually on page 23](#)

## 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: <ul style="list-style-type: none"> <li>• Delivering unsolicited pop-up advertisements</li> <li>• Stealing personal information, including financial information, such as credit card numbers</li> <li>• Monitoring web-browsing activity for marketing purposes</li> <li>• Routing HTTP requests to advertising sites</li> </ul> See also Potentially unwanted program.
Stealth	Is a type of virus that attempts to avoid detection from anti-virus software. Also known as <i>interrupt interceptor</i> . 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	<p>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.</p> <p>Typically, a computer becomes infected:</p> <ul style="list-style-type: none"> <li>• When a user opens a trojan attachment in email.</li> <li>• When a user downloads a trojan from a website.</li> <li>• Peer-to-peer networking.</li> </ul> <p>Because they don't replicate themselves, trojans aren't considered viruses.</p>
Virus	<p>Attaches to disks or other files and replicates itself repeatedly, typically without user knowledge or permission.</p> <p>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.</p>

## 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.

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 settings	Process file name or path, MD5 hash, or signer	All except MD5 hash			
Exploit Prevention	Processes	Exploit Prevention settings	Process file name or path, MD5 hash, or signer Caller Module file name or path, MD5 hash, or signer API	All except MD5 hash			
All scans	Detection names	Options settings	Detection name (case-sensitive)	Yes			
	Potentially unwanted programs		Name	Yes			
On-access scan <ul style="list-style-type: none"> <li>• Default</li> <li>• High Risk</li> <li>• Low Risk</li> </ul>	Files, file types, and folders	On-Access Scan settings	File name or folder, file type, or file age	Yes			
	ScriptScan URLs		URL name	No			
On-demand scan <ul style="list-style-type: none"> <li>• Quick Scan</li> <li>• Full Scan</li> <li>• Right-Click Scan</li> </ul>	Files, folders, and drives	On-Demand Scan settings	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 KnowledgeBase article [KB85746](#) and 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, and processes.

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, and registry keys, registry values, and processes.



Access Protection is enabled by default.



## 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	<ul style="list-style-type: none"> <li>• These rules prevent modification of commonly used files and settings.</li> <li>• You can enable, disable, and change the configuration of McAfee-defined rules, but you can't delete these rules.</li> </ul>
User-defined rules	<ul style="list-style-type: none"> <li>• These rules supplement the protection provided by McAfee-defined rules.</li> <li>• An empty <b>Executables</b> table indicates that the rule applies to all executables.</li> <li>• An empty <b>User Names</b> table indicates that the rule applies to all users.</li> <li>• You can add and delete, as well as enable, disable, and change the configuration of these rules.</li> </ul>

## 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 27](#)


[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
Altering any file extension registrations	<p>Protects the registry keys under HKEY_CLASSES_ROOT where file extensions are registered.</p> <p>This rule prevents malware from changing the file extension registrations to allow malware to execute silently.</p> <p> <b>Best practice:</b> Disable this rule when installing valid applications that change file extension registrations in the registry.</p> <p>This rule is a more restrictive alternative to <b>Hijacking .EXE and other executable extensions</b>.</p>
Altering user rights policies	<p>Protects registry values that contain Windows security information.</p> <p>This rule prevents worms from changing accounts that have administrator rights.</p>
Creating new executable files in the Program Files folder	<p>Prevents the creation new executable files in the Program Files folder.</p> <p>This rule prevents adware and spyware from creating new .EXE and .DLL files and installing new executable files in the Program Files folder.</p> <p> <b>Best practice:</b> Install applications before enabling this rule, or place the blocked processes in the exclusion list.</p>
Creating new executable files in the Windows folder	<p>Prevents the creation of files from any process, not just from over the network.</p> <p>This rule prevents the creation of .EXE and .DLL files in the Windows folder.</p> <p> <b>Best practice:</b> Add processes that must place files in the Windows folder to the exclusion list.</p>
Disabling Registry Editor and Task Manager	<p>Protects Windows registry entries, preventing disabling the registry editor and Task Manager.</p> <p> In an outbreak, disable this rule to be able to change the registry, or open Task Manager to stop active processes.</p>

McAfee-defined rule	Description
<b>Executing scripts by Windows script host (CScript.exe or Wscript.exe) from any temp folder</b>	<p>Prevents the Windows scripting host from running VBScript and JavaScript scripts in any folder with "temp" in the folder name.</p> <p>This rule protects against many trojans and questionable web installation mechanisms used by adware and spyware applications.</p> <p>This rule might block legitimate scripts and third-party applications from being installed or run.</p>
<b>Hijacking .EXE or other executable extensions</b>	<p>Protects .EXE, .BAT, and other executable registry keys under HKEY_CLASSES_ROOT.</p> <p>This rule prevents malware from changing registry keys to run the virus when another executable runs.</p> <p>This rule is a less restrictive alternative to <b>Altering all file extension registrations</b>.</p>
<b>Installing Browser Helper Objects or Shell Extensions</b>	<p>Prevents adware, spyware, and trojans that install as Browser Helper Objects from installing on to the host computer.</p> <p>This rule prevents adware and spyware from installing on systems.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <p><b>Best practice:</b> 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.</p> </div>
<b>Installing new CLSIDs, APPIDs, and TYPELIBs</b>	<p>Prevents the installation or registration of new COM servers.</p> <p>This rule protects against adware and spyware programs that install themselves as a COM add-on Internet Explorer or Microsoft Office applications.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <p><b>Best practice:</b> Allow legitimate applications that register COM add-ons, including some common applications like Adobe Flash by adding them to the exclusion list.</p> </div>
<b>Internet Explorer launching files from the Downloaded Program Files folder</b>	<p>Prevents software from installing through the web browser. This rule is specific to Microsoft Internet Explorer.</p> <p>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.</p> <p>This rule is set to <b>Report</b> by default.</p> <p>This rule prevents adware and spyware from installing and running executables from this folder.</p>
<b>Modifying core Windows processes</b>	<p>Prevents files from being created or executed with the most commonly spoofed names.</p> <p>This rule prevents viruses and trojans from running with the name of a Windows process. This rule excludes authentic Windows files.</p>
<b>Modifying Internet Explorer settings</b>	<p>Blocks processes from changing settings in Internet Explorer.</p> <p>This rule prevents start-page trojans, adware, and spyware from changing browser settings, such as changing the start page or installing favorites.</p>
<b>Modifying network settings</b>	<p>Prevents processes that aren't listed in the exclusion list from changing a system's network settings.</p> <p>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.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <p><b>Best practice:</b> Add processes that must change network settings to the exclusion list or disable the rule while changes are made.</p> </div>

McAfee-defined rule	Description
<b>Registering of programs to autorun</b>	<p>Blocks adware, spyware, trojans, and viruses from trying to register themselves to load every time a system is restarted.</p> <p>This rule prevents processes that aren't on the excluded list from registering processes that execute each time a system restarts.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <b>Best practice:</b> Add legitimate applications to the exclusion list, or install them before this rule is enabled.         </div>
<b>Remotely accessing local files or folders</b>	<p>Prevents read and write access from remote computers to the computer. This rule prevents a share-hopping worm from spreading.</p> <p>In a typical environment, this rule is suitable for workstations, but not servers, and is only useful when computers are actively under attack.</p> <p>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.</p>
<b>Remotely creating autorun files</b>	<p>Prevents other computers from making a connection and creating or changing autorun (autorun.inf) files.</p> <p>Autorun files are used to automatically start program files, typically setup files from CDs.</p> <p>This rule prevents spyware and adware distributed on CDs from being executed.</p> <p>This rule is selected to <b>Block</b> and <b>Report</b> by default.</p>
<b>Remotely creating or modifying files or folders</b>	<p>Blocks write access to all shares.</p> <p>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.</p> <p>In a typical environment, this rule is suitable for workstations, but not servers, and is only useful when computers are actively under attack.</p> <p>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.</p>
<b>Remotely creating or modifying Portable Executable, .INI, .PIF file types, and core system locations</b>	<p>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.</p> <p>This rule protects against fast spreading worms or viruses, which traverse a network through open or administrative shares.</p> <p>This rule is a less secure alternative to <b>Making all shares read only</b>.</p>

McAfee-defined rule	Description
Running files from any temp folder	<p>Blocks any executable from running or starting from any folder with "temp" in the folder name.</p> <p>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.</p> <p>Although this rule provides the most protection, it might block legitimate applications from being installed.</p>
Running files from the Temp folder by common programs	<p>Blocks applications from installing software from the browser or from the email client.</p> <p>This rule prevents email attachments and executables from running on webpages.</p>



**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.

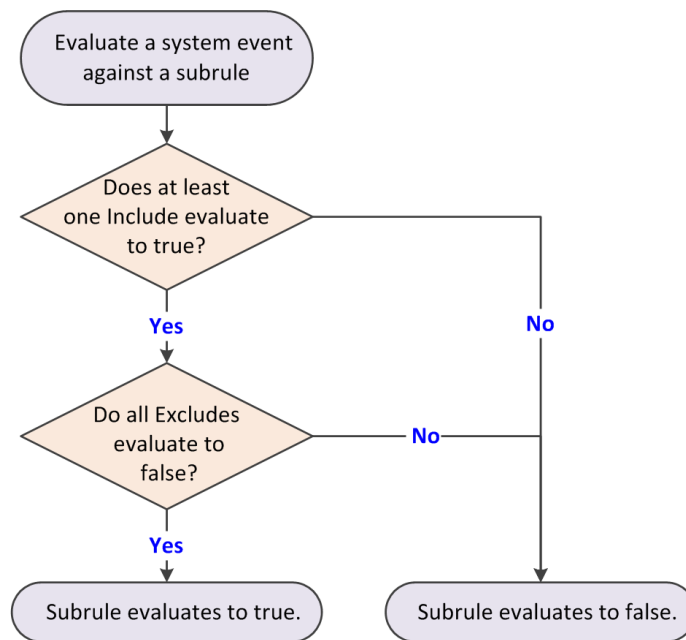
- 6 In the **Rules** section, select **Block**, **Report**, or both for the rule.
  - To block or report all, select **Block** or **Report** in the first row.
  - To disable the rule, deselect both **Block** and **Report**.
- 7 Click **Apply** to save your changes or click **Cancel**.

### 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.



Access Protection is enabled by default.

- 6 Perform one of the following:

To...	Do this...
Create a policy-based exclusion.	<ol style="list-style-type: none"> <li>1 In the <b>Exclusions</b> section, click <b>Add</b> to add processes to exclude from all rules.</li> <li>2 On the <b>Add Executable</b> page, configure the executable properties.</li> <li>3 Click <b>Save</b>, then click <b>Apply</b> to save the settings.</li> </ol>
Create a rule-based exclusion.	<ol style="list-style-type: none"> <li>1 Edit an existing rule or add a new rule.</li> <li>2 On the <b>Add Rule</b> or <b>Edit Rule</b> page, click <b>Add</b> to add an executable to exclude.</li> <li>3 On the <b>Add Executable</b> page, configure the executable properties.</li> <li>4 Click <b>Save</b> to save the exclusions.</li> </ol>

## 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 10.2. 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.

More than 25 percent of malware attacks are buffer overflow attacks that attempt 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 within 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.

## Configure Exploit Prevention settings


To prevent applications from executing arbitrary code on your computer, configure the Exploit Prevention 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 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 27](#)

## Excluding processes from Exploit Prevention

When an Exploit Prevention violation event occurs, there's an associated process and a possible caller module or API.

If you suspect the violation event is a false positive, you can add an exclusion that specifies the process, caller module, or API.

Within one exclusion, the process, module, and API are connected by a logical AND. To exclude that violation from occurring again, the process, module, and API associated with the violation event must all match.

Each exclusion is independent: multiple exclusions are connected by a logical OR so that if one exclusion matches, the violation event doesn't occur.

## 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 74](#)

[Enable and configure potentially unwanted program detection and responses on page 75](#)

[Configure On-Access Scan settings on page 77](#)

[Configure On-Demand Scan settings on page 81](#)

## 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 27](#)

## 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 77](#)

[Configure On-Demand Scan settings on page 81](#)

[Log on as administrator on page 27](#)

## 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 27](#)

[Configure On-Access Scan settings on page 77](#)

[Configure On-Demand Scan settings on page 81](#)

## 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 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 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. However, allowing more detections can result in more false positive results.

- For Threat Prevention, the McAfee GTI sensitivity level is set to Medium by default. Configure the sensitivity level for each scanner in the Threat Prevention settings.
- For Web Control, 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** settings.

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

## 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 27](#)

[Configure common scan settings on page 76](#)

## 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.

The on-access scanner delivers notifications to the Service Interface when detections occur.

When an attempt is made to open or close a file, the scanner intercepts the operation, then:

1 The scanner determines if the item must be scanned, using this criteria:

- The file extension matches the configuration.
- The file hasn't been cached, excluded, or previously scanned.



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 it to the signatures in the currently loaded AMCore content file.

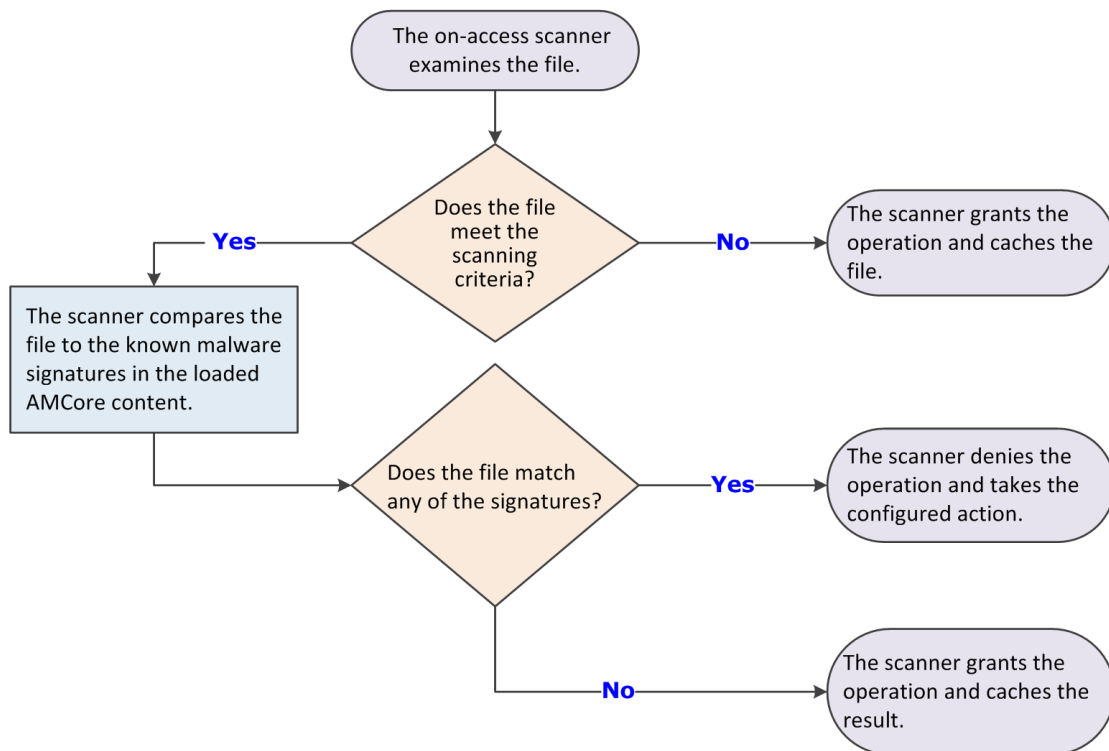
- If the file is clean, the result is cached and the read or write operation is granted.
- If the file contains a threat, the operation is denied and the scanner takes the configured action.

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 prompts for the action to take (clean or delete the file).

**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 file doesn't meet the scanning requirements, the scanner caches the file and grants the operation.



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.

### Scanning when writing to disk, reading from disk, or letting McAfee decide

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

When files are written to disk, the on-access scanner scans these files:

- Incoming files written to the local hard drive.
- Files (new, modified, or files copied or moved from one drive to another) created on the local hard drive or a mapped network drive (if enabled).

When files are read from disk, the scanner scans these files:

- Outgoing files read from the local hard drive or mapped network drives (if enabled).
- Files attempting to execute a process on the local hard drive.
- Files opened on the local hard drive.

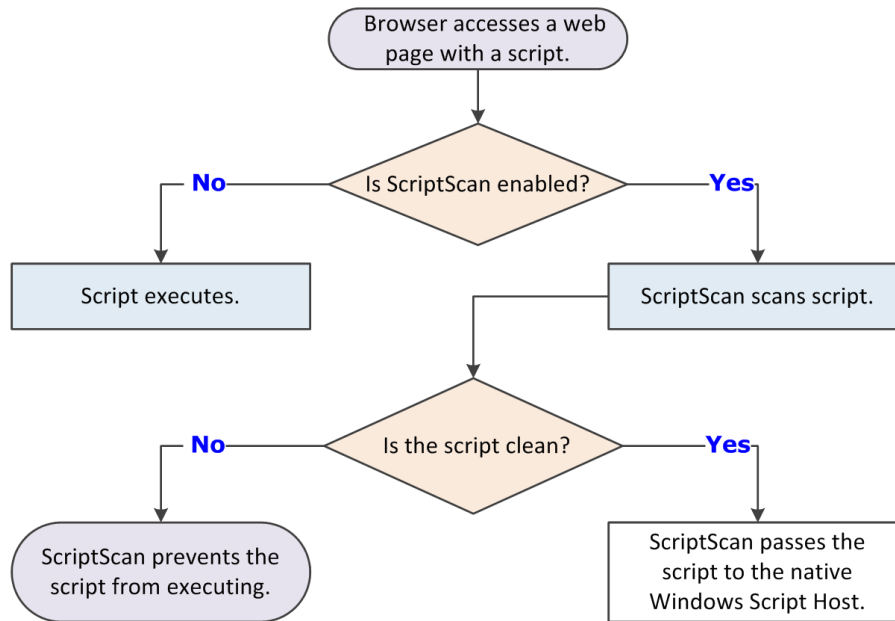
When you let McAfee decide whether a file requires scanning, the on-access scanner uses *trust logic* to optimize scanning. Trust logic improves your security and boosts performance by avoiding unnecessary scans. For example, McAfee analyzes and considers some programs to be trustworthy. If McAfee verifies that these programs haven't been tampered with, the scanner might perform reduced or optimized scanning.



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

### About ScriptScan

The Threat Prevention script scanner operates as a proxy component to the native Windows Script Host, intercepting and scanning scripts before they execute.



- 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.

### 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 within an intranet or web applications that are known safe.

When creating URL exclusions:

- Don't use wildcard characters.
- Don't include port numbers.
- We recommend that you use only Fully Qualified Domain Names (FQDN) and NetBIOS names.



On Windows Server 2008 systems, ScriptScan URL exclusions don't work with Internet Explorer unless you enable third-party browser extensions and restart the system. See KnowledgeBase article [KB69526](#).

### ScriptScan and Internet Explorer

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.
- The add-on must be enabled in the browser.

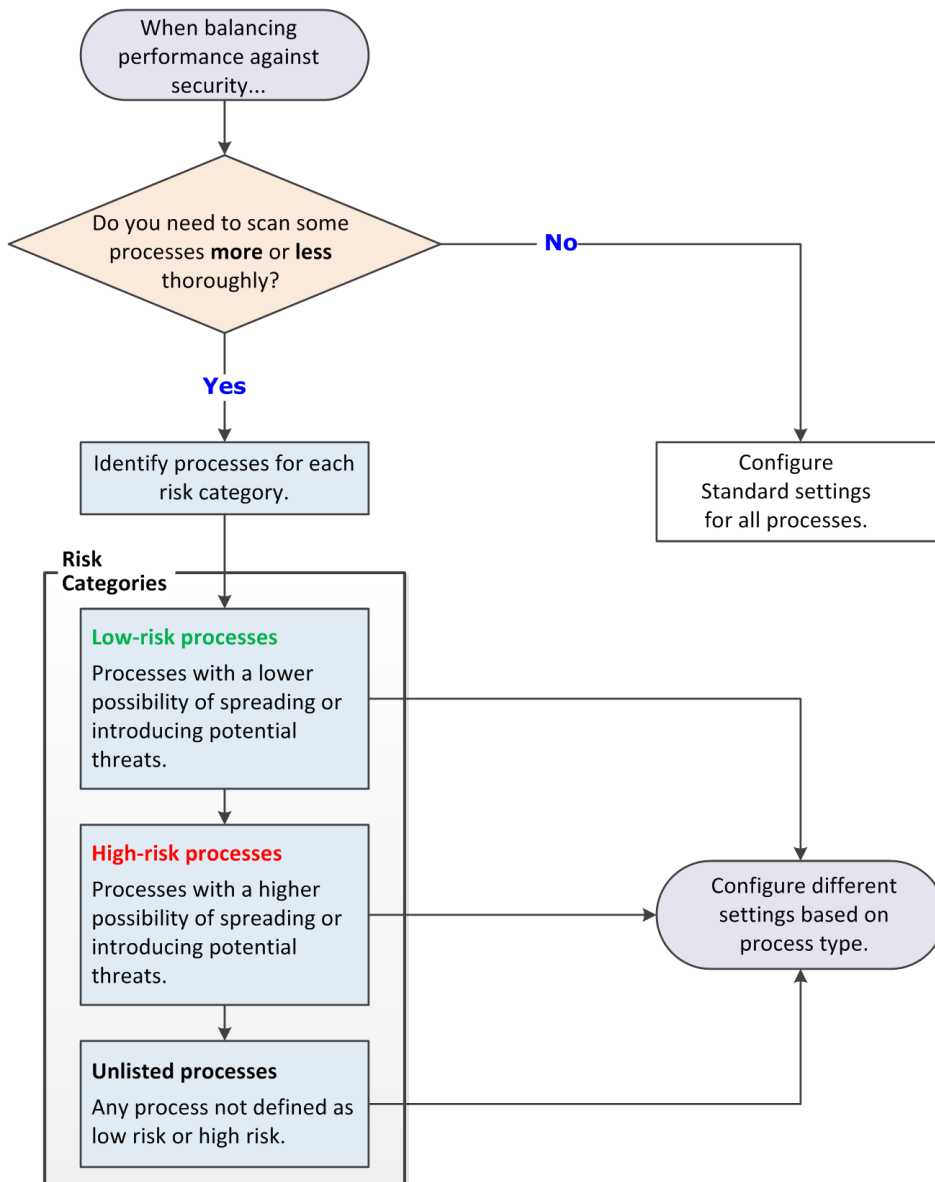


If ScriptScan is disabled when Internet Explorer is launched and then is enabled, it doesn't detect malicious scripts in that instance of Internet Explorer. You must restart Internet Explorer after enabling ScriptScan for it to detect malicious scripts.



## 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 27](#)

[Configure common scan settings on page 76](#)


[Configure, schedule, and run scan tasks on page 85](#)

### 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.

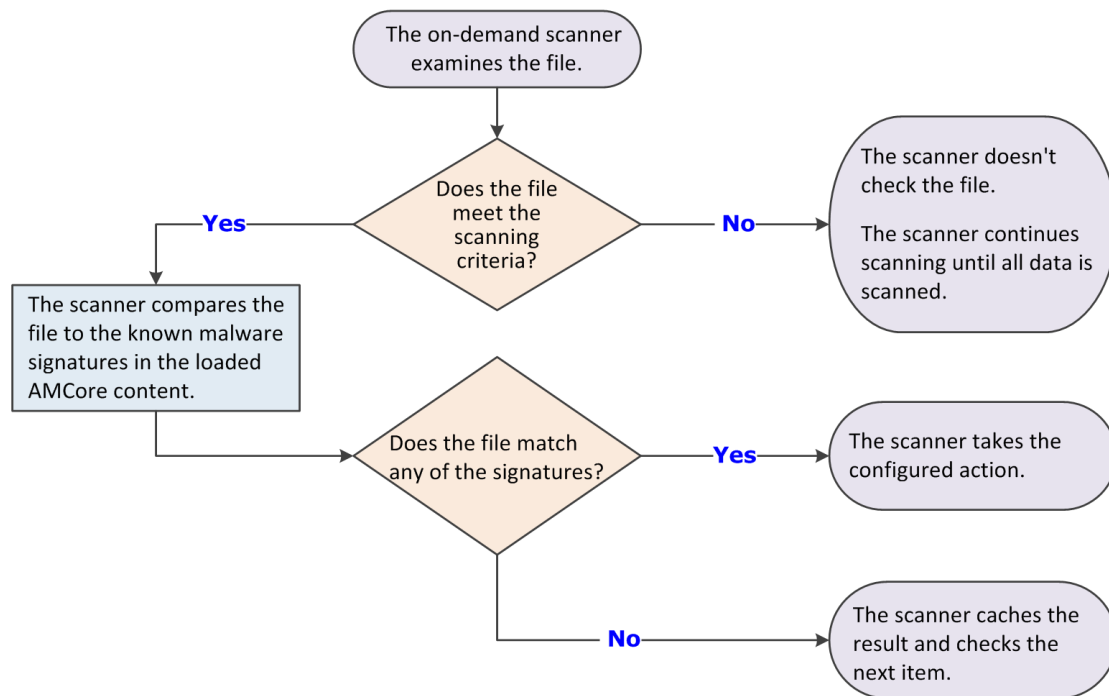
You decide when and how often the on-demand scans occur. You can scan systems manually, at a scheduled time, or at startup.

- 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.

### Reducing the impact of scans on users

To minimize the impact that on-demand scans have on a system, specify performance options when configuring these scans.

#### 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 selected, 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 on server systems and systems that users access using Remote Desktop Connection (RDP) only. 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.

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

- **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 selected)

### 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 zero, 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 entire 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.

### See also

[Configure On-Demand Scan settings on page 81](#)

[Configure, schedule, and run scan tasks on page 85](#)

## 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.	<ol style="list-style-type: none"> <li>1 Click <b>Add</b>.</li> <li>2 Enter the name, select <b>Custom scan</b> from the drop-down list, then click <b>Next</b>.</li> <li>3 Configure the scan task settings and schedule, then click <b>OK</b> to save the task.</li> </ol>
Change a scan task.	<ul style="list-style-type: none"> <li>• Double-click the task, make your changes, then click <b>OK</b> to save the task.</li> </ul>
Remove a custom scan task.	<ul style="list-style-type: none"> <li>• Select the task, then click <b>Delete</b>.</li> </ul>
Create a copy of a scan task.	<ol style="list-style-type: none"> <li>1 Select the task, then click <b>Duplicate</b>.</li> <li>2 Enter the name, configure the settings, then click <b>OK</b> to save the task.</li> </ol>
Change the schedule for a <b>Full Scan</b> or <b>Quick Scan</b> task.	<ol style="list-style-type: none"> <li>1 Double-click <b>Full Scan</b> or <b>Quick Scan</b>.</li> <li>2 Click the <b>Schedule</b> tab, change the schedule, then click <b>OK</b> to save the task.</li> </ol> <p>You can configure <b>Full Scan</b> and <b>Quick Scan</b> task settings on self-managed systems only.</p> <p>By default, the <b>Full Scan</b> is scheduled to run every Wednesday at 12 midnight. The <b>Quick Scan</b> is scheduled to run every day at 7 p.m. The schedules are enabled.</p>
Run a scan task.	<ul style="list-style-type: none"> <li>• Select the task, then click <b>Run Now</b>.</li> </ul> <p>If the task is already running, including paused or deferred, the button changes to <b>View</b>.</p> <p>If you run a task before applying changes, Endpoint Security Client prompts you to save the settings.</p>

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

### See also

- [Log on as administrator on page 27](#)
- [Configure On-Demand Scan settings on page 81](#)
- [Run a Full Scan or Quick Scan on page 56](#)

## Client Interface Reference — Threat Prevention

The interface reference help topics provide context-sensitive help for pages in the client interface.

### Contents

- [Quarantine page](#)
- [Threat Prevention — Access Protection](#)
- [Threat Prevention — Exploit Prevention](#)
- [Threat Prevention — On-Access Scan](#)
- [Threat Prevention — On-Demand Scan](#)
- [Scan Locations](#)
- [McAfee GTI](#)
- [Actions](#)

- ▶ [Add Exclusion or Edit Exclusion](#)
- ▶ [Threat Prevention — Options](#)
- ▶ [Roll Back AMCore Content](#)

## Quarantine page

Manage items in the Quarantine.

**Table 3-3 Options**

Option	Definition
<b>Delete</b>	Deletes selected items from the Quarantine. Deleted items can't be restored.
<b>Restore</b>	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.
<b>Rescan</b>	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...
<b>Detection Name</b>	Name of the detection.
<b>Type</b>	Type of threat, for example, <b>Trojan</b> or <b>Adware</b> .
<b>Time quarantined</b>	The length of time the item has been quarantined.
<b>Number of objects</b>	The number of objects in the detection.
<b>AMCore content version</b>	The version number of AMCore content that identified the threat.
<b>Rescan status</b>	The status of the rescan, if the item has been rescanned: <ul style="list-style-type: none"> <li>• <b>Clean</b> — The rescan resulted in no threat detections.</li> <li>• <b>Infected</b> — Endpoint Security detected a threat during the rescan.</li> </ul>

### 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.

See the settings in the Common module for logging configuration.

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		<p>Allows access to the specified processes, also called executables, for all rules.</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Adds a process to the exclusion list.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected item.</li> <li>• <b>Duplicate</b> — Creates a copy of the selected item.</li> </ul>
Rules		<p>Configures Access Protection rules.</p> <p>You can enable, disable, and change McAfee-defined rules, but you can't delete these rules.</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Creates a custom rule and adds it to the list.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected item.</li> <li>• <b>Duplicate</b> — Creates a copy of the selected item.</li> <li>• <b>Block (only)</b> — Blocks access attempts without logging.</li> <li>• <b>Report (only)</b> — Warns without blocking access attempts.</li> <li>• <b>Block and Report</b> — Blocks and logs access attempts.</li> </ul> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p> <b>Best practice:</b> When the full impact of a rule is not known, select <b>Report</b> but not <b>Block</b> to receive a warning without blocking access attempts. To determine whether to block access, monitor the logs and reports.</p> </div> <p>To block or report all, select <b>Block</b> or <b>Report</b> in the first row.</p> <p>To disable the rule, deselect both <b>Block</b> and <b>Report</b>.</p>

**See also**

[Configure McAfee-defined Access Protection rules on page 66](#)

[Configure user-defined Access Protection rules on page 70](#)

[Add Rule or Edit Rule on page 88](#)


[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	<p>Specifies actions for the rule.</p> <ul style="list-style-type: none"> <li>• <b>Block</b> (only) — Blocks access attempts without logging.</li> <li>• <b>Report</b> (only) — Warns without blocking access attempts.</li> <li>• <b>Block and Report</b> — Blocks and logs access attempts.</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> <b>Best practice:</b> When the full impact of a rule is not known, select <b>Report</b> but not <b>Block</b> to receive a warning without blocking access attempts. To determine whether to block access, monitor the logs and reports.</p> </div> <p>To block or report all, select <b>Block</b> or <b>Report</b> in the first row. To disable the rule, deselect both <b>Block</b> and <b>Report</b>.</p>
	Executables	<p>Specifies executables for the rule.</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Creates an executable and adds it to the list.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected item.</li> <li>• <b>Duplicate</b> — Creates a copy of the selected item.</li> <li>• <b>Toggle Inclusion Status</b> — Changes the inclusion status of the item between <b>Include</b> and <b>Exclude</b>.</li> </ul>
	User Names	<p>Specifies user names that the rule applies to (for user-defined rules only).</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Selects a user name and adds it to the list.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected item.</li> <li>• <b>Duplicate</b> — Creates a copy of the selected item.</li> <li>• <b>Toggle Inclusion Status</b> — Changes the inclusion status of the item between <b>Include</b> and <b>Exclude</b>.</li> </ul>
	Subrules	<p>Configures subrules (for user-defined rules only).</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Creates a subrule and adds it to the list.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected item.</li> <li>• <b>Duplicate</b> — Creates a copy of the selected item.</li> </ul>
	Notes	Provides more information about the item.

**See also**

- [Add Executable or Edit Executable on page 95](#)
- [Add User Name or Edit User Name on page 90](#)
- [Add Subrule or Edit Subrule on page 90](#)

## 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
<b>Name</b>	<p>Specifies the name of the user that the rule applies to. Use this format to specify the user:</p> <ul style="list-style-type: none"> <li>• <b>Local user</b> — Valid entries include: <ul style="list-style-type: none"> <li>&lt;machine_name&gt;\&lt;local_user_name&gt;</li> <li>.\&lt;local_user_name&gt;</li> <li>.\administrator (for the local administrator)</li> </ul> </li> <li>• <b>Domain user</b> — &lt;domain name&gt;\&lt;domain user_name&gt;</li> <li>• <b>Local system</b> — Local\System specifies the NT AUTHORITY\System account on the system.</li> </ul>
<b>Inclusion status</b>	<p>Specifies the inclusion status for the user.</p> <ul style="list-style-type: none"> <li>• <b>Include</b> — Triggers the rule if the specified user runs the executable that violates a subrule.</li> <li>• <b>Exclude</b> — Doesn't trigger the rule if the specified user runs the executable that violates a subrule.</li> </ul>

### See also

[Add Rule or Edit Rule on page 88](#)


## Add Subrule or Edit Subrule

Add or edit a subrule (for user-defined rules only).

**Table 3-8 Options**

Section	Option	Definition
<b>Description</b>	<b>Name</b>	Specifies the name of the subrule.
<b>Properties</b>	<b>Subrule type</b>	<p>Specifies the subrule type. Changing the subrule type removes any previously defined entries in the <b>Targets</b> table.</p> <ul style="list-style-type: none"> <li>• <b>Files</b> — 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.</li> <li>• <b>Registry key</b> — Protects the specified key. A registry key is the container for the registry value. For example, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.</li> <li>• <b>Registry value</b> — 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.</li> <li>• <b>Processes</b> — Protects the specified process. For example, create a custom rule to block or report attempted operations on a process.</li> </ul>

**Table 3-8 Options** *(continued)*

Section	Option	Definition
	Operations	<p data-bbox="548 279 1523 338">Indicates the operations permitted with the subrule type. You must specify at least one operation to apply to the subrule.</p> <div data-bbox="570 352 1503 394" style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px;">  <b>Best practice:</b> To avoid impacting performance, don't select the <b>Read</b> operation.                 </div> <ul style="list-style-type: none"> <li data-bbox="548 422 630 447">• <b>Files:</b> <ul style="list-style-type: none"> <li data-bbox="574 464 1523 522">• <b>Change read-only or hidden attributes</b> — Blocks or reports changing these attributes of files in the specified folder.</li> <li data-bbox="574 537 1370 562">• <b>Create</b> — Blocks or reports creation of files in the specified folder.</li> <li data-bbox="574 577 1370 602">• <b>Delete</b> — Blocks or reports deletion of files in the specified folder.</li> <li data-bbox="574 617 1403 642">• <b>Execute</b> — Blocks or reports execution of files in the specified folder.</li> <li data-bbox="574 657 1500 716">• <b>Change permissions</b> — Blocks or reports changing permissions settings of files in the specified folder.</li> <li data-bbox="574 730 1297 756">• <b>Read</b> — Blocks or reports read access to the specified files.</li> <li data-bbox="574 770 1365 795">• <b>Rename</b> — Blocks or reports rename access to the specified files.</li> </ul> </li> </ul>

**Table 3-8 Options** *(continued)*

Section	Option	Definition
		<p>If the <b>Destination File</b> target is specified, <b>Rename</b> is the only valid operation.</p> <ul style="list-style-type: none"> <li>• <b>Write</b> — Blocks or reports write access to the specified files.</li> <li>• <b>Registry key:</b> <ul style="list-style-type: none"> <li>• <b>Write</b> — Blocks or reports write access to the specified key.</li> <li>• <b>Create</b> — Blocks or reports creation of the specified key.</li> <li>• <b>Delete</b> — Blocks or reports deletion of the specified key.</li> <li>• <b>Read</b> — Blocks or reports read access to the specified key.</li> <li>• <b>Enumerate</b> — Blocks or reports enumeration of the subkeys for the specified registry key.</li> <li>• <b>Load</b> — Blocks or reports the ability to unload the specified registry key and its subkeys from the registry.</li> <li>• <b>Replace</b> — Blocks or reports replacement of the specified registry key and its subkeys with another file.</li> <li>• <b>Restore</b> — Blocks or reports the ability to save registry information in a specified file and copies over the specified key.</li> <li>• <b>Change permissions</b> — Blocks or reports changing permissions settings of specified registry key and its subkeys.</li> </ul> </li> <li>• <b>Registry value:</b> <ul style="list-style-type: none"> <li>• <b>Write</b> — Blocks or reports write access to the specified value.</li> <li>• <b>Create</b> — Blocks or reports creation of the specified value.</li> <li>• <b>Delete</b> — Blocks or reports deletion of the specified value.</li> <li>• <b>Read</b> — Blocks or reports read access to the specified value.</li> </ul> </li> <li>• <b>Processes:</b> <ul style="list-style-type: none"> <li>• <b>Any access</b> — Blocks or reports opening the process with any access.</li> <li>• <b>Create thread</b> — Blocks or reports opening the process with access to create a thread.</li> <li>• <b>Modify</b> — Blocks or reports opening the process with access to modify.</li> <li>• <b>Terminate</b> — Blocks or reports opening the process with access to terminate.</li> <li>• <b>Run</b> — Blocks or reports running the specified target executable.</li> </ul> </li> </ul> <p>You must add at least one target executable to the rule.</p> <p>For the <b>Run</b> 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.</p>
	<b>Targets</b>	<ul style="list-style-type: none"> <li>• <b>Add</b> — 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 <b>Add</b>, select the inclusion status, then enter or select the target to include or exclude.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected item.</li> </ul>



**See also**

- [Add Rule or Edit Rule on page 88](#)
- [Targets on page 93](#)
- [Add Executable or Edit Executable on page 95](#)

**Targets**

Specify the inclusion status and definition for a target.

**Table 3-9 Options**

Section	Option	Definition
Targets		<p>Determines whether the target is a positive match for the subrule. Also specifies the status of the inclusion for the target.</p> <ul style="list-style-type: none"> <li>• <b>Include</b> — Indicates that the subrule can match the specified target.</li> <li>• <b>Exclude</b> — Indicates that the subrule must not match the specified target.</li> </ul>
	<i>If you selected the Files subrule type...</i>	<p>Specifies the file name, folder name, path, or drive type target for a <b>Files</b> subrule.</p> <ul style="list-style-type: none"> <li>• <b>File path</b> — Browse to select the file.</li> <li>• <b>Destination file</b> — Browse to select the target file name or path for a <b>Rename</b> operation. If the <b>Destination file</b> target is selected, the <b>Rename</b> operation (only) must be selected.</li> <li>• <b>Drive type</b> — Select the drive type target from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Removable</b> — 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.</li> </ul> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 2px; margin: 5px 0;">  Blocking this drive type also blocks drives with Windows To Go installed. </div> </li> <li>• <b>Network</b> — Files on a network share</li> <li>• <b>Fixed</b> — Files on the local hard drive or other fixed hard disk</li> <li>• <b>CD/DVD</b> — Files on a CD or DVD</li> <li>• <b>Floppy</b> — Files on a floppy disk</li> </ul> <p>You can use <code>?</code>, <code>*</code>, and <code>**</code> as wildcards.</p> <p><b>Files subrule target best practices</b></p> <p>For example, to protect:</p> <ul style="list-style-type: none"> <li>• A file or folder named <code>c:\testap</code>, use a target of <code>c:\testap</code> or <code>c:\testap\</code></li> <li>• The contents of a folder, use the asterisk wildcard — <code>c:\testap\*</code></li> <li>• The contents of a folder and its subfolders, use 2 asterisks — <code>c:\testap\**</code></li> </ul> <p>System environment variables are supported. Environment variables can be specified in one of the following formats:</p> <ul style="list-style-type: none"> <li>• <code>\$(EnvVar) - \$(SystemDrive), \$(SystemRoot)</code></li> <li>• <code>%EnvVar% - %SystemRoot%, %SystemDrive%</code></li> </ul> <p>Not all system-defined environment variables can be accessed using the <code>\$(var)</code> syntax, specifically those containing the <code>or</code> characters. You can use the <code>%var%</code> syntax to avoid this issue.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 2px; margin: 5px 0;">  User environment variables are not supported. </div>

**Table 3-9 Options** (continued)

Section	Option	Definition
<i>If you selected the Registry key subrule type...</i>		<p>Defines registry keys using root keys. These root keys are supported:</p> <ul style="list-style-type: none"> <li>• HKLM or HKEY_LOCAL_MACHINE</li> <li>• HKCU or HKEY_CURRENT_USER</li> <li>• HKCR or HKEY_CLASSES_ROOT</li> <li>• HKCCS matches HKLM/SYSTEM/CurrentControlSet and HKLM/SYSTEM/ControlSet00X</li> <li>• HKLMS matches HKLM/Software on 32-bit and 64-bit systems, and HKLM/Software/Wow6432Node on 64-bit systems only</li> <li>• HKCUS matches HKCU/Software on 32-bit and 64-bit systems, and HKCU/Software/Wow6432Node on 64-bit systems only</li> <li>• HKULM treated as both HKLM and HKCU</li> <li>• HKULMS treated as both HKLMS and HKCUS</li> <li>• HKALL treated as both HKLM and HKU</li> </ul> <p>You can use ?, *, and ** as wildcards, and   (pipe) as an escape character.</p> <p><b>Registry key subrule target best practices</b></p> <p>For example, to protect:</p> <ul style="list-style-type: none"> <li>• A registry key named HKLM\SOFTWARE\testap, use a target of HKLM\SOFTWARE\testap or HKLM\SOFTWARE\testap\</li> <li>• The contents of a registry key, use the asterisk wildcard — HKLM\SOFTWARE\testap\*</li> <li>• The contents of a registry key and its subkeys, use 2 asterisks — HKLM\SOFTWARE\testap\**</li> <li>• Registry keys and values under a registry key, enable the <b>Write</b> operation</li> </ul>

**Table 3-9 Options** (continued)

Section	Option	Definition
	<i>If you selected the Registry value subrule type...</i>	<p>Defines registry values using root keys. These root keys are supported:</p> <ul style="list-style-type: none"> <li>• HKLM or HKEY_LOCAL_MACHINE</li> <li>• HKCU or HKEY_CURRENT_USER</li> <li>• HKCR or HKEY_CLASSES_ROOT</li> <li>• HKCCS matches HKLM/SYSTEM/CurrentControlSet and HKLM/SYSTEM/ControlSet00X</li> <li>• HKLMS matches HKLM/Software on 32-bit and 64-bit systems, and HKLM/Software/Wow6432Node on 64-bit systems only</li> <li>• HKCUS matches HKCU/Software on 32-bit and 64-bit systems, and HKCU/Software/Wow6432Node on 64-bit systems only</li> <li>• HKULM treated as both HKLM and HKCU</li> <li>• HKULMS treated as both HKLMS and HKCUS</li> <li>• HKALL treated as both HKLM and HKU</li> </ul> <p>You can use <code>?</code>, <code>*</code>, and <code>**</code> as wildcards, and <code> </code> (pipe) as an escape character.</p> <p><b>Registry value subrule target best practices</b></p> <p>For example, to protect:</p> <ul style="list-style-type: none"> <li>• A registry value named HKLM\SOFTWARE\testap, use a target of HKLM\SOFTWARE\testap</li> <li>• The registry values under a registry key, use the asterisk wildcard — HKLM\SOFTWARE\testap\*</li> <li>• The registry values under a registry key and its subkeys, use 2 asterisks — HKLM\SOFTWARE\testap\**</li> </ul>
	<i>If you selected the Processes subrule type...</i>	<p>Specifies the process file name or path, MD5 hash, or signer target for a <b>Processes</b> subrule.</p> <p>You can use <code>?</code>, <code>*</code>, and <code>**</code> as wildcards for all except MD5 hash.</p> <p><b>Processes subrule target best practices</b></p> <p>For example, to protect:</p> <ul style="list-style-type: none"> <li>• A process named c:\testap.exe, use a target file name or path of c:\testap.exe</li> <li>• All processes in a folder, use the asterisk wildcard — c:\testap\*</li> <li>• All processes in a folder and its subfolders, use 2 asterisks — c:\testap\**</li> </ul>

**See also**

[Add Subrule or Edit Subrule on page 90](#)

**Add Executable or Edit Executable**

Add or edit an executable to exclude or include.

For Threat Prevention Access Protection, you can exclude executables at the policy level, or include or exclude at the rule level. For Threat Intelligence Dynamic Application Containment, you can exclude executables at the policy 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
<b>Name</b>	Specifies the name that you call the executable. This field is required with at least one other field: <b>File name or path</b> , <b>MD5 hash</b> , or <b>Signer</b> .
<b>Inclusion status</b>	Determines the inclusion status for the executable. <ul style="list-style-type: none"> <li>• <b>Include</b> — Triggers the rule if the executable violates a subrule.</li> <li>• <b>Exclude</b> — Doesn't trigger the rule if the executable violates a subrule.</li> </ul> <b>Inclusion status</b> only appears for Threat Prevention Access Protection when adding an executable to a rule or the target for the Processes subrule.
<b>File name or path</b>	Specifies the file name or path of the executable to add or edit. Click <b>Browse</b> to select the executable. The file path can include wildcards.
<b>MD5 hash</b>	Indicates the (32-digit hexadecimal number) MD5 hash of the process.



**Table 3-10 Options** (continued)

Option	Definition
Signer	<p><b>Enable digital signature check</b> — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash.</p> <p>If enabled, specify:</p> <ul style="list-style-type: none"> <li>• <b>Allow any signature</b> — Allows files signed by any process signer.</li> <li>• <b>Signed by</b> — Allows only files signed by the specified process signer.</li> </ul> <p>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.</p> <p>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:</p> <p>C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS</p> <p>To obtain the SDN of an executable:</p> <ol style="list-style-type: none"> <li>1 Right-click an executable and select <b>Properties</b>.</li> <li>2 On the <b>Digital Signatures</b> tab, select a signer and click <b>Details</b>.</li> <li>3 On the <b>General</b> tab, click <b>View Certificate</b>.</li> <li>4 On the <b>Details</b> tab, select the <b>Subject</b> field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: <ul style="list-style-type: none"> <li>• CN = Mozilla Corporation</li> <li>• OU = Release Engineering</li> <li>• O = Mozilla Corporation</li> <li>• L = Mountain View</li> <li>• S = California</li> <li>• C = US</li> </ul> </li> </ol>
Notes	Provides more information about the item.

**See also**

[Add Rule or Edit Rule on page 88](#)

## Threat Prevention — Exploit Prevention

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

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 10.2. 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
Protection Level		Specifies the Exploit Prevention protection level.
	Standard	<p>Detects and blocks only high-severity buffer overflow exploits identified in the Exploit Prevention content file and stops the detected thread.</p> <p>Use the feature in <b>Standard</b> mode for a short while. Review the log file during that time to determine whether to change to <b>Maximum</b> protection.</p>
	Maximum	<p>Detects and blocks high- and medium-severity buffer overflow exploits identified in the Exploit Prevention content file and stops the detected thread.</p> <p>This setting can result in false positives.</p>
Generic Privilege Escalation Prevention	<p><b>Enable Generic Privilege Escalation Prevention</b></p>	<p>Enables Generic Privilege Escalation Prevention (GPEP) support. (Disabled by default)</p> <p>GPEP uses GPEP signatures in the Exploit Prevention Content to provide coverage for privilege escalation exploits in kernel mode and user mode.</p> <p>Because GPEP might generate false positive reports, this option is disabled by default.</p>
Windows Data Execution Prevention	<p><b>Enable Windows Data Execution Prevention</b></p>	<p>Enables Windows Data Execution Prevention (DEP) integration. (Disabled by default)</p> <p>Select this option to:</p> <ul style="list-style-type: none"> <li>• 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).</li> <li>• Caller validation and Targeted API Monitoring are still enforced.</li> <li>• Monitor for DEP detections in the DEP-enabled 32-bit applications.</li> <li>• Monitor for DEP detections in 64-bit applications in the McAfee application protection list.</li> <li>• Log any DEP detections and send an event to McAfee ePO.</li> </ul> <p>Disabling this option doesn't affect any processes that have DEP enabled as a result of the Windows DEP policy.</p>
Action		<p>Specifies the <b>Block</b> or <b>Report</b> actions for Exploit Prevention.</p> <p>The report setting is not applicable when Windows Data Execution Prevention is enabled.</p>
	Block	<p>Blocks the specified process. Select <b>Block</b> to enable Exploit Prevention or deselect to disable Exploit Prevention.</p> <p>To block access attempts without logging, select <b>Block</b> but do not select <b>Report</b>.</p>

**Table 3-12 Advanced options** *(continued)*

Section	Option	Definition
	Report	<p>Enables reporting of attempts to violate Exploit Prevention. When a detection occurs, information is recorded in the activity log.</p> <p> <b>Best practice:</b> When the full impact of a rule is not known, select <b>Report</b> but not <b>Block</b> to receive a warning without blocking access attempts. To determine whether to block access, monitor the logs and reports.</p>
Exclusions		<p>Specifies the process, caller module, or API to exclude. Exclusions with Caller Module or API don't apply to DEP.</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Creates an exclusion and adds it to the list.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected item.</li> <li>• <b>Duplicate</b> — Creates a copy of the selected item.</li> </ul>

**See also**

[Configure Exploit Prevention settings on page 73](#)

[Add Exclusion or Edit Exclusion on page 99](#)

**Add Exclusion or Edit Exclusion**

Add or edit an Exploit Prevention exclusion.

You must specify at least one of **Process**, **Caller Module**, or **API**. Exclusions with Caller Module or API don't apply to DEP.

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 to the exclusion.
- 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 3-13 Options**

Section	Option	Definition
Process	Name	<p>Specifies the process name to exclude. Exploit Prevention excludes the process wherever it is located.</p> <p>This field is required with at least one other field: <b>File name or path</b>, <b>MD5 hash</b>, or <b>Signer</b>.</p>
	File name or path	<p>Specifies the file name or path of the executable to add or edit.</p> <p>Click <b>Browse</b> to select the executable.</p>
	MD5 hash	<p>Indicates the (32-digit hexadecimal number) MD5 hash of the process.</p>

**Table 3-13 Options** (continued)

Section	Option	Definition
	<b>Signer</b>	<p><b>Enable digital signature check</b> — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash.</p> <p>If enabled, specify:</p> <ul style="list-style-type: none"> <li>• <b>Allow any signature</b> — Allows files signed by any process signer.</li> <li>• <b>Signed by</b> — Allows only files signed by the specified process signer.</li> </ul> <p>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.</p> <p>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:</p> <p>C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS</p> <p>To obtain the SDN of an executable:</p> <ol style="list-style-type: none"> <li>1 Right-click an executable and select <b>Properties</b>.</li> <li>2 On the <b>Digital Signatures</b> tab, select a signer and click <b>Details</b>.</li> <li>3 On the <b>General</b> tab, click <b>View Certificate</b>.</li> <li>4 On the <b>Details</b> tab, select the <b>Subject</b> field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: <ul style="list-style-type: none"> <li>• CN = Mozilla Corporation</li> <li>• OU = Release Engineering</li> <li>• O = Mozilla Corporation</li> <li>• L = Mountain View</li> <li>• S = California</li> <li>• C = US</li> </ul> </li> </ol>
	<b>Caller Module Name</b>	<p>Specifies the name of the module that owns the writeable memory that is making the call.</p> <p>This field is required with at least one other field: <b>File name or path</b>, <b>MD5 hash</b>, or <b>Signer</b>.</p>
	<b>File name or path</b>	<p>Specifies the file name or path of the executable to add or edit.</p> <p>Click <b>Browse</b> to select the executable.</p>
	<b>MD5 hash</b>	<p>Indicates the (32-digit hexadecimal number) MD5 hash of the process.</p>

**Table 3-13 Options** *(continued)*

Section	Option	Definition
	Signer	<p><b>Enable digital signature check</b> — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash.</p> <p>If enabled, specify:</p> <ul style="list-style-type: none"> <li>• <b>Allow any signature</b> — Allows files signed by any process signer.</li> <li>• <b>Signed by</b> — Allows only files signed by the specified process signer.</li> </ul> <p>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.</p> <p>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:</p> <p>C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS</p> <p>To obtain the SDN of an executable:</p> <ol style="list-style-type: none"> <li>1 Right-click an executable and select <b>Properties</b>.</li> <li>2 On the <b>Digital Signatures</b> tab, select a signer and click <b>Details</b>.</li> <li>3 On the <b>General</b> tab, click <b>View Certificate</b>.</li> <li>4 On the <b>Details</b> tab, select the <b>Subject</b> field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: <ul style="list-style-type: none"> <li>• CN = Mozilla Corporation</li> <li>• OU = Release Engineering</li> <li>• O = Mozilla Corporation</li> <li>• L = Mountain View</li> <li>• S = California</li> <li>• C = US</li> </ul> </li> </ol>
API	Name	Specifies the name of the API (application programming interface) being called.
	Notes	Provides more information about the item.

**See also**

[Threat Prevention — Exploit Prevention on page 97](#)




[Excluding processes from Exploit Prevention on page 74](#)

**Threat Prevention — On-Access Scan**



Enable and configure the on-access scan settings.

See the settings in the Common module for logging configuration.

**Table 3-14 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.
	Scan boot sectors	Examines the disk boot sector. (Enabled by default)   <b>Best practice:</b> Disable 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: <ul style="list-style-type: none"> <li>You re-enable on-access scans.</li> <li>Content files are updated.</li> <li>The system starts.</li> <li>The McShield.exe process starts.</li> </ul>  <b>Best practice:</b> Because some programs or executables start automatically when you start your system, disable this option to improve system startup time.  (Disabled by default) 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)   <b>Best practice:</b> Disable this option to improve the performance of large Microsoft application installers.
Scan when copying between local folders	Scans files whenever the user copies from one local folder to another. If this option is: <ul style="list-style-type: none"> <li><b>Disabled</b> — Only items in the destination folder are scanned.</li> <li><b>Enabled</b> — Items in both source (read) and destination (write) folders are scanned.</li> </ul> (Disabled by default)	
McAfee GTI	Enables and configures McAfee GTI settings.	






**Table 3-14 Options** (continued)

Section	Option	Definition
ScriptScan	Enable ScriptScan	<p>Enables scanning JavaScript and VBScript scripts to prevent unwanted scripts from executing. (Enabled by default)</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>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.</p> </div>
	Exclude these URLs	<p>Specifies ScriptScan exclusions by URL.</p> <p><b>Add</b> — Adds a URL to the exclusion list.</p> <p><b>Delete</b> — Removes a URL from the exclusion list.</p> <p>URLs can't include wildcard characters. However, any URL containing a string from an excluded URL is also excluded. For example, if the URL msn.com is excluded, the following URLs are also excluded:</p> <ul style="list-style-type: none"> <li>• http://weather.msn.com</li> <li>• http://music.msn.com</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>On Windows Server 2008 systems, ScriptScan URL exclusions don't work with Internet Explorer unless you enable third-party browser extensions and restart the system. See KnowledgeBase article <a href="#">KB69526</a>.</p> </div>

**Table 3-15 Advanced options**

Section	Option	Definition
Threat Detection User Messaging	Display the On-Access Scan window to users when a threat is detected	<p>Displays the <b>On-Access Scan</b> page with the specified message to client users when a detection occurs. (Enabled by default)</p> <p>When this option is selected, users can open this page from the <b>Scan Now</b> page at any time the detection list includes at least one threat.</p> <p>The on-access scan detection list is cleared when the Endpoint Security service restarts or the system reboots.</p>
	Message	<p>Specifies the message to display to client users when a detection occurs.</p> <p>The default message is: McAfee Endpoint Security detected a threat.</p>
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	<p>Configures settings for processes that aren't identified as either high risk or low risk. (Enabled by default)</p>
	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 <b>High Risk</b> or <b>Low Risk</b> list.

**Table 3-15 Advanced options** (continued)

Section	Option	Definition
	Delete	Removes a process from the <b>High Risk</b> or <b>Low Risk</b> 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.
	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.
		 <b>Best practice:</b> Enable this option for the best protection and performance.
	Do not scan when reading from or writing to disk	Specifies to not scan <b>Low Risk</b> processes only.
	What to scan	
	All files	Scans all files, regardless of extension.
		 Failure to enable <b>All files</b> leaves your system vulnerable to malware attacks.
	Default and specified file types	Scans: <ul style="list-style-type: none"> <li>• Default list of file extensions defined in the current AMCore content file, including files with no extension</li> <li>• Any additional file extensions that you specify Separate extensions with a comma.</li> <li>• (Optional) Known macro threats in the list of default and specified file extensions</li> </ul>
	Specified file types only	Scans either or both: <ul style="list-style-type: none"> <li>• Only files with the (comma-separated) extensions that you specify</li> <li>• All files with no extension</li> </ul>
	On network drives	Scans resources on mapped network drives.
	 <b>Best practice:</b> Disable this option to improve performance.	
Opened for backups	Scans files when accessed by backup software.	
	 <b>Best practice:</b> For most environments, you don't need to enable this setting.	
Compressed archive files	Examines the contents of archive (compressed) files, including .jar files.	
	 Scanning compressed files can negatively affect system performance.	
Compressed MIME-encoded files	Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.	



**Table 3-15 Advanced options** (continued)

Section	Option	Definition
	<b>Additional scan options</b>	
	<b>Detect unwanted programs</b>	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.
	<b>Detect unknown program threats</b>	Uses McAfee GTI to detect executable files that have code resembling malware.
	<b>Detect unknown macro threats</b>	Uses McAfee GTI to detect unknown macro viruses.
<b>Actions</b>		Specifies how the scanner responds when it detects a threat.
<b>Exclusions</b>		Specifies files, folders, and drives to exclude from scanning.
	<b>Add</b>	Adds an item to the exclusion list.
	<b>Delete</b>	Removes an item from the exclusion list.

**See also**

[Configure On-Access Scan settings on page 77](#)

[McAfee GTI on page 109](#)

[Actions on page 110](#)

[Add Exclusion or Edit Exclusion on page 112](#)

**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 3-16 Options**

Section	Option	Definition
<b>What to Scan</b>	<b>Boot sectors</b>	Examines the disk boot sector.   <b>Best practice:</b> Disable boot sector scanning when a disk contains a unique or abnormal boot sector that can't be scanned.
	<b>Files that have been migrated to storage</b>	Scans files that Remote Storage manages. Some offline data storage solutions replace files with a <i>stub</i> 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.  We recommend disabling this option.
	<b>Compressed MIME-encoded files</b>	Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.

**Table 3-16 Options** (continued)

Section	Option	Definition
	<b>Compressed archive files</b>	Examines the contents of archive (compressed) files, including .jar files.   <b>Best practice:</b> Use this option in scans during off hours when the system isn't being used because scanning compressed files can negatively affect system performance.
	<b>Subfolders (Right-Click Scan only)</b>	Examines all subfolders of the specified folder.
<b>Additional Scan Options</b>	<b>Detect unwanted programs</b>	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.
	<b>Detect unknown program threats</b>	Uses McAfee GTI to detect executable files that have code resembling malware.
	<b>Detect unknown macro threats</b>	Uses McAfee GTI to detect unknown macro viruses.
<b>Scan Locations</b>	<b>(Full Scan and Quick Scan only)</b>	Specifies the locations to scan. These options apply to <b>Full Scan</b> , <b>Quick Scan</b> , and custom scans only.
<b>File Types to Scan</b>	<b>All files</b>	Scans all files, regardless of extension. McAfee strongly recommends enabling <b>All files</b> .   Failure to enable <b>All files</b> leaves your system vulnerable to malware attacks.
	<b>Default and specified file types</b>	Scans: <ul style="list-style-type: none"> <li>• Default list of file extensions defined in the current AMCore content file, including files with no extension</li> <li>• Any additional file extensions that you specify Separate extensions with a comma.</li> <li>• (Optional) Known macro threats in the list of default and specified file extensions</li> </ul>
	<b>Specified file types only</b>	Scans either or both: <ul style="list-style-type: none"> <li>• Only files with the (comma-separated) extensions that you specify</li> <li>• All files with no extension</li> </ul>
<b>McAfee GTI</b>		Enables and configures McAfee GTI settings.
<b>Exclusions</b>		Specifies files, folders, and drives to exclude from scanning.
	<b>Add</b>	Adds an item to the exclusion list.
	<b>Delete</b>	Removes an item from the exclusion list.
<b>Actions</b>		Specifies how the scanner responds when it detects a threat.
<b>Performance</b>	<b>Use the scan cache</b>	Enables the scanner to use the existing clean scan results. Select this option to reduce duplicate scanning and improve performance.

**Table 3-16 Options** (continued)

Section	Option	Definition
	System utilization	<p>Enables the operating system to specify the amount of CPU time that the scanner receives during the scan.</p> <p>Each task runs independently, unaware of the limits for other tasks.</p> <ul style="list-style-type: none"> <li>• <b>Low</b> — Provides improved performance for other running applications.</li> </ul> <p> <b>Best practice:</b> Select this option for systems with end-user activity.</p> <ul style="list-style-type: none"> <li>• <b>Below normal</b> — Sets the system utilization for the scan to the McAfee ePO default.</li> <li>• <b>Normal (Default)</b> — Enables the scan to complete faster.</li> </ul> <p> <b>Best practice:</b> Select this option for systems that have large volumes and little end-user activity.</p>
<b>Scheduled Scan Options</b>		These options apply to <b>Full Scan</b> , <b>Quick Scan</b> , and custom scans only.
	Scan only when the system is idle	<p>Runs the scan only when the system is idle.</p> <p>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.</p> <p>Disable this option on server systems and systems that users access using Remote Desktop Connection (RDP) only. 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.</p>
	Scan anytime	<p>Runs the scan even if the user is active and specifies options for the scan.</p> <p><b>User can defer scans</b> — Allows the user to defer scheduled scans, and specifies options for scan deferral.</p> <ul style="list-style-type: none"> <li>• <b>Maximum number of times user can defer for one hour</b> — Specifies the number of times (1–23) that the user can defer the scan for one hour.</li> <li>• <b>User message</b> — Specifies the message to display when a scan is about to start.</li> </ul> <p>The default message is: <i>McAfee Endpoint Security is about to scan your system.</i></p> <ul style="list-style-type: none"> <li>• <b>Message duration (seconds)</b> — 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.</li> </ul>
		<b>Do not scan when the system is in presentation mode</b> — 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 81*

*Configure, schedule, and run scan tasks on page 85*

*Run a Full Scan or Quick Scan on page 56*

*Scan a file or folder on page 58*

*Scan Locations on page 108*

*McAfee GTI on page 109*

*Actions on page 110*



*Add Exclusion or Edit Exclusion on page 112*

**Scan Locations**

Specify the locations to scan.

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

**Table 3-17 Options**

Section	Option	Definition
Scan Locations	Scan subfolders	Examines all subfolders in the specified volumes when any of these options are selected: <ul style="list-style-type: none"> <li>• Home folder</li> <li>• User profile folder</li> <li>• Program files folder</li> <li>• Temp folder</li> <li>• File or folder</li> </ul> <p>Deselect this option to scan only the root level of the volumes.</p>
	Specify locations	Specifies the locations to scan. <ul style="list-style-type: none"> <li>• <b>Add</b> — Adds a location to the scan. Click <b>Add</b>, then select the location from the drop-down.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Removes a location from the scan. Select the location and click <b>Delete</b>.</li> </ul>
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. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Failure to enable this option leaves your system unprotected from malware attacks.           </div>
Running processes		Scans the memory of all running processes. Actions other than <b>Clean files</b> are treated as <b>Continue scanning</b> . <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Failure to enable this option leaves your system unprotected from malware attacks.           </div>
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 3-17 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.

**See also**

[Threat Prevention — On-Demand Scan on page 105](#)


## McAfee GTI

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

**Table 3-18 Options**

Section	Option	Definition
Enable McAfee GTI		<p>Enables and disables heuristic checks.</p> <ul style="list-style-type: none"> <li>When enabled, fingerprints of samples, or <i>hashes</i>, 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.</li> <li>When disabled, no fingerprints or data is submitted to McAfee Labs.</li> </ul>
Sensitivity level		<p>Configures the sensitivity level to use when determining if a detected sample is malware.</p> <p>The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results.</p>
	Very low	<p>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 waiting for the next AMCore content file update.</p> <p>Use this setting for desktops and servers with restricted user rights and a strong security footprint.</p> <p>This setting results in an average of 10–15 queries per day, per computer.</p>
	Low	<p>This setting is the minimum recommendation for laptops or desktops and servers with a strong security footprint.</p> <p>This setting results in an average of 10–15 queries per day, per computer.</p>

**Table 3-18 Options** (continued)

Section	Option	Definition
	<b>Medium</b>	Use this level 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. However, 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 or desktops and servers. This setting results in an average of 20–25 queries per day, per computer.
	<b>High</b>	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.
	<b>Very high</b>	McAfee recommends using this level only for scanning volumes and directories that don't support executing programs or operating systems. Detections found with this level are presumed malicious, but haven't been fully tested to determine if they are false positives.  <div style="border: 1px solid gray; padding: 2px; display: inline-block;">  <b>Best practice:</b> Use this setting for non-operating system volumes. </div> This setting results in an average of 20–25 queries per day, per computer.

**See also**

[Threat Prevention — On-Access Scan](#) on page 101

[Threat Prevention — On-Demand Scan](#) on page 105

[Web Control — Options](#) on page 151

**Actions**

Specify how the scanner responds when it detects a threat.

**Table 3-19 Options**

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

**Table 3-19 Options** (continued)

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

**See also**


[Threat Prevention — On-Access Scan on page 101](#)

[Threat Prevention — On-Demand Scan on page 105](#)

## Add Exclusion or Edit Exclusion

Add or edit an exclusion definition.

**Table 3-20 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.  <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  To exclude a folder on Windows systems, append a backslash (\) character to the path.         </div> Select <b>Also exclude subfolders</b> if necessary.	✓	✓
	File type	Specifies file types (file extensions) to exclude.	✓	✓
	File age	Specifies the access type ( <b>Modified</b> , <b>Accessed</b> (On-Demand Scan only), or <b>Created</b> ) of files to exclude and the <b>Minimum age in days</b> .	✓	✓
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 101  
[Threat Prevention — On-Demand Scan](#) on page 105  
[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 3-21 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	<p>Specifies detection exclusions by detection name.</p> <p>For example, to specify that the on-access scanner and on-demand scanner not detect <b>Installation Check</b> threats, enter <code>Installation Check</code>.</p> <p><b>Add</b> — Adds a detection name to the exclusion list. Click <b>Add</b>, then enter the detection name.</p> <p><i>Double-click an item</i> — Changes the selected item.</p> <p><b>Delete</b> — Removes a detection name from the exclusion list. Select the name, then click <b>Delete</b>.</p>
Potentially Unwanted Program Detections	Exclude custom unwanted programs	<p>Specifies individual files or programs to treat as potentially unwanted programs.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p> The scanners detect the programs you specify as well as programs specified in the AMCore content files.</p> </div> <p>The scanner doesn't detect a zero-byte sized user-defined unwanted program.</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Defines a custom unwanted program. Click <b>Add</b>, enter the name, then press <b>Tab</b> to enter the description.</li> <li>• <b>Name</b> — Specifies the file name of the potentially unwanted program.</li> <li>• <b>Description</b> — Specifies the information to display as the detection name when a detection occurs.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Removes a potentially unwanted program from the list. Select the program in the table, then click <b>Delete</b>.</li> </ul>
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 3-21** Advanced options (continued)


Section	Option	Definition
	Safety pulse	<p>Performs a health check on the client system before and after AMCore content file updates, and at regular intervals, and sends results to McAfee.</p> <p>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.</p> <p>Safety pulse collects the following types of data:</p> <ul style="list-style-type: none"> <li>• Operating system version and locale</li> <li>• McAfee product version</li> <li>• AMCore content and engine version</li> <li>• McAfee and Microsoft running process information</li> </ul>
	AMCore Content Reputation	<p>Performs a McAfee GTI reputation lookup on the AMCore content file before updating the client system.</p> <ul style="list-style-type: none"> <li>• If McAfee GTI allows the file, Endpoint Security updates AMCore content.</li> <li>• If McAfee GTI doesn't allow the file, Endpoint Security doesn't update AMCore content.</li> </ul>

**See also**

[Configure common scan settings on page 76](#)

**Roll Back AMCore Content**

Changes the AMCore content to a previous version.

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

**See also**

[Change the AMCore content version on page 28](#)

# 4

## Using Firewall

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

### Contents

- ▶ *How Firewall works*
- ▶ *Enable and disable Firewall from the McAfee system tray icon*
- ▶ *Enable or view Firewall timed groups from the McAfee system tray icon*
- ▶ *Managing Firewall*
- ▶ *Client Interface Reference — Firewall*

---

## 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 117*

*How firewall rules work on page 121*

*How firewall rule groups work on page 122*

---

## 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 117](#)  
Configure settings in Options to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options.
- [Block DNS traffic on page 118](#)  
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 119](#)  
Define network addresses, subnets, or ranges to use in rules and groups. Optionally, specify that those networks are trusted.
- [Configure trusted executables on page 120](#)  
Define or edit the list of trusted executables that are considered safe for your environment.

### See also

[FAQ — McAfee GTI and Firewall on page 118](#)

## 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 10.2. 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 27](#)

## 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.

### How does it work?

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.
- **Unverified** — This appears to be a legitimate source or destination of content/traffic. However, this site also displays certain properties suggesting that further inspection is necessary.

- **Medium Risk** — This source/destination shows behavior that we believe is suspicious and content/traffic to or from it requires special scrutiny.
- **High Risk** — This source/destination is known or to or likely to send/host potentially malicious content/traffic. We believe that it presents a serious risk.

### 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 it can 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 <b>Add</b> and enter the details for the trusted network. Define the network as trusted by selecting <b>Yes</b> from the <b>Trusted</b> drop-down menu.  If you select <b>No</b> , 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 <b>Delete</b> .

- 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 <b>Add</b> 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 <b>Delete</b> .

- 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 126](#)  
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 128](#)  
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 129](#)  
Create Firewall timed groups to restrict Internet access until a client system connects over a VPN.

### How firewall rules work

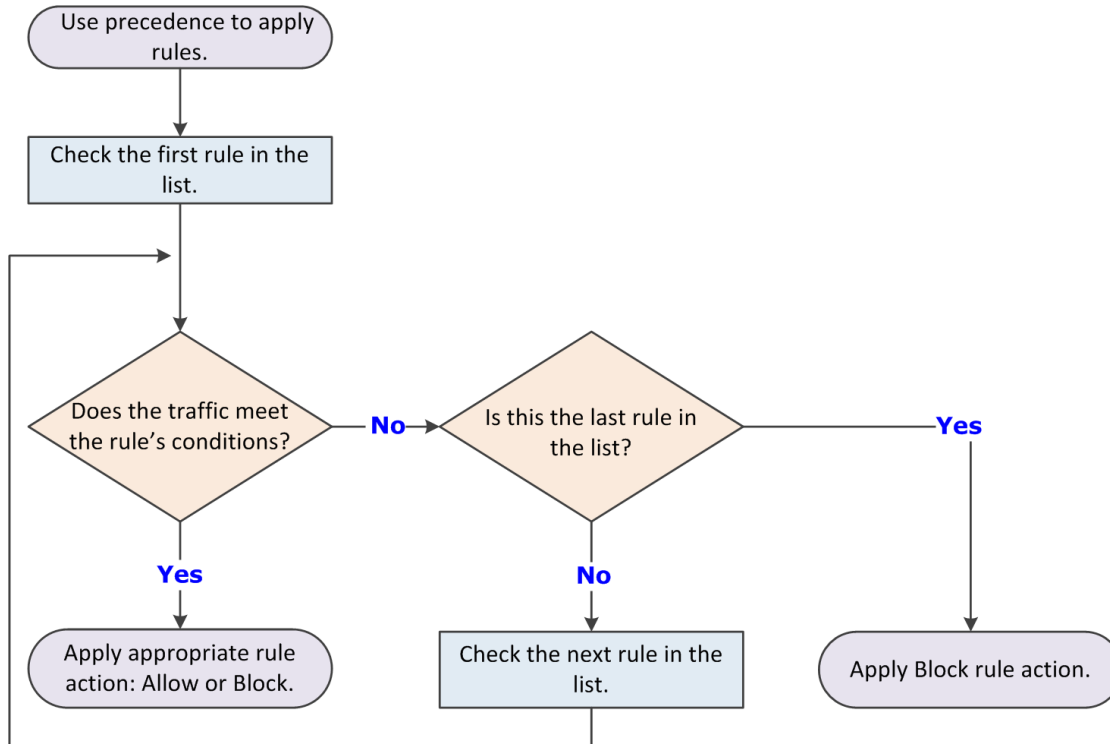
Firewall rules determine how to handle network traffic. Each rule provides a set of conditions that traffic must meet and an action to allow or block traffic.

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
- 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.
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	The specified domain must be reachable.

## Firewall rule groups and connection isolation

Use connection isolation for groups to prevent undesirable traffic from accessing a designated network.

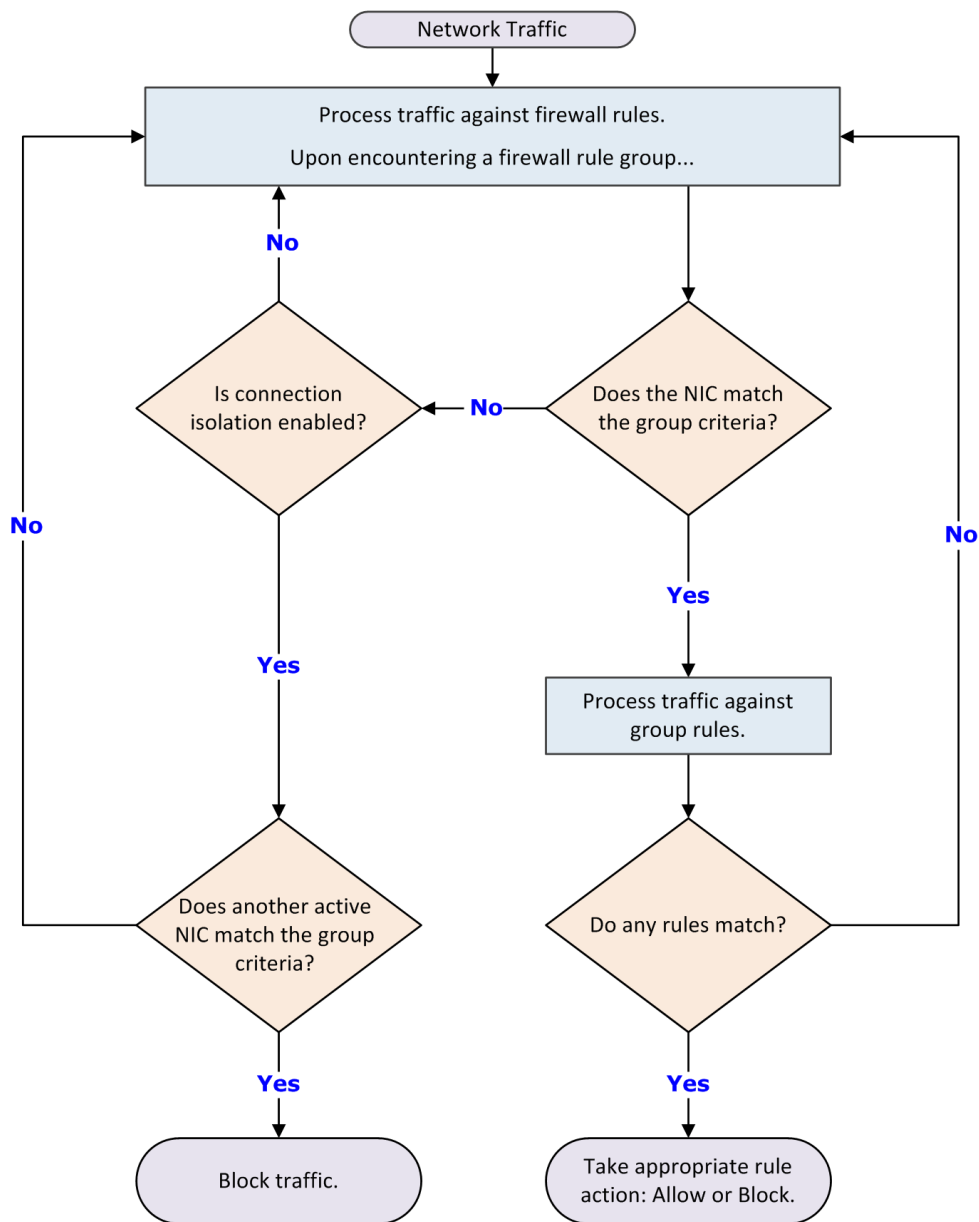
When connection isolation is enabled for a group, and an active Network Interface Card (NIC) matches the group criteria, Firewall only processes traffic that matches:

- 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	<p>Contains the core networking rules provided by McAfee and includes rules to allow McAfee applications and DNS.</p> <p> 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.</p>
Admin added	<p>Contains rules defined by the administrator at the management server.</p> <p> These rules can't be changed or deleted on the Endpoint Security Client.</p>
User added	<p>Contains rules defined on the Endpoint Security Client.</p> <p> Depending on policy settings, these rules might be overwritten when the policy is enforced.</p>
Dynamic	<p>Contains rules created dynamically by other Endpoint Security modules installed on the system.</p> <p>For example, Threat Prevention might send an event to the Endpoint Security Client module to create a rule to block access to a system on the network.</p>
Adaptive	<p>Contains client exception rules that are created automatically when the system is in Adaptive mode.</p> <p> Depending on policy settings, these rules might be overwritten when the policy is enforced.</p>
Default	<p>Contains default rules provided by McAfee.</p> <p> These rules can't be changed or deleted.</p>

## 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  .
Modify an existing rule.   You can modify rules in the <b>User added</b> group only.	<ol style="list-style-type: none"> <li>1 Expand the <b>User added</b> group.</li> <li>2 Double-click the rule.</li> <li>3 Change the rule settings.</li> <li>4 Click <b>OK</b> to save your changes.</li> </ol>
View an existing rule in any group.	<ol style="list-style-type: none"> <li>1 Expand the group.</li> <li>2 Select the rule to view its details in the bottom pane.</li> </ol>
Create a rule.	<ol style="list-style-type: none"> <li>1 Click <b>Add Rule</b>.</li> <li>2 Specify the rule settings.</li> <li>3 Click <b>OK</b> to save your changes.</li> </ol> <p>The rule appears at the end of the <b>User added</b> group.</p>
Create copies of rules.	<ol style="list-style-type: none"> <li>1 Select the rule or rules and click <b>Duplicate</b>. Copied rules appear with the same name at the end of the <b>User added</b> group.</li> <li>2 Modify the rules to change the name and settings.</li> </ol>
Delete rules.   You can delete rules from the <b>User added</b> and <b>Adaptive</b> groups only.	<ol style="list-style-type: none"> <li>1 Expand the group.</li> <li>2 Select the rule or rules and click <b>Delete</b>.</li> </ol>
Create a group.	<ol style="list-style-type: none"> <li>1 Click <b>Add Group</b>.</li> <li>2 Specify the group settings.</li> <li>3 Click <b>OK</b> to save your changes.</li> </ol> <p>The group appears in the <b>User added</b> group.</p>
Move rules and groups within and between groups.   You can move rules and groups in the <b>User added</b> group only.	<p>To move elements:</p> <ol style="list-style-type: none"> <li>1 Select elements to move. The grip  appears to the left of elements that can be moved.</li> <li>2 Drag-and-drop the elements to the new location. A blue line appears between elements where you can drop the dragged elements.</li> </ol>

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

### See also

[Wildcards in firewall rules on page 128](#)

[Log on as administrator on page 27](#)


[Create connection isolation groups on page 128](#)

## 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 124](#)  
[How firewall rule groups work on page 122](#)

**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 128](#)

---

## Client Interface Reference — Firewall

The interface reference help topics provide context-sensitive help for pages in the client interface.

**Contents**

- [Firewall — Options](#)
- [Firewall — Rules](#)

## 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 10.2. 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.
	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: <ul style="list-style-type: none"> <li>• <b>Incoming packets</b> if the destination MAC address is in the supported VM MAC address range and is not a local MAC address on the system.</li> <li>• <b>Outgoing packets</b> if the source MAC address is in the supported MAC address range and is not a local MAC address on the system.</li> </ul>
	Enable IP spoof protection	Blocks network traffic from non-local host IP addresses or from local processes that attempt to spoof their IP address.
	Enable dynamic block rules	Allows other Endpoint Security modules to dynamically create and add block rules to the <b>Dynamic Rules</b> group on the Endpoint Security Client.  (Disabled by default)
	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. <ul style="list-style-type: none"> <li>• <b>Add</b> — 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.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Removes the selected domain name from the blocked list.</li> </ul>

**Table 4-2 Advanced options**

Section	Option	Definition
Tuning Options	Enable Adaptive mode	<p>Creates rules automatically to allow traffic.</p> <p> <b>Best practice:</b> 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.</p>
	Disable McAfee core networking rules	<p>Disables the built-in McAfee networking rules (in the <b>McAfee core networking</b> rule group). (Disabled by default)</p> <p> Enabling this option might disrupt network communications on the client.</p>
	Log all blocked traffic	<p>Logs all blocked traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client. (Enabled by default)</p>
	Log all allowed traffic	<p>Logs all allowed traffic to the Firewall event log (FirewallEventMonitor.log) on the Endpoint Security Client. (Disabled by default)</p> <p> Enabling this option might negatively affect performance.</p>
McAfee GTI Network Reputation	Treat McAfee GTI match as intrusion	<p>Treats traffic that matches the McAfee GTI block threshold setting as an <i>intrusion</i>. Enabling this option displays an alert, sends an event to the management server, and adds it Endpoint Security Client log file.</p> <p>Any IP address for a trusted network is excluded from McAfee GTI lookup. (Enabled by default)</p>
	Log matching traffic	<p>Treats traffic that matches the McAfee GTI block threshold setting as a <i>detection</i>. Enabling this option sends an event to the management server and adds it to the Endpoint Security Client log file. (Enabled by default)</p> <p>Any IP address for a trusted network is excluded from McAfee GTI lookup.</p>
	Block all untrusted executables	<p>Blocks all executables that are not signed or have an unknown McAfee GTI reputation.</p>

**Table 4-2 Advanced options** (continued)

Section	Option	Definition
	Incoming network-reputation threshold Outgoing network-reputation threshold	Specifies the McAfee GTI rating threshold for blocking incoming or outgoing traffic from a network connection. <ul style="list-style-type: none"> <li>• <b>Do not block</b> — This site is a legitimate source or destination of content/traffic.</li> <li>• <b>High Risk</b> — This source/destination sends or hosts potentially malicious content/traffic that McAfee considers risky.</li> <li>• <b>Medium Risk</b> — This source/destination shows behavior that McAfee considers suspicious. Any content/traffic from the site requires special scrutiny.</li> <li>• <b>Unverified</b> — This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary.</li> </ul>
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.
Defined Networks		Defines network addresses, subnets, or ranges to use in rules and groups. <ul style="list-style-type: none"> <li>• <b>Add</b> — Adds a network address, subnet, or range to the defined networks list. Click <b>Add</b>, then complete fields in the row define the network.</li> <li>• <b>Double-click an item</b> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected address from the defined networks list.</li> </ul>
	Address type	Specifies the address type of the network to define.
	Trusted	<ul style="list-style-type: none"> <li>• <b>Yes</b> — 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.</li> <li>• <b>No</b> — Adds the network to the list of defined networks for creating rules.</li> </ul>

**Table 4-2 Advanced options** *(continued)*

Section	Option	Definition
<b>Owner</b>		
Trusted Executables		<p>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.</p> <p>Configuring a trusted executable creates a bi-directional Allow rule for that executable at the top of the Firewall rules list.</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Adds a trusted executable.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Removes the executable from the trusted list.</li> </ul>

**See also**

*Configure Firewall options on page 117*

*Define networks to use in rules and groups on page 119*

*Configure trusted executables on page 120*

*Add Executable or Edit Executable on page 138*

## 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.		✓
	<i>Double-click an item</i>	Changes the selected item.	✓	✓
	Duplicate	Creates a copy of the selected item.	✓	✓
	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 126*

*Add Rule or Edit Rule, Add Group or Edit Group on page 134*

## 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 <i>intrusion</i> . Enabling this option displays an alert, sends an event to the management server, and adds it Endpoint Security Client log file.		
		 <b>Best practice:</b> Don't enable this option for an <b>Allow</b> rule because it results in many events.			
		Log matching traffic	Treats traffic that matches the rule as a <i>detection</i> . Enabling this option sends an event to the management server and adds it to the Endpoint Security Client log file.	✓	
Direction	Direction	Specifies the direction:			
		• <b>Either</b> — Monitors both incoming and outgoing traffic.	✓	✓	
		• <b>In</b> — Monitors incoming traffic.			
	• <b>Out</b> — 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).		✓	
	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 <b>Transport</b> and <b>Executables</b> 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 in 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 <b>Allow Rule</b> 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.		✓	

**Table 4-4 Options** (continued)


Section	Option	Definition	Rule Group	
	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.		✓
	Location criteria	<ul style="list-style-type: none"> <li>• <b>Connection-specific DNS suffix</b> — Specifies a connection-specific DNS suffix in the format: <code>example.com</code>.</li> <li>• <b>Default gateway</b> — Specifies a single IP address for a default gateway in IPv4 or IPv6 format.</li> <li>• <b>DHCP server</b> — Specifies a single IP address for a DHCP server in IPv4 or IPv6 format.</li> <li>• <b>DNS server</b> — Specifies a single IP address for a domain name server in IPv4 or IPv6 format.</li> <li>• <b>Primary WINS server</b> — Specifies a single IP address for a primary WINS server in IPv4 or IPv6 format.</li> <li>• <b>Secondary WINS server</b> — Specifies a single IP address for a secondary WINS server in IPv4 or IPv6 format.</li> <li>• <b>Domain reachability</b> — Requires that the specified domain is reachable.</li> <li>• <b>Registry key</b> — Specifies the registry key and key value.                             <ol style="list-style-type: none"> <li>1 Click <b>Add</b>.</li> <li>2 In the <b>Value</b> column, specify the registry key in the format: <code>&lt;ROOT&gt;\&lt;KEY&gt;\ [VALUE_NAME]</code> <ul style="list-style-type: none"> <li>• <b>&lt;ROOT&gt;</b> — Must use the full root name, such as <code>HKEY_LOCAL_MACHINE</code>, and not the shortened <code>HKLM</code>.</li> <li>• <b>&lt;KEY&gt;</b> — Is the key name under the root.</li> <li>• <b>[VALUE_NAME]</b> — is the name of the key value. If no value name is included, it is assumed to be the default value.</li> </ul> </li> </ol> <p>Example formats:</p> <ul style="list-style-type: none"> <li>• <b>IPv4</b> — <code>123.123.123.123</code></li> <li>• <b>IPv6</b> — <code>2001:db8:c0fa:f340:9219: bd20:9832:0ac7</code></li> </ul> </li> </ul>		
<b>Networks</b>		Specifies the network host options that apply to the item.	✓	✓
	<b>Network protocol</b>	Specifies the network protocol that applies to the item.	✓	✓
	<b>Any protocol</b>	Allows both IP and non-IP protocols. If a transport protocol or an application is specified, only IP protocols are allowed.	✓	✓
	<b>IP protocol</b>	Excludes non-IP protocols. <ul style="list-style-type: none"> <li>• <b>IPv4 protocol</b></li> <li>• <b>IPv6 protocol</b></li> </ul> 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
	<b>Non-IP protocol</b>	Includes non-IP protocols only. <ul style="list-style-type: none"> <li>• <b>Select EtherType from list</b> — Specifies an EtherType.</li> <li>• <b>Specify custom EtherType</b> — Specifies the four-characters of the hexadecimal EtherType value of the non-IP protocol. See <a href="#">Ethernet Numbers</a> for EtherType values. For example, enter 809B for AppleTalk, 8191 for NetBEUI, or 8037 for IPX.</li> </ul>	✓	✓
	<b>Connection types</b>	Indicates if one or all connection types apply: <ul style="list-style-type: none"> <li>• <b>Wired</b></li> <li>• <b>Wireless</b></li> <li>• <b>Virtual</b></li> </ul> <p>A <b>Virtual</b> connection type is an adapter presented by a VPN or a virtual machine application, such as VMware, rather than a physical adapter.</p>	✓	✓
	<b>Specify networks</b>	Specifies the networks that apply to the item. <ul style="list-style-type: none"> <li>• <b>Add</b> — Creates and adds a network.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Removes the network from the list.</li> </ul>	✓	✓
<b>Transport</b>		Specifies transport options that apply to the item.		
	<b>Transport protocol</b>	Specifies the transport protocol associated with the item. Select the protocol, then click <b>Add</b> to add ports. <ul style="list-style-type: none"> <li>• <b>All protocols</b> — Allows IP, non-IP, and unsupported protocols.</li> <li>• <b>TCP and UDP</b> — Select from the drop-down: <ul style="list-style-type: none"> <li>• <b>Local port</b> — Specifies the local traffic service or port to which the item applies.</li> <li>• <b>Remote port</b> — Specifies the traffic service or port on another computer to which the item applies.</li> </ul> <p><b>Local port and Remote port can be:</b></p> <ul style="list-style-type: none"> <li>• A single service. For example, 23.</li> <li>• A range. For example, 1-1024.</li> <li>• A comma-separated list of single ports and ranges. For example, 80, 8080, 1-10, 8443 (up to 4 items).</li> </ul> <p>By default, rules apply to all services and ports.</p></li> </ul> <ul style="list-style-type: none"> <li>• <b>ICMP</b> — In the <b>Message type</b> drop-down, specify an ICMP message type. See <a href="#">ICMP</a>.</li> <li>• <b>ICMPv6</b> — In the <b>Message type</b> drop-down, specify an ICMP message type. See <a href="#">ICMPv6</a>.</li> <li>• <b>Other</b> — Selects from a list of less common protocols.</li> </ul>	✓	✓



**Table 4-4 Options** *(continued)*

Section	Option	Definition	Rule	Group
Executables		<p>Specifies the executables that apply to the rule.</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Creates and adds an executable.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Removes an executable from the list.</li> </ul>	✓	✓
Schedule		<p>Specifies schedule settings for the rule or group.</p>	✓	✓
	<b>Enable schedule</b>	<p>Enables the schedule for the timed rule or group.</p> <p>When the schedule is disabled, the rule or rules in the group, don't apply.</p> <ul style="list-style-type: none"> <li>• <b>Start time</b> — Specifies the start time to enable the schedule.</li> <li>• <b>End time</b> — Specifies the time to disable the schedule.</li> <li>• <i>Days of the week</i> — Specifies the days of the week to enable the schedule.</li> </ul> <p>For start and end times, use a 24-hour clock style. For example, 13:00 = 1:00 p.m.</p> <p>You can either schedule Firewall timed groups or allow the user to enable them from the McAfee system tray icon.</p>	✓	✓
	<b>Disable schedule and enable the group from the McAfee system tray icon</b>	<p>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.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> <b>Best practice:</b> Use this option to allow broad network access, for example at a hotel, before a VPN connection can be established.</p> </div> <p>Selecting this option displays more menu options under <b>Quick Settings</b> in the McAfee system tray icon:</p> <ul style="list-style-type: none"> <li>• <b>Enable Firewall Timed Groups</b> — 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 <b>Disable Firewall Timed Groups</b>.</li> </ul> <p>Each time you select this option, you reset the time for the groups.</p> <p>Depending on settings, you might be prompted to provide the administrator with a reason for enabling timed groups.</p> <ul style="list-style-type: none"> <li>• <b>View Firewall Timed Groups</b> — Displays the names of the timed groups and the amount of time remaining for each group to be active.</li> </ul>		✓
	<b>Number of minutes (1-60) to enable the group</b>	<p>Specifies the number of minutes (1–60) that the timed group is enabled after selecting <b>Enable Firewall Timed Groups</b> from the McAfee system tray icon.</p>		✓

**See also**

[Create and manage Firewall rules and groups on page 126](#)

[Create timed groups on page 129](#)

[Enable or view Firewall timed groups from the McAfee system tray icon on page 116](#)

[Add Network or Edit Network on page 139](#)

[Add Executable or Edit Executable on page 138](#)

**Add Executable or Edit Executable**

Add or edit an executable associated with a rule or group.

**Table 4-5 Options**

Option	Definition
<b>Name</b>	Specifies the name that you call the executable. This field is required with at least one other field: <b>File name or path</b> , <b>File description</b> , <b>MD5 hash</b> , or <b>signer</b> .
<b>File name or path</b>	Specifies the file name or path of the executable to add or edit. Click <b>Browse</b> to select the executable. The file path can include wildcards.
<b>File description</b>	Indicates the description of the file.
<b>MD5 hash</b>	Indicates the (32-digit hexadecimal number) MD5 hash of the process.
<b>Signer</b>	<p><b>Enable digital signature check</b> — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash. If enabled, specify:</p> <ul style="list-style-type: none"> <li>• <b>Allow any signature</b> — Allows files signed by any process signer.</li> <li>• <b>Signed by</b> — Allows only files signed by the specified process signer.</li> </ul> <p>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.</p> <p>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</p> <p>To obtain the SDN of an executable:</p> <ol style="list-style-type: none"> <li>1 Right-click an executable and select <b>Properties</b>.</li> <li>2 On the <b>Digital Signatures</b> tab, select a signer and click <b>Details</b>.</li> <li>3 On the <b>General</b> tab, click <b>View Certificate</b>.</li> <li>4 On the <b>Details</b> tab, select the <b>Subject</b> field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: <ul style="list-style-type: none"> <li>• CN = Mozilla Corporation</li> <li>• OU = Release Engineering</li> <li>• O = Mozilla Corporation</li> <li>• L = Mountain View</li> <li>• S = California</li> <li>• C = US</li> </ul> </li> </ol>
<b>Notes</b>	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: <ul style="list-style-type: none"> <li>• <b>Local network</b> — Creates and adds a local network.</li> <li>• <b>Remote network</b> — Creates and adds a remote network.</li> </ul>	✓	✓
Add	Adds a network type to the network list.	✓	✓
<i>Double-click an item</i>	Changes the selected item.		
Delete	Deletes the selected item.	✓	✓
Address type	Specifies the origin or destination of traffic. Select from the <b>Address type</b> drop-down list.	✓	✓
Address	Specifies the IP address to add to the network. Wildcards are valid.	✓	✓

### See also

[Address type](#) on page 139

## 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: <ul style="list-style-type: none"> <li>• <b>IPv4</b> — 123.123.123.123</li> <li>• <b>IPv6</b> — 2001:db8::c0fa:f340:9219:bd20:9832:0ac7*</li> </ul>
Subnet	Specifies the subnet address of any adapter on the network. For example: <ul style="list-style-type: none"> <li>• <b>IPv4</b> — 123.123.123.0/24</li> <li>• <b>IPv6</b> — 2001:db8::0/32</li> </ul>
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: <ul style="list-style-type: none"> <li>• <b>IPv4</b> — 123.123.1.0 - 123.123.255.255</li> <li>• <b>IPv6</b> — 2001:db8::0000:0000:0000:0000 - 2001:db8::ffff:ffff:ffff:ffff</li> </ul>
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*
- ▶ *Access Web Control features*
- ▶ *Managing Web Control*
- ▶ *Client Interface Reference — Web Control*

---

## About Web Control features

As Web Control runs on each managed system, it notifies you about threats while you 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 you about web-based threats that you 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. You 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. You can access more information by clicking the button.

The button also notifies you 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 your 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 you from uninstalling or changing Web Control files, registry keys, registry values, services, and processes.
- Customize the notification that appears when you attempt 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.

The software supports Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome browsers.

On self-managed systems, all browsers — supported and unsupported — are allowed by default.

Chrome doesn't support the **Show Balloon** option.

### See also

*Web Control button identifies threats while browsing on page 142*

*Safety icons identify threats while searching on page 143*

*Site reports provide details on page 144*

*How safety ratings are compiled on page 144*

## How Web Control blocks or warns a site or download

When a user visits 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 146](#)

## 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 147](#)

**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.

<b>This item...</b>	<b>Indicates...</b>
Overview	<p>The overall rating for the website, determined from these tests:</p> <ul style="list-style-type: none"> <li>• Evaluation of a website's email and download practices using proprietary data collection and analysis techniques.</li> <li>• 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.</li> <li>• Analysis of the website's online affiliations to see if it associates with other suspicious sites.</li> <li>• Combination of the McAfee review of suspicious sites with feedback from our Threat Intelligence services.</li> </ul>
Online Affiliations	<p>How aggressively the site tries to get you to go to other sites that McAfee flagged with a red rating.</p> <p>Suspicious sites often associate with other suspicious sites. The primary purpose of <i>feeder</i> 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 <i>red by association</i>.</p>
Web Spam Tests	<p>The overall rating for a website's email practices, based on the test results.</p> <p>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.</p>
Download Tests	<p>The overall rating about the impact a site's downloadable software had on our test computer, based on the test results.</p> <p>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.</p>

**See also**

[View site report while searching on page 147](#)

[View information about a site while browsing on page 146](#)

**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 145](#)  
On some browsers, 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 146](#)  
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 147](#)  
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

On some browsers, 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.

When you first start Internet Explorer or Chrome, you are prompted to enable plug-ins. The Web Control plug-in is enabled by default on Firefox.

### Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- At the prompt, click the button to 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**.

**Firefox**

- Click **Add-ons | Extensions**.
- Click **Enable** to activate the Endpoint Security Web Control extension.
- Restart Firefox.



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 142*

*Site reports provide details on page 144*

## 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 143*

*Site reports provide details on page 144*

---

## 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 <b>Hide the toolbar on the client browser</b> .	
Track browser events to use for reports.	Configure settings in the <b>Event Logging</b> 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 <b>Action Enforcement</b> , select the action ( <b>Block</b> , <b>Allow</b> , or <b>Warn</b> ) for sites not yet verified by McAfee GTI.	
Scan files before downloading.	In <b>Action Enforcement</b> , select <b>Enable file scanning for file downloads</b> , then select the McAfee GTI risk level to block.	
Add external sites to the local private network.	In <b>Action Enforcement</b> , under <b>Specify additional IP addresses and ranges to allow</b> , click <b>Add</b> , then enter an external IP address or range.	
Block risky sites from appearing in search results.	In <b>Secure Search</b> , select <b>Enable Secure Search</b> , 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.

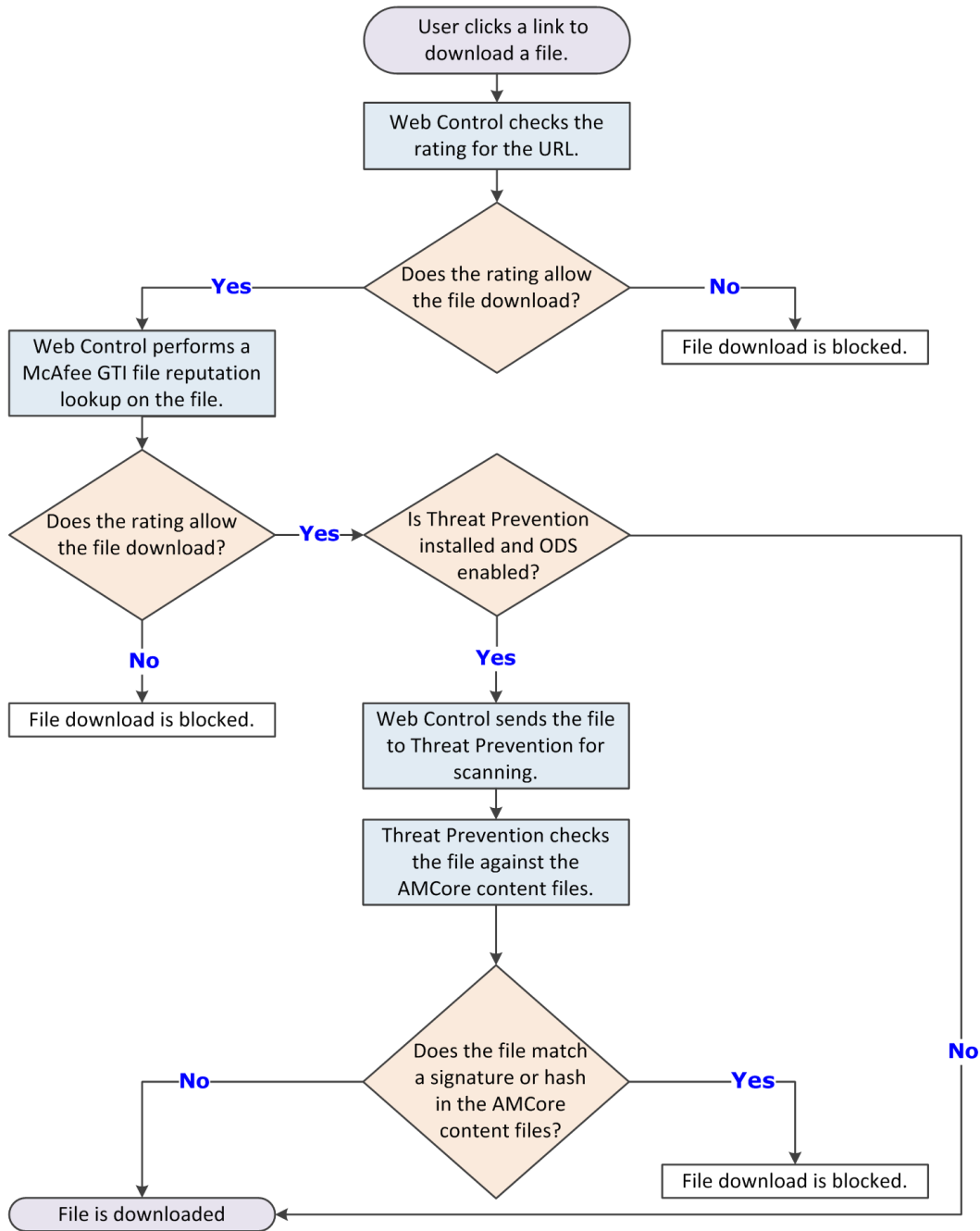
- 6 Configure other options as needed.
- 7 Click **Apply** to save your changes or click **Cancel**.

#### See also

[How file downloads are scanned on page 149](#)  
[Log on as administrator on page 27](#)

## How file downloads are scanned

Web Control sends file download requests to Threat Prevention for scanning before downloading.



## 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 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 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. However, allowing more detections can result in more false positive results.

- For Threat Prevention, the McAfee GTI sensitivity level is set to Medium by default. Configure the sensitivity level for each scanner in the Threat Prevention settings.
- For Web Control, 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** settings.

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

## 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.



Use the settings in Enforcement Messaging to customize the message to display for blocked and warned sites and file downloads, and blocked phishing pages.

### 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 151](#)

[Using safety ratings to control access on page 151](#)

[Log on as administrator on page 27](#)

**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.

For each site or file download, specify whether to allow, warn, or block, based on the 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.

---

## Client Interface Reference — Web Control

The interface reference help topics provide context-sensitive help for pages in the client interface.

**Contents**

- ▶ [Web Control — Options](#)
- ▶ [Web Control — Content Actions](#)

**Web Control — Options**


Configure general Web Control settings, which include enabling, specifying 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.

**Table 5-1 Options** (continued)

Section	Option	Definition
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. <ul style="list-style-type: none"> <li>• <b>Allow</b> (Default) — Permits users to access the site.</li> <li>• <b>Warn</b> — Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before continuing.</li> <li>• <b>Block</b> — Prevents users from accessing the site and displays a message that the site download is blocked.</li> </ul>
	Enable HTML iFrames support	Blocks access to malicious (Red) and warn (Yellow) sites that appear in an HTML iframe. (Enabled by default)
	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. <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <b>Best practice:</b> Use this option to treat external sites as if they belong to the local network. </div> <ul style="list-style-type: none"> <li>• <b>Add</b> — Adds an IP address to the list of private addresses in the local network.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes an IP address from the list of private addresses in the local network.</li> </ul>
	Secure Search	Enable Secure Search
	Set the default search engine in supported browsers	Specifies the default search engine to use for supported browsers: <ul style="list-style-type: none"> <li>• Yahoo</li> <li>• Google</li> <li>• Bing</li> <li>• Ask</li> </ul>
	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 147*

*How file downloads are scanned on page 149*


*McAfee GTI on page 109*

**Web Control — Content Actions**

Define actions to take for rated sites and web content categories.

For sites and file downloads in the unblocked categories, Web Control applies the rating actions.

**Table 5-4 Options**

Section	Option	Definition
Rating Actions	Rating actions for sites	<p>Specifies actions for sites that are rated red, yellow, or unrated. Green-rated sites and downloads are allowed automatically.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b> — Permits users to access the site. (Default for <b>Unrated</b> sites)</li> <li>• <b>Warn</b> — Displays a warning to notify users of potential dangers associated with the site. Users must click <b>Cancel</b> to return to the previously viewed site or <b>Continue</b> to proceed to the site. If browser tab has no previously viewed site, <b>Cancel</b> is unavailable. (Default for <b>Yellow</b> sites)</li> <li>• <b>Block</b> — Prevents users from accessing the site and displays a message that the site is blocked. Users must click <b>OK</b> to return to the previously viewed site. If browser tab has no previously viewed site, <b>OK</b> is unavailable. (Default for <b>Red</b> sites)</li> </ul>
	Rating actions for file downloads	<p>Specifies actions for file downloads that are rated red, yellow, or unrated. These Rating Actions are applicable only when <b>Enable file scanning for file downloads</b> is enabled in the <b>Options</b> settings.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b> — Permits users to proceed with the download. (Default for <b>Unrated</b> sites)</li> <li>• <b>Warn</b> — 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 <b>Yellow</b> sites)</li> <li>• <b>Block</b> — Displays a message that the download is blocked and prevents users from downloading the file. (Default for <b>Red</b> sites)</li> </ul> <p> Use settings in Enforcement Messaging to customize the message.</p>

**Table 5-5 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 150*

*Using safety ratings to control access on page 151*

*Using web categories to control access on page 151*

# 6

## Using Threat Intelligence

Threat Intelligence provides context-aware adaptive security for your network environment.

Endpoint Security Threat Intelligence 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.



Threat Intelligence isn't supported on McAfee ePO Cloud-managed systems.

### Contents

- ▶ [How Threat Intelligence works](#)
- ▶ [Managing Threat Intelligence](#)
- ▶ [Client Interface Reference — Threat Intelligence](#)

---

## How Threat Intelligence works

Threat Intelligence uses the Data Exchange Layer framework to share file and threat information instantly across the entire network.

In the past, you sent an unknown file or certificate to McAfee for analysis, then updated the file information throughout the network days later. Threat Intelligence enables file reputation to be controlled at a local level, your environment. You decide which files can run and which are blocked, and the Data Exchange Layer shares the information immediately throughout your environment.

### Scenarios for using Threat Intelligence

- **Immediately block a file** — Threat Intelligence 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 Threat Intelligence to learn whether the file is a threat and how many systems ran the file.
- **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 prompting.
- **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 category. Containment rules define which actions the contained application is allowed to perform.

## Managing Threat Intelligence

As administrator, you can specify Threat Intelligence settings, such as selecting rule groups and setting reputation thresholds.



Policy changes from McAfee ePO overwrite changes from the Settings page.



Threat Intelligence isn't supported on McAfee ePO Cloud-managed systems.

### About Threat Intelligence

Threat Intelligence provides a security ecosystem that allows instant communication between systems and devices in your environment. This communication is made possible with the Data Exchange Layer framework.

You can see the specific system where a threat was first detected, where it went from there, and stop it immediately.

Threat Intelligence 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 block, allow, or contain specific files and certificates based on their threat reputations and your risk criteria.
- 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.



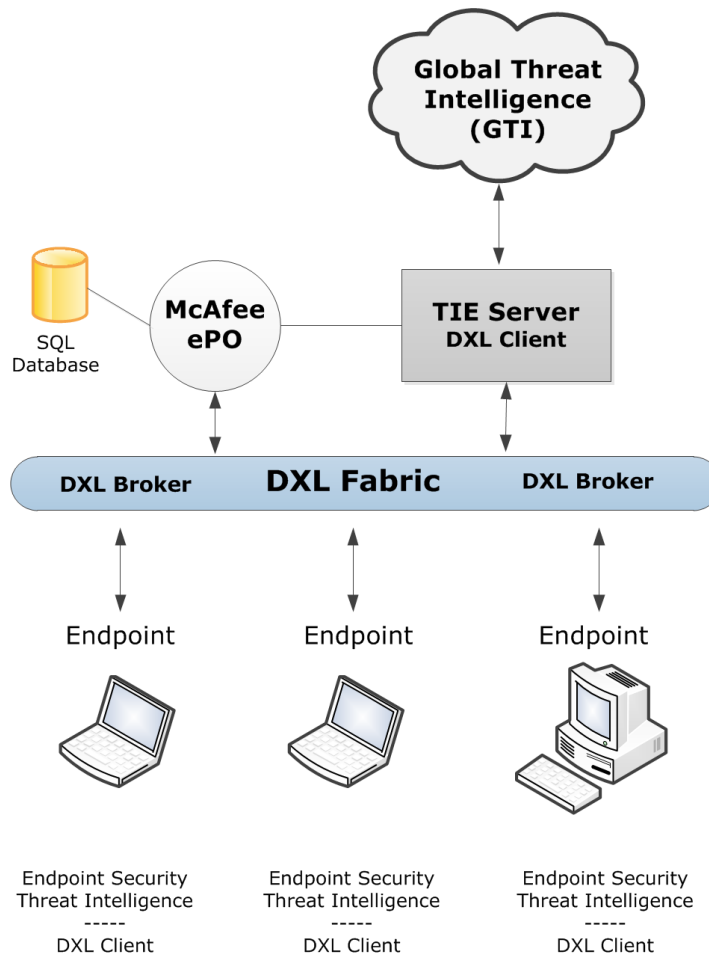
Threat Intelligence isn't supported on McAfee ePO Cloud-managed systems.

### Threat Intelligence components

Threat Intelligence includes these components.

- A module for Endpoint Security that allows you to create policies for blocking, allowing, or containing a file or certificate based on its reputation.
- A server that stores information about file and certificate reputations, then passes that information to other systems.
- Data Exchange Layer brokers that allow bidirectional communication between managed systems on a network.

These components are installed as McAfee® ePolicy Orchestrator® (McAfee ePO™) extensions and add several new features and reports.



The module and 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<sup>®</sup> Enterprise Security Manager (McAfee<sup>®</sup> ESM) and McAfee<sup>®</sup> Network Security Platform.

### Threat Intelligence module

The Threat Intelligence module 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.

You can perform these tasks using the Threat Intelligence module.

The client uses rules for determining actions based on multiple datapoints such as reputations, local intelligence, and contextual information. You can update the rules independently.

- Create policies to:
  - Allow, block, clean, or contain files depending on their reputation.
  - Receive a prompt each time a file or certificate with a certain reputation attempts to run.
  - Send files automatically to Advanced Threat Defense for further evaluation.
- View events on the Threat Intelligence dashboards. You can view allowed, blocked, cleaned, and contained events for the past 30 days or by event type.

## Threat Intelligence Exchange server

The server stores information about file and certificate reputations, then passes that information to other systems in your environment.

For information about the server, see the *Threat Intelligence Exchange Product Guide*.

## Combining TIE servers and databases

If you have TIE servers and databases managed by different McAfee ePO systems, you can combine them to share reputation information. For details about combining TIE servers and databases, see *McAfee Data Exchange Layer Product Guide*, and the KnowledgeBase article [KB83896](#).

## Data Exchange Layer

The Data Exchange Layer includes client software and brokers that allow bidirectional communication between endpoints on a network.

The Data Exchange Layer works in the background, communicating with services, databases, endpoints, and applications. The Data Exchange Layer client is installed on each managed endpoint, so that threat information from security products that use DXL can be shared immediately with all other services and devices. Sharing reputation information as soon as it is available reduces the security assumptions that applications and services make about each other when they exchange information. This shared information reduces the spread of threats.

See *McAfee Data Exchange Layer Product Guide* for details about installing and using Data Exchange Layer.

## 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 inspects the file and can't determine its validity and reputation.
- 3 The Threat Intelligence module inspects the file and gathers file and local system properties of interest.
- 4 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.
- 5 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.
- 6 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 one of the following is 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*.

- 7 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 Threat Intelligence module. If McAfee Web Gateway is present and eventually sends a reputation score, Threat Intelligence returns the reputation of the file.
- 8 The module evaluates this metadata to determine the file's reputation:
  - File and system properties
  - Enterprise age and prevalence data
  - Reputation
- 9 The module acts based on the policy assigned to the system that is running the file.
- 10 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.
- 11 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 Threat Intelligence-enabled systems to immediately protect your environment. Threat Intelligence or any other McAfee product can initiate this process. In either case, Threat Intelligence processes the reputation and saves it in the database.

For information about how Advanced Threat Defense is integrated with Threat Intelligence, 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 Threat Intelligence cache is flushed when the rules configuration changes:
  - The state of one or more rules has changed, for example from enabled to disabled.
  - The set of rules 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 Threat Intelligence receives notice for the file, the reputation is recalculated.

## Getting started

After you install Threat Intelligence, what do you do next?

To get started with Threat Intelligence, do the following:

- 1 Create Threat Intelligence policies to determine what is blocked, allowed, or contained. Then, run Threat Intelligence in Observe mode to build file prevalence and observe what Threat Intelligence detects in your environment. File prevalence indicates how often a file is seen in your environment.
- 2 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 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 Threat Intelligence 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 but no action is taken. You can see what Threat Intelligence 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 in your environment. 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.

### 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 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 Threat Intelligence 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
<b>File and certificate</b>	<ul style="list-style-type: none"> <li>• TIE server and module versions</li> <li>• Reputation override settings made with the TIE server</li> <li>• External reputation information, for example from Advanced Threat Defense</li> </ul>
<b>File-only</b>	<ul style="list-style-type: none"> <li>• File name, path, size, product, publisher, and prevalence</li> <li>• SHA-1, SHA-256, and MD5 information</li> <li>• Operating system version of the reporting computer</li> <li>• Maximum, minimum, and average reputation set for the file</li> <li>• Whether the reporting module is in Observe mode</li> <li>• Whether the file was allowed to run, was blocked, contained, or cleaned</li> <li>• The product that detected the file, for example Advanced Threat Defense or Threat Prevention</li> </ul>
<b>Certificate-only</b>	<ul style="list-style-type: none"> <li>• SHA-1 information</li> <li>• The name of the certificate's issuer and its subject</li> <li>• The date the certificate was valid and its expiration date</li> </ul>

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, Threat Intelligence requests that Dynamic Application Containment contain the application. Contained applications are 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 Threat Intelligence or TIE server to allow it to run normally.

To use Dynamic Application Containment:

- 1 Enable Threat Intelligence 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 165](#)

[Configure McAfee-defined containment rules on page 166](#)

[Enable the Dynamic Application Containment trigger threshold on page 165](#)

## How Dynamic Application Containment works

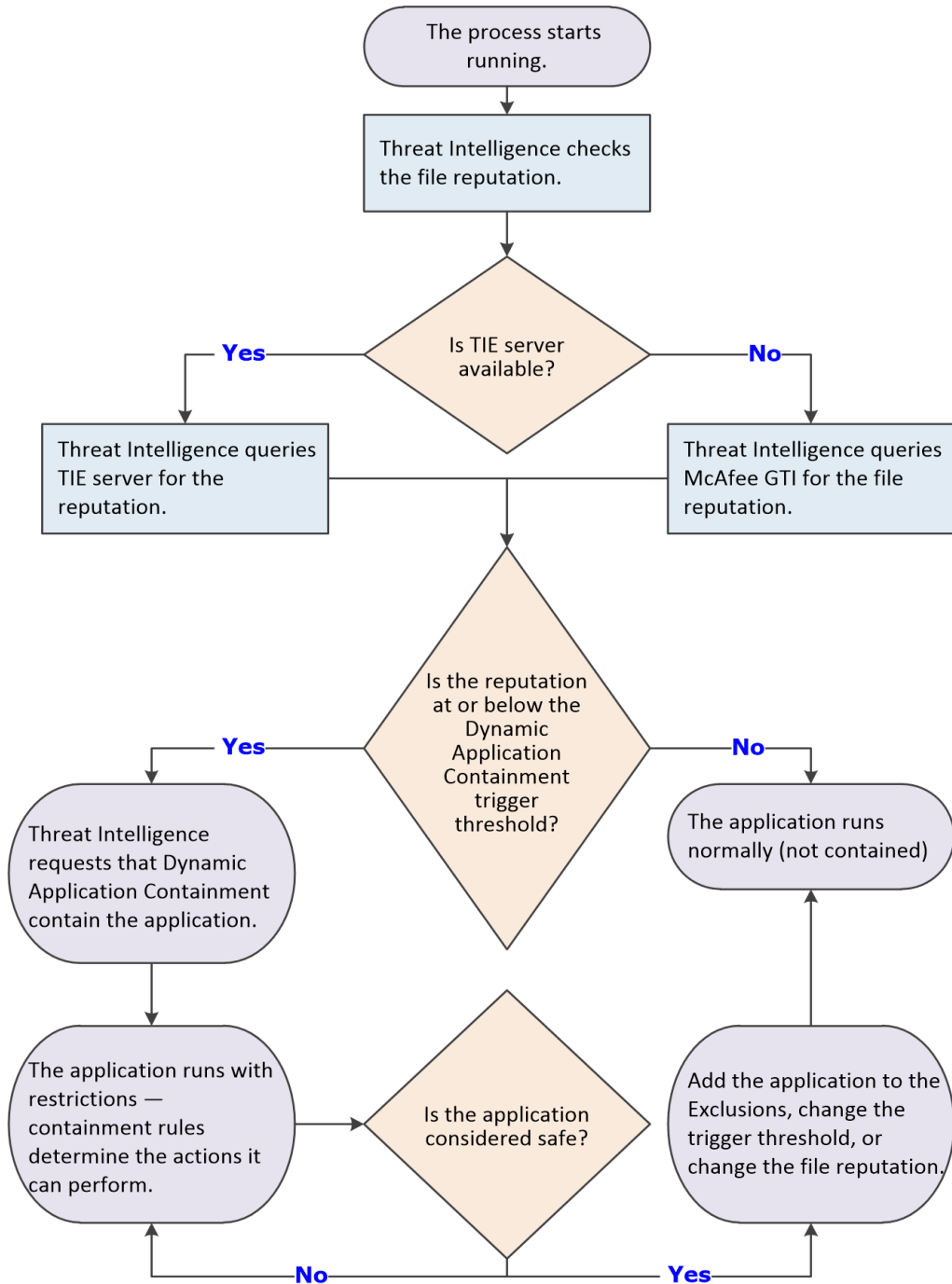
Threat Intelligence uses an application's reputation to determine whether to request that Dynamic Application Containment run the application with restrictions. When a file with the specified reputation

runs in your environment, Dynamic Application Containment blocks or logs unsafe actions, based on containment rules.

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 Threat Intelligence checks the file reputation.  
Threat Intelligence uses TIE server, if it is available, for the application reputation. If TIE server isn't available, Threat Intelligence uses McAfee GTI for reputation information.
- 3 If the application reputation is at or below the Threat Intelligence containment reputation threshold, Threat Intelligence 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**

*Configure McAfee-defined containment rules on page 166*

*Allowing contained applications to run normally on page 165*

## 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 Threat Intelligence 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 **Might be 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 168](#)

## 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 **Threat Intelligence** on the main **Status** page.  
Or, from the **Action** menu , select **Settings**, then click **Threat Intelligence** on the **Settings** page.
- 3 Click **Show Advanced**.
- 4 Click **Options**.
- 5 Verify that Threat Intelligence 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** (Default for the **Security** rule group)
  - **Unknown** (Default for the **Balanced** rule group)
  - **Might Be Malicious** (Default for the **Productivity** rule group)

- **Most Likely Malicious**
- **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.

### Task

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

- 1 Select **Menu | Policy | Policy Catalog**, then select **Endpoint Security Threat Intelligence** from the **Product** list.
- 2 Open the Endpoint Security Client.
- 3 Click **Threat Intelligence** on the main **Status** page.  
Or, from the **Action** menu , select **Settings**, then click **Threat Intelligence** on the **Settings** page.
- 4 Click **Show Advanced**.
- 5 Click **Dynamic Application Containment**.
- 6 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**.
- 7 In the **Exclusions** section, configure executables to exclude from Dynamic Application Containment. Processes in the **Exclusions** list run normally (not contained).
- 8 Click **Apply** to save your changes or click **Cancel**.

### See also

[Exclude processes from Dynamic Application Containment on page 168](#)  
[McAfee-defined containment rules on page 166](#)

## McAfee-defined containment rules

McAfee-defined containment rules to control what changes contained applications can make to your system.



You can change the block and report settings, but you can't otherwise modify or delete these rules.

- **Accessing insecure password LM hashes**
- **Accessing user cookie locations**
- **Allocating memory in another process**

- Creating a thread in another process
- Creating files on any network location
- Creating files on CD, floppy, and removable drives
- Creating files with the .bat extension
- Creating files with the .exe extension
- Creating files with the .html, .jpg, or .bmp extension
- Creating files with the .job extension
- Creating files with the .vbs extension
- Creating new CLSIDs, APPIDs, and TYPELIBs
- Deleting files commonly targeted by ransomware-class malware
- Disabling critical operating system executables
- Executing any child process
- Modifying appinit DLL registry entries
- Modifying application compatibility shims
- Modifying critical Windows files and registry locations
- Modifying desktop background settings
- Modifying file extension associations
- Modifying files with the .bat extension
- Modifying files with the .vbs extension
- Modifying Image File Execution Options registry entries
- Modifying portable executable files
- Modifying screen saver settings
- Modifying startup registry locations
- Modifying the automatic debugger
- Modifying the hidden attribute bit
- Modifying the read-only attribute bit
- Modifying the Services registry location
- Modifying the Windows Firewall policy
- Modifying the Windows Tasks folder
- Modifying user policies
- Modifying users' data folders
- Reading files commonly targeted by ransomware-class malware
- Reading from another process' memory
- Reading or modifying files on any network location

- Reading or modifying files on CD, floppy, and removable drives
- Suspending a process
- Terminating another process
- Writing to another process' memory
- Writing to files commonly targeted by ransomware-class malware

## 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 **Threat Intelligence** on the main **Status** page.  
Or, from the **Action** menu , select **Settings**, then click **Threat Intelligence** 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**.  
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.
- 6 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 **Threat Intelligence** on the main **Status** page.  
Or, from the **Action** menu , select **Settings**, then click **Threat Intelligence** 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 Threat Intelligence options

Use settings to 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 **Threat Intelligence** on the main **Status** page.  
Or, from the **Action** menu , select **Settings**, then click **Threat Intelligence** 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 Threat Intelligence 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 **Threat Intelligence**.

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.

## Client Interface Reference — Threat Intelligence

The interface reference help topics provide context-sensitive help for pages in the client interface.


### Contents

- ▶ [Threat Intelligence — Dynamic Application Containment](#)
- ▶ [Threat Intelligence — Options](#)

## Threat Intelligence — 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		<p>Configures Dynamic Application Containment rules.</p> <p>You can change whether McAfee-defined containment rules block or report, but you can't otherwise change or delete these rules.</p> <ul style="list-style-type: none"> <li>• <b>Block (only)</b> — Blocks, without logging, contained applications from performing actions specified by the rule.</li> <li>• <b>Report (only)</b> — Logs when applications try to perform actions in the rule, but doesn't prevent applications from performing actions.</li> <li>• <b>Block and Report</b> — Blocks and logs access attempts.</li> </ul> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p> <b>Best practice:</b> When the full impact of a rule is not known, select <b>Report</b> but not <b>Block</b> to receive a warning without blocking access attempts. To determine whether to block access, monitor the logs and reports.</p> </div> <p>To block or report all, select <b>Block</b> or <b>Report</b> in the first row.</p> <p>To disable the rule, deselect both <b>Block</b> and <b>Report</b>.</p>
Contained Applications		<p>Lists applications that are currently contained.</p> <ul style="list-style-type: none"> <li>• <b>Exclude</b> — Moves a contained application to the <b>Exclusions</b> list, releasing it from containment and allowing it to run normally.</li> </ul>
Exclusions		<p>Excludes processes from containment.</p> <ul style="list-style-type: none"> <li>• <b>Add</b> — Adds a process to the exclusion list.</li> <li>• <i>Double-click an item</i> — Changes the selected item.</li> <li>• <b>Delete</b> — Deletes the selected item.</li> <li>• <b>Duplicate</b> — Creates a copy of the selected item.</li> </ul>

### See also

[How Dynamic Application Containment works on page 162](#)

[McAfee-defined containment rules on page 166](#)

[Configure McAfee-defined containment rules on page 166](#)

[Exclude processes from Dynamic Application Containment on page 168](#)

## Add Executable or Edit Executable

Add or edit an executable to exclude or include.

For Threat Prevention Access Protection, you can exclude executables at the policy level, or include or exclude at the rule level. For Threat Intelligence Dynamic Application Containment, you can exclude executables at the policy 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 6-2 Options**

Option	Definition
<b>Name</b>	Specifies the name that you call the executable. This field is required with at least one other field: <b>File name or path</b> , <b>MD5 hash</b> , or <b>Signer</b> .
<b>Inclusion status</b>	Determines the inclusion status for the executable. <ul style="list-style-type: none"> <li>• <b>Include</b> — Triggers the rule if the executable violates a subrule.</li> <li>• <b>Exclude</b> — Doesn't trigger the rule if the executable violates a subrule.</li> </ul> <b>Inclusion status</b> only appears for Threat Prevention Access Protection when adding an executable to a rule or the target for the Processes subrule.
<b>File name or path</b>	Specifies the file name or path of the executable to add or edit. Click <b>Browse</b> to select the executable. The file path can include wildcards.
<b>MD5 hash</b>	Indicates the (32-digit hexadecimal number) MD5 hash of the process.

**Table 6-2 Options** (continued)

Option	Definition
<b>Signer</b>	<p><b>Enable digital signature check</b> — Guarantees that code hasn't been changed or corrupted since it was signed with cryptographic hash.</p> <p>If enabled, specify:</p> <ul style="list-style-type: none"> <li>• <b>Allow any signature</b> — Allows files signed by any process signer.</li> <li>• <b>Signed by</b> — Allows only files signed by the specified process signer.</li> </ul> <p>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.</p> <p>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:</p> <p>C=US, S=WASHINGTON, L=REDMOND, O=MICROSOFT CORPORATION, OU=MOPR, CN=MICROSOFT WINDOWS</p> <p>To obtain the SDN of an executable:</p> <ol style="list-style-type: none"> <li>1 Right-click an executable and select <b>Properties</b>.</li> <li>2 On the <b>Digital Signatures</b> tab, select a signer and click <b>Details</b>.</li> <li>3 On the <b>General</b> tab, click <b>View Certificate</b>.</li> <li>4 On the <b>Details</b> tab, select the <b>Subject</b> field. Signer distinguished name appears. For example, Firefox has this signer distinguished name: <ul style="list-style-type: none"> <li>• CN = Mozilla Corporation</li> <li>• OU = Release Engineering</li> <li>• O = Mozilla Corporation</li> <li>• L = Mountain View</li> <li>• S = California</li> <li>• C = US</li> </ul> </li> </ol>
<b>Notes</b>	Provides more information about the item.


## Threat Intelligence — Options

Configure settings for Threat Intelligence.


**Table 6-3 Options**

Section	Option	Definition
<b>Options</b>	<b>Enable Threat Intelligence</b>	Enables the Threat Intelligence module. (Disabled by default)
	<b>Allow the Threat Intelligence Exchange server to collect anonymous diagnostic and usage data</b>	Allows the TIE server to send anonymous file information to McAfee.
	<b>Use McAfee GTI file reputation if the Threat Intelligence Exchange server is not reachable</b>	Gets file reputation information from the Global Threat Intelligence proxy if the TIE server is unavailable.

**Table 6-3 Options** (continued)

Section	Option	Definition
	<b>Prevent users from changing settings (Threat Intelligence Exchange 1.0 clients only)</b>	Prevents users on managed systems from changing Threat Intelligence settings.
<b>Rule Assignment</b>	<b>Productivity</b>	<p>Assigns the <b>Productivity</b> rule group.</p> <p>Use this group for high-change systems with frequent installations and updates of trusted software.</p> <p>This group uses the least number of rules. Users experience minimum prompts and blocks when new files are detected.</p>
	<b>Balanced</b>	<p>Assigns the <b>Balanced</b> rule group.</p> <p>Use this group for typical business systems with infrequent new software and changes.</p> <p>This group uses more rules — and users experience more prompts and blocks — than the <b>Productivity</b> group.</p>
	<b>Security</b>	<p>Assigns the <b>Security</b> rule group.</p> <p>Use this group for low-change systems, such as IT-managed systems and servers with tight control.</p> <p>Users experience more prompts and blocks than with the <b>Balanced</b> group.</p>
<b>Action Enforcement</b>	<b>Enable Observe mode</b>	<p>Generates events and sends them to the server, but doesn't enforce actions.</p> <p>Enable Observe mode temporarily on a few systems only while tuning Threat Intelligence.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  Because enabling this mode causes Threat Intelligence to generate events but not enforce actions, your systems might be vulnerable to threats.                 </div>
	<b>Trigger Dynamic Application Containment when reputation threshold reaches</b>	<p>Contains applications when the reputation reaches the specified threshold:</p> <ul style="list-style-type: none"> <li>• <b>Might Be Trusted</b> (Default for the <b>Security</b> rule group)</li> <li>• <b>Unknown</b> (Default for the <b>Balanced</b> rule group)</li> <li>• <b>Might Be Malicious</b> (Default for the <b>Productivity</b> rule group)</li> <li>• <b>Most Likely Malicious</b></li> <li>• <b>Known Malicious</b></li> </ul> <p>The Dynamic Application Containment reputation threshold must be higher than the block and clean thresholds. For example, if the block threshold is set to <b>Known Malicious</b>, the Dynamic Application Containment threshold must be set to <b>Most Likely Malicious</b> or higher.</p> <p>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.</p>

**Table 6-3 Options** (continued)

Section	Option	Definition
	<b>Block when reputation threshold reaches</b>	<p>Blocks files when the file reputation reaches a specific threshold, and specifies the threshold:</p> <ul style="list-style-type: none"> <li>• <b>Might Be Trusted</b></li> <li>• <b>Unknown</b> (Default for the <b>Security</b> rule group)</li> <li>• <b>Might Be Malicious</b> (Default for the <b>Balanced</b> rule group)</li> <li>• <b>Most Likely Malicious</b> (Default for the <b>Productivity</b> rule group)</li> <li>• <b>Known Malicious</b></li> </ul> <p>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 <b>Might be Trusted</b>.</p>
	<b>Clean when reputation threshold reaches</b>	<p>Cleans files when the file reputation reaches a specific threshold, and specifies the threshold:</p> <ul style="list-style-type: none"> <li>• <b>Unknown</b></li> <li>• <b>Might Be Malicious</b></li> <li>• <b>Most Likely Malicious</b></li> <li>• <b>Known Malicious</b> (Default for the <b>Balanced</b> and <b>Security</b> rule groups)</li> </ul> <p>The default for the <b>Productivity</b> rule group is deselected.</p> <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <b>Best practice:</b> Use this option with <b>Known Malicious</b> file reputations because a file might be removed when cleaned.         </div>

**Table 6-4 Advanced options**

Section	Option	Description
Threat Detection User Messaging	<b>Display threat notifications to the user</b>	Displays threat notifications to the user.
	<b>Notify the user when reputation threshold reaches</b>	<p>Notifies the user when the file reputation reaches a specified threshold:</p> <ul style="list-style-type: none"> <li>• <b>Most Likely Trusted</b></li> <li>• <b>Might Be Trusted</b> (Default for the <b>Security</b> rule group)</li> <li>• <b>Unknown</b> (Default for the <b>Balanced</b> rule group)</li> <li>• <b>Might Be Malicious</b> (Default for the <b>Productivity</b> rule group)</li> <li>• <b>Most Likely Malicious</b></li> <li>• <b>Known Malicious</b></li> </ul> <p>The prompt level can't conflict with the clean or block settings. For example, if you block unknown files, you can't set this field to <b>Might Be Trusted</b> because it is a higher threshold than <b>Unknown</b>.</p>
	<b>Default action</b>	<p>Specifies the action to take if the user doesn't respond to the prompt:</p> <ul style="list-style-type: none"> <li>• <b>Allow</b></li> <li>• <b>Block</b></li> </ul>

**Table 6-4 Advanced options** *(continued)*

Section	Option	Description
	<b>Specify length (minutes) of timeout</b>	Specifies the number of minutes to display the prompt before performing the default action. The default is 5 minutes.
	<b>Message</b>	Specifies the message that the user sees when a file, which meets the prompting criteria, tries to run.
	<b>Disable threat notifications if the Threat Intelligence Exchange server is not reachable</b>	Disables prompts when the TIE server is unreachable so that users don't receive prompts about files whose reputations are unavailable.
<b>Advanced Threat Defense</b>	<b>Send files not yet verified to McAfee Advanced Threat Defense for analysis</b>	Sends executable files to McAfee Advanced Threat Defense for analysis. When enabled, Threat Intelligence sends files securely over HTTPS using port 443 to Advanced Threat Defense when: <ul style="list-style-type: none"> <li>• The TIE server doesn't have Advanced Threat Defense information about the file.</li> <li>• The file is at or below the specified reputation level.</li> <li>• The file is at or below the specified file size limit.</li> </ul> Specify information for the Advanced Threat Defense server in the management policy for the TIE server.
	<b>Submit files when reputation threshold reaches</b>	Submits files to Advanced Threat Defense when the file reputation reaches a specified threshold: <ul style="list-style-type: none"> <li>• <b>Most Likely Trusted</b></li> <li>• <b>Unknown</b></li> <li>• <b>Most Likely Malicious</b></li> </ul> The default for all rule groups is <b>Unknown</b> .
	<b>Limit size (MB) to</b>	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 Threat Intelligence options on page 169*

*Enable the Dynamic Application Containment trigger threshold on page 165*

*Blocking or allowing files and certificates on page 169*





# Index

## A

- About page [10](#), [22](#)
- access modes, Endpoint Security Client [15](#)
- Access Protection
  - about [64](#)
  - examples [65](#)
  - excluding processes [63](#)
  - log files [25](#)
  - McAfee-defined rules, about [67](#)
  - McAfee-defined rules, configuring [66](#)
  - processes, including and excluding [66](#), [72](#)
  - rules, about [65](#)
  - user-defined rules, configuring [70](#)
- Action menu, about [14](#)
- actions, Threat Prevention
  - enabling users to clean and delete infected files [77](#), [81](#)
  - performing on quarantined items [59](#)
  - specifying what happens when threat is found [77](#), [81](#)
  - unwanted programs [75](#)
- activity logs, Endpoint Security Client [25](#)
- Adaptive mode
  - configuring in Firewall [117](#)
  - rule precedence [121](#)
- Adaptive rules group, Firewall [126](#)
- Admin added rules group, Firewall [126](#)
- Administrator Log On page
  - unlocking the client interface [27](#)
  - when opening Endpoint Security Client [19](#)
- administrators
  - defined [10](#)
  - logging on to Endpoint Security Client [27](#)
  - password [27](#)
- Advanced Threat Defense [161](#)
  - sending files to [169](#)
  - used in determining reputations [158](#)
- adware, about [61](#)
- alerts, Firewall [13](#)
- alerts, Threat Prevention
  - on-access scan overview [77](#)
  - on-demand scan overview [82](#)
- AMCore content files
  - about [10](#)
  - about signatures and updates [11](#)
  - changing version [28](#)

- AMCore content files (*continued*)
  - Extra.DAT files [29](#), [30](#)
  - on-access scan overview [77](#)
  - on-demand scan overview [82](#)
- applications, about [120](#)
- applications, contained
  - allowing to run normally [165](#)
  - managing on the Endpoint Security Client [168](#)
- apps, Windows Store [77](#), [82](#)
- archives, specifying scan options [77](#), [81](#)
- Ask search engine, and safety icons [143](#)
- attacks, buffer overflow exploits [72](#)

## B

- backups, specifying scan options [77](#), [81](#)
- balloons, Web Control [143](#), [147](#)
- best practices
  - using trusted networks [120](#)
- Bing search engine, and safety icons [143](#)
- boot sectors, scanning [77](#), [81](#)
- browsers
  - disabling Web Control plug-in [147](#)
  - enabling the plug-in [145](#)
  - supported [141](#), [146](#)
  - viewing information about a site [146](#)
- buffer overflow exploits, about [72](#)
- buttons
  - Scan Now [56](#)
  - View Detections [59](#)
  - View Scan [56](#)
- buttons, Web Control [142](#)

## C

- cache, global scan
  - on-access scans [77](#)
  - on-demand scans [82](#)
- certificates
  - how reputations are determined [158](#)
- Chrome
  - enabling the plug-in [145](#)
  - supported browsers [141](#), [146](#)
  - viewing information about a site [146](#)
  - Web Control buttons [142](#)

- client, *See* Endpoint Security Client
- Client Interface Mode, options [15](#)
- client logging, configuring [31](#)
- client software, defined [10](#)
- colors, Web Control buttons [142](#)
- Common module, configuring
  - client interface security [32](#)
  - logging [31](#)
  - McAfee GTI proxy server settings [33](#)
  - Self Protection [31](#)
  - settings [30](#)
  - source sites for client updates [34](#)
  - source sites for client updates, configuring [34](#)
  - update settings [34, 36](#)
- Common module, Endpoint Security Client [9, 16](#)
- configuration, bridging TIE servers [158](#)
- Contained Application List, managing [168](#)
- contained applications, Dynamic Application Containment
  - managing on the Endpoint Security Client [168](#)
- containment rules
  - Dynamic Application Containment [162](#)
- Content Actions settings
  - Web Control [151](#)
- Content Actions settings, Web Control [150](#)
- content categories, *See* web categories
- content files
  - about [10](#)
  - and detections [20](#)
  - changing AMCore version [28](#)
  - checking for updates manually [12, 23](#)
  - Extra.DAT files [29, 30](#)
  - on-access scan overview [77](#)
  - on-demand scan overview [82](#)
  - scheduling updates from client [37](#)
- content updates [11](#)
- content, updating from the client [23](#)
- CPU time, on-demand scans [85](#)
- credentials, repository list [35](#)
- custom rules, *See* user-defined rules, Access Protection
- custom scans, *See* on-demand scans
- custom update tasks, *See* tasks, Endpoint Security Client

## D

- Data Exchange Layer
  - about [158](#)
- debug logs, Endpoint Security Client [25](#)
- Default Client Update task
  - about [37](#)
  - configuring [36](#)
  - configuring source sites for updates [34](#)
  - scheduling with Endpoint Security Client [37](#)
- Default rules group, Firewall [126](#)
- defining networks [119](#)
- Desktop mode, Windows 8 and 10
  - notification messages [13](#)

- Desktop mode, Windows 8 and 10 (*continued*)
  - responding to threat detection prompts [20](#)
- detection definition files, *See* content files
- detections
  - displaying messages to users [77, 81](#)
  - excluding by name [76](#)
  - managing [56, 59](#)
  - names [61](#)
  - reporting to management server [10](#)
  - responding to [20](#)
  - types [56, 58](#)
- dialers, about [61](#)
- DNS traffic, blocking [118](#)
- domains, blocking [118](#)
- download requests, *See* file downloads
- downloads
  - block and warn behavior [142](#)
- Dynamic Application Containment
  - about [162](#)
  - allowing contained applications to run normally [165](#)
  - enabling the trigger threshold [165](#)
  - log files [25](#)
  - managing contained applications [168](#)
  - McAfee-defined rules, about [166](#)
  - McAfee-defined rules, configuring [166](#)
  - processes, including and excluding [168](#)
  - Threat Intelligence [155](#)
- Dynamic rules group, Firewall [126](#)

## E

- Endpoint Security Client
  - about [14](#)
  - configuring security settings [32](#)
  - configuring source sites for updates [34](#)
  - custom update tasks, creating [37](#)
  - Default Client Update task, about [37](#)
  - Default Client Update task, configuring [36](#)
  - Default Client Update task, scheduling [37](#)
  - displaying help [20](#)
  - displaying protection information [22](#)
  - Full Scan and Quick Scan, scheduling [85](#)
  - interacting with [11](#)
  - logging on as administrator [27](#)
  - logs, about [25](#)
  - management types [10, 22](#)
  - managing threat detections [59](#)
  - mirror tasks, about [39](#)
  - mirror tasks, configuring and scheduling [38](#)
  - modules [16](#)
  - opening [12, 19](#)
  - policy settings [15](#)
  - protecting with a password [33](#)
  - running scans [56](#)
  - scanning for malware [55](#)
  - system scans [55](#)

- Endpoint Security Client (*continued*)
    - Threat Summary [15](#)
    - unlocking the interface [27](#)
    - updating protection [23](#)
    - viewing the Event Log [24](#)
  - Endpoint Security, how it protects your computer [10](#)
  - Endpoint Security, managing [27](#)
  - error logs, Endpoint Security Client [25](#)
  - error messages, system tray icon states [12](#)
  - event logs, Endpoint Security Client
    - about [25](#)
    - update failures [23](#)
    - viewing Event Log page [24](#)
  - events, tracking Web Control browser events [147](#)
  - exceptions
    - McAfee GTI [120](#)
  - exclusions
    - Access Protection, policy-based and rule-based [72](#)
    - configuring [63](#)
    - detection name [76](#)
    - Dynamic Application Containment [168](#)
    - on-access scan, specifying files, folders, and drives [77](#)
    - on-demand scan, specifying [81](#)
    - root-level [64](#)
    - specifying URLs for ScriptScan [77](#)
    - using wildcards [64](#)
  - executables
    - configuring trusted [120](#)
    - trusted, *See* trusted executables
  - Exploit Prevention
    - about [72](#)
    - and Host IPS [72](#)
    - configuring [73](#)
    - content file updates [11](#)
    - excluding processes [63](#)
    - log files [25](#)
  - exploits
    - blocking buffer overflows [72](#), [73](#)
    - how buffer overflow exploits occur [72](#)
  - Extra.DAT files
    - about [29](#)
    - AMCore content files [11](#)
    - downloading [30](#)
    - loading [30](#)
    - on-access scan overview [77](#)
    - on-demand scan overview [82](#)
    - using [29](#)
- F**
- failures, update [23](#)
  - false positives
    - Firewall, reducing [120](#)
  - features
    - enabling and disabling [28](#)
  - features (*continued*)
    - Endpoint Security Client access based on policies [15](#)
  - file downloads
    - blocking from unknown sites [147](#)
    - blocking or warning based on ratings [150](#)
    - scanning with Threat Prevention [149](#)
  - file reputation
    - responding to prompts [21](#)
  - files
    - configuring for quarantine [76](#)
    - configuring log files [31](#)
    - Endpoint Security Client logs [24](#)
    - excluding specific types from scans [63](#)
    - how reputations are determined [158](#)
    - log files [25](#)
    - managing in the Quarantine [59](#)
    - preventing from modification [31](#)
    - rescanning in the Quarantine [62](#)
    - running scans [58](#)
    - wildcards in exclusions [64](#)
  - files and certificates, blocking [169](#)
  - files and certificates, sending [169](#)
  - files, content
    - changing AMCore content version [28](#)
    - Exploit Prevention [11](#)
    - Extra.DAT and AMCore [11](#)
    - Extra.DAT files [29](#), [30](#)
    - loading Extra.DAT files [30](#)
    - on-access scan overview [77](#)
    - on-demand scan overview [82](#)
    - signatures and updates [11](#)
    - Threat Intelligence [11](#)
    - using Extra.DAT files [29](#)
  - Firefox
    - enabling the plug-in [145](#)
    - supported browsers [141](#), [146](#)
    - viewing information about a site [146](#)
    - Web Control buttons [142](#)
  - firewall
    - about timed groups [12](#)
    - enabling from McAfee system tray icon [12](#)
  - Firewall
    - about [9](#)
    - activity log [25](#)
    - blocking DNS traffic [118](#)
    - creating timed groups [129](#)
    - debug log [25](#)
    - enabling and disabling from the system tray icon [115](#)
    - enabling and disabling protection [117](#)
    - enabling and viewing timed groups [116](#)
    - Endpoint Security Client [16](#)
    - how firewall rules work [121](#)
    - how it works [115](#)
    - intrusion alerts [13](#)
    - location-aware groups, about [122](#)

Firewall (*continued*)

- location-aware groups, creating [128](#)
- log files [25](#)
- managing [116](#)
- managing rules and groups [126](#)
- modifying options [117](#)
- rules, *See* firewall rules
- timed groups, about [116](#)
- trusted executables [120](#)
- updating content from the client [23](#)
- firewall groups, *See* firewall rule groups
- firewall options
  - modifying [117](#)
- firewall rule groups
  - and connection isolation [124](#)
  - configuring [121](#)
  - creating timed groups [129](#)
  - how the Firewall works [115](#)
  - location-aware, about [122](#)
  - location-aware, creating [128](#)
  - managing timed groups from the system tray icon [12](#), [116](#)
  - precedence [122](#)
  - predefined [126](#)
  - timed groups, about [116](#)
- firewall rules
  - allow and block [121](#)
  - configuring [121](#)
  - how the Firewall works [115](#)
  - how they work [121](#)
  - ordering and precedence [121](#)
  - using wildcards [128](#)
- Firewall settings
  - Options [120](#)
- folders
  - configuring for quarantine [76](#)
  - managing in the Quarantine [59](#)
  - rescanning in the Quarantine [62](#)
  - running scans [58](#)
  - wildcards in exclusions [64](#)
- frequently asked questions, McAfee GTI [118](#)
- Full access mode
  - modifying firewall options [117](#)
  - policy settings [15](#)
- Full Scan
  - about [55](#)
  - configuring [81](#)
  - running from Endpoint Security Client [56](#)
  - scheduling on the client [85](#)

**G**

- GBOP signatures, *See* Generic Buffer Overflow Protection signatures
- Generic Buffer Overflow Protection signatures [11](#)
- Generic Privilege Escalation Prevention signatures [11](#)
- getting started with Threat Intelligence [160](#)

- global scan cache
  - on-access scans [77](#)
  - on-demand scans [82](#)
- Google
  - Chrome [141](#)
  - safety icons [143](#)
  - supported search engines [143](#)
- GPEP signatures, *See* Generic Privilege Escalation Prevention signatures
- groups, firewall, *See* firewall rule groups

**H**

- hashes, about [33](#), [76](#), [149](#)
- heap-based attacks, buffer overflow exploits [72](#)
- Help, displaying [14](#), [20](#)
- high-risk processes, specifying [77](#)
- Host Intrusion Prevention, and Exploit Prevention [72](#)
- Host IPS, and Exploit Prevention [72](#)

**I**

- icons, McAfee, *See* system tray icon, McAfee
- icons, Web Control [143](#)
- incremental scans [83](#)
- information, displaying protection [22](#)
- installers, scanning trusted [77](#)
- interface modes
  - configuring client security settings [32](#)
  - Standard access [27](#), [33](#)
- Internet Explorer
  - and ScriptScan behavior [79](#)
  - displaying Endpoint Security help [20](#)
  - enabling the plug-in [145](#)
  - supported browsers [141](#), [146](#)
  - viewing information about a site [146](#)
- intrusions, enabling Firewall alerts [117](#)
- IP addresses [119](#)
  - location-aware groups [122](#)
  - rule groups [122](#)
  - trusted [120](#)

**J**

- jokes, about [61](#)

**K**

- keyloggers, about [61](#)

**L**

- location-aware groups
  - about [122](#)
  - connection isolation [124](#)
  - creating [128](#)
- Lock client interface mode
  - and policy settings [15](#)
  - unlocking the interface [27](#)

Lock client interface mode (*continued*)  
 when opening Endpoint Security Client [19](#)

log files  
 configuring [31](#)  
 locations [25](#)  
 update failures [23](#)  
 viewing [24](#)

low-risk processes, specifying [77](#)

## M

malware  
 detections while scanning [56, 58](#)  
 responding to detections [20](#)  
 scanning for [55](#)

management types  
 about [22](#)  
 displaying [22](#)

manual scans  
 about scan types [55](#)  
 running from Endpoint Security Client [56, 58](#)

manual updates, running [23](#)

McAfee Agent  
 Product Update task and repository list [35](#)

McAfee client, *See* Endpoint Security Client

McAfee core networking rules group, Firewall [126](#)

McAfee Endpoint Security Client, *See* Endpoint Security Client

McAfee ePO  
 and management types [22](#)  
 retrieving AMCore content files [11](#)  
 updating protection [10](#)

McAfee ePO Cloud management type [22](#)

McAfee GTI  
 and web categories [151](#)  
 configuring sensitivity level [76](#)  
 exceptions [120](#)  
 firewall options, configuring [117](#)  
 frequently asked questions [118](#)  
 network reputation for firewall, configuring [117](#)  
 on-access scans, configuring [77](#)  
 on-access scans, how they work [77](#)  
 on-demand scans, configuring [81](#)  
 on-demand scans, how they work [82](#)  
 overview [33, 76, 149](#)  
 scanning files before downloading [147, 149](#)  
 sending block events to server [117](#)  
 specifying proxy server settings [33](#)  
 telemetry feedback [76](#)  
 Web Control communication error [142](#)  
 Web Control safety ratings [144](#)  
 Web Control site reports [144](#)

McAfee icon, *See* system tray icon, McAfee

McAfee Labs  
 AMCore content file updates [11](#)  
 and McAfee GTI [33, 76, 149](#)  
 downloading Extra.DAT [29](#)

McAfee Labs (*continued*)

Extra.DAT [30](#)  
 getting more information about threats [59](#)

McAfee protection client, *See* Endpoint Security Client

McAfee SECURE, Web Control button [142](#)

McAfee Security Status page, displaying [12](#)

McAfee-defined rules, Access Protection [67](#)

McAfee-defined rules, Dynamic Application Containment [166](#)

McTray, starting [83](#)

menus

About [22](#)  
 Action [14, 28](#)  
 Help [14, 20](#)  
 Settings [14–16, 117, 126](#)  
 Web Control [146](#)

messages, Endpoint Security

about [13](#)  
 displaying when threat detected [77, 81](#)

Microsoft Internet Explorer, *See* Internet Explorer

mirror tasks

about [39](#)  
 configuring and scheduling [38](#)

modules

about Endpoint Security [9](#)  
 displaying information about [22](#)  
 Endpoint Security Client access based on policies [15](#)  
 installed in Endpoint Security Client [16](#)

modules, Common

client interface security, configuring [32](#)  
 configuring source sites for client updates [34](#)  
 how McAfee GTI works [33, 76, 149](#)  
 logging, configuring [31](#)  
 McAfee GTI proxy server settings, configuring [33](#)  
 Self Protection, configuring [31](#)  
 source sites for client updates, configuring [34](#)  
 update settings, configuring [34, 36](#)

Mozilla Firefox, *See* Firefox

## N

network adapters, allowing connection [122](#)

network drives, specifying scan options [77](#)

networks

defining [119](#)  
 trusted [120](#)

notification messages

about [13](#)  
 interacting with Endpoint Security Client [11](#)  
 Windows 8 and 10 [13](#)

## O

On-Access Scan page [59](#)

on-access scans

about [55](#)  
 configuring [76, 77](#)

- on-access scans (*continued*)
    - excluding items [63](#)
    - log files [25](#)
    - number of scanning policies [81](#)
    - optimizing with trust logic [77](#)
    - overview [77](#)
    - potentially unwanted programs, enabling detection [75](#)
    - scanning scripts [79](#)
    - ScriptScan [79](#)
    - threat detections [20](#)
    - writing to vs. reading from disk [77](#)
  - on-demand scans
    - about [55](#)
    - configuring [76](#)
    - excluding items [63](#)
    - log files [25](#)
    - overview [82](#)
    - potentially unwanted programs, enabling detection [75](#)
    - Remote Storage scans [85](#)
    - responding to prompts [21](#)
    - running Full Scan or Quick Scan [56](#)
    - running Right-Click Scan [58](#)
    - scanning files or folders [58](#)
    - system utilization [85](#)
  - on-demand updates, *See* manual updates, running
  - options
    - configuring on-access scans [77](#)
    - configuring on-demand scans [81](#)
    - scanning for malware [55](#)
  - Options, Common
    - client interface security, configuring [32](#)
    - configuring [30](#)
    - logging settings, configuring [31](#)
    - proxy server settings, configuring [33](#)
    - scheduling on-demand scans [55](#)
    - Self Protection, configuring [31](#)
    - source sites for client updates, configuring [34](#)
    - update settings, configuring [34](#), [36](#)
  - Options, Firewall
    - defined networks [119](#)
    - trusted executables [120](#)
  - Options, Threat Prevention
    - common scan settings [76](#)
    - unwanted programs [74](#)
- P**
- pages
    - About [10](#), [22](#)
    - Event Log [24](#)
    - McAfee Security Status [12](#)
    - On-Access Scan [20](#), [59](#)
    - Quarantine [59](#)
    - Roll Back AMCore Content [28](#)
    - Scan for threats [58](#)
  - pages (*continued*)
    - Scan System [56](#), [59](#)
    - scan, displaying [56](#)
    - Settings [15](#), [31–34](#), [36](#), [81](#), [117](#)
    - Update [23](#)
  - password crackers, about [61](#)
  - passwords
    - administrator [27](#)
    - configuring client security [32](#)
    - controlling access to client [33](#)
  - phishing, reports submitted by site users [144](#)
  - plug-ins, enabling Web Control in the browser [145](#)
  - policies
    - accessing Endpoint Security Client [15](#)
    - client features [11](#)
    - defined [10](#)
  - policies, Common
    - configuring [30](#)
  - policies, Threat Prevention
    - common scan settings [76](#)
    - on-access scans [81](#)
    - on-demand scans, deferring [83](#)
  - pop-ups, and safety ratings [144](#)
  - potentially unwanted programs
    - about [61](#)
    - configuring detection [74](#)
    - detections while scanning [56](#), [58](#)
    - enabling detection [75](#), [77](#), [81](#)
    - excluding items [63](#)
    - specifying [74](#)
    - specifying programs to detect [76](#)
    - wildcards in exclusions [64](#)
  - precedence
    - firewall groups [122](#)
    - firewall rules [121](#)
  - predefined firewall rule groups [126](#)
  - priorities, on-access scans [85](#)
  - private network, adding external sites [147](#)
  - process settings, on-demand scans [85](#)
  - processes, Access Protection
    - policy-based exclusion [72](#)
    - rule-based exclusion [72](#)
  - processes, Dynamic Application Containment
    - exclusions [168](#)
  - processes, Threat Intelligence
    - including and excluding in Dynamic Application Containment [168](#)
  - processes, Threat Prevention
    - excluding [63](#)
    - including and excluding in access protection [72](#)
    - including and excluding in Access Protection [66](#)
    - scanning [77](#)
    - specifying high- and low-risk [77](#)
  - Product Improvement Program [161](#)

- Product Update client tasks
  - about [35](#)
  - repository list [35](#)
- product updates
  - checking for manually [12, 23](#)
  - scheduling from client [37](#)
- programs, enabling detection of potentially unwanted [77, 81](#)
- prompts, Endpoint Security
  - about [13](#)
  - responding to file reputation [21](#)
  - responding to scan [21](#)
  - Windows 8 and 10 [20](#)
- protection
  - configuring Self Protection [31](#)
  - displaying information about [22](#)
  - interacting with [11](#)
  - keeping up to date [10](#)
- proxy server
  - configuring for McAfee GTI [33](#)
  - how McAfee GTI works [33, 76, 149](#)
  - settings in repository list [35](#)

## Q

- Quarantine page [59](#)
- Quarantine, Threat Prevention
  - configuring location and retention settings [76](#)
  - rescanning quarantined items [62](#)
- Quick Scan
  - configuring [81](#)
  - running from Endpoint Security Client [56](#)
  - scheduling on the client [85](#)
  - types of scans [55](#)

## R

- ransomware
  - creating Access Protection rules to protect against [70](#)
- ratings, safety, *See* safety ratings
- ratings, Web Control, *See* safety ratings
- remote admin tools, about [61](#)
- Remote Desktop, and scan on idle feature [83](#)
- Remote Storage scans, overview [85](#)
- reports, Web Control [144](#)
  - displaying [147](#)
  - safety [141](#)
  - viewing [146](#)
  - website safety [144](#)
- repository list
  - location on client [35](#)
  - order preference, repository list [35](#)
  - overview [35](#)
- reputations
  - Dynamic Application Containment [162](#)
  - enabling the Dynamic Application Containment trigger threshold [165](#)

- reputations (*continued*)
  - how they are determined [158](#)
- responses, configuring for unwanted program detection [75](#)
- resumable scans, *See* incremental scans
- Right-Click Scan
  - about [55](#)
  - configuring [81](#)
  - running from Windows Explorer [58](#)
- Roll Back AMCore Content page [28](#)
- root-level exclusions, *See* exclusions
- rule groups, Firewall, *See* firewall rule groups
- rules, Access Protection
  - types [65](#)
- rules, Dynamic Application Containment
  - configuring [166](#)
- rules, firewall, *See* Firewall
- rules, Threat Prevention
  - configuring [66](#)
  - how Access Protection works [65](#)

## S

- Safari (Macintosh)
  - Web Control buttons [142](#)
- safety ratings
  - configuring actions for sites and downloads [150](#)
  - controlling access to sites [151](#)
  - how website ratings are derived [144](#)
  - safety icons [143](#)
  - Web Control and [141](#)
- safety reports, *See* reports, Web Control
- scan avoidance [77](#)
- scan cache
  - on-access scans [77](#)
  - on-demand scans [82](#)
- scan deferral, overview [83](#)
- scan engines, AMCore content file overview [11](#)
- Scan for threats page [58](#)
- Scan Now button [56](#)
- scan on idle feature [21, 83](#)
- scan page, displaying [20, 56](#)
- Scan System page [56, 59](#)
- scans
  - common settings for on-access and on-demand scans [76](#)
  - custom, creating and scheduling on the client [85](#)
  - deferring, pausing, resuming, and canceling [21](#)
  - responding to prompts [21](#)
  - running from Endpoint Security Client [56](#)
  - running Right-Click Scan [58](#)
  - scheduling with Endpoint Security Client [85](#)
  - types [55](#)
  - using wildcards in exclusions [64](#)
  - Web Control [149](#)
- scans, custom, *See* scans, on-demand

- scans, on-access
  - configuring [77](#)
  - detecting threats in Windows Store apps [77](#)
  - excluding items [63](#)
  - number of policies [81](#)
  - optimizing with trust logic [77](#)
  - overview [77](#)
  - ScriptScan [79](#)
  - threat detections, responding to [20](#)
- scans, on-demand
  - configuring [81](#)
  - detecting threats in Windows Store apps [82](#)
  - excluding items [63](#)
  - Remote Storage scans [85](#)
  - scheduling on the client [85](#)
  - system utilization [85](#)
- schedules, on-demand scans, deferring [83](#)
- scripts, scanning [79](#)
- ScriptScan
  - about [79](#)
  - enabling [77](#)
  - excluding URLs [63](#)
- searches
  - blocking risky sites from results [147](#)
  - safety icons [143](#)
- Secure Search, configuring Web Control [147](#)
- security
  - configuring client interface security [32](#)
- security levels
  - examples [169](#)
- Self Protection, configuring [31](#)
- self-managed, about [22](#)
- sensitivity level, McAfee GTI [33](#), [76](#), [149](#)
- server systems, and scan on idle feature [83](#)
- servers
  - about TIE servers [158](#)
  - bridging TIE servers managed by McAfee ePO [158](#)
- servers, proxy, *See* proxy servers
- settings
  - source sites for client updates, configuring [34](#)
  - source sites, configuring for [34](#)
  - updates, configuring for [34](#), [36](#)
- Settings page
  - and Client Interface Mode [15](#)
  - client interface security, configuring [32](#)
  - logging, configuring [31](#)
  - managing firewall rules and groups [126](#)
  - modifying firewall options [117](#)
  - on-access scan settings, configuring [77](#)
  - on-demand scan settings, configuring [81](#)
  - proxy server settings, configuring [33](#)
  - Self Protection, configuring [31](#)
  - update settings, configuring [34](#), [36](#)
- settings, Firewall
  - Options [120](#)
- settings, Threat Intelligence
  - Dynamic Application Containment technology [166](#)
- settings, Threat Prevention
  - Access Protection feature [66](#)
  - configuring potentially unwanted programs [74](#)
  - on-access scans [75](#)
  - on-demand scans [75](#)
- settings, Web Control
  - controlling access to websites [150](#)
  - controlling access with safety ratings [151](#)
  - controlling access with web categories [151](#)
- signatures
  - known threat information [11](#)
- site reports, *See* reports, Web Control
- sites
  - block and warn behavior [142](#)
  - browsing protection [142](#)
  - protection while searching [143](#)
  - safety ratings [144](#)
  - viewing Web Control site reports [146](#)
- sites, blocking
  - based on ratings [150](#)
  - based on safety ratings [151](#)
  - based on web category [150](#), [151](#)
- sites, controlling access
  - with safety ratings [151](#)
  - with web categories [150](#), [151](#)
- sites, warning
  - based on ratings [150](#)
  - based on safety ratings [151](#)
- software updates
  - checking for manually [12](#), [23](#)
  - scheduling from client [37](#)
- spyware, about [61](#)
- stack-based attacks, buffer overflow exploits [72](#)
- standalone, *See* self-managed, about
- Standard access mode
  - and policy settings [15](#)
  - configuring client security settings [32](#)
  - effects of setting a password [33](#)
  - logging on as administrator [27](#)
  - managing firewall rules and groups [126](#)
- Start menu, opening Endpoint Security Client [19](#)
- Status page, viewing Threat Summary [15](#)
- status, Endpoint Security, displaying with McAfee system tray icon [12](#)
- stealth, about [61](#)
- submit files for further analysis
  - Advanced Threat Defense [161](#)
  - Product Improvement Program [161](#)
- subrules, Access Protection
  - evaluating with targets [71](#)
  - excluding and including [72](#)
- system scans, types [55](#)



- system tray icon, McAfee [11](#), [12](#), [32](#)
  - configuring access to Endpoint Security [32](#)
  - defined [12](#)
  - enabling and disabling Firewall [115](#)
  - enabling and viewing timed groups [116](#)
  - Firewall timed groups [12](#)
  - opening Endpoint Security Client [19](#)
  - updating security [12](#)
- system utilization options, overview [85](#)

## T

- Targeted API Monitoring signatures [11](#)
- targets, Access Protection
  - evaluating with subrules [71](#)
  - examples [71](#)
- tasks, Endpoint Security
  - Default Client Update, about [37](#)
- tasks, Endpoint Security Client
  - configuring and scheduling mirror tasks [38](#)
  - custom update, configuring and scheduling [37](#)
  - Default Client Update, configuring [36](#)
  - Default Client Update, scheduling [37](#)
  - mirror tasks, about [39](#)
- tasks, Threat Prevention
  - custom scans, scheduling [85](#)
  - Full and Quick Scans, about [55](#)
  - Full Scan and Quick Scan, scheduling [85](#)
- threads, priority [85](#)
- Threat Intelligence
  - about [156](#)
  - activity log [25](#)
  - bridging TIE servers managed by McAfee ePO [158](#)
  - components [156](#)
  - configuring [169](#)
  - configuring Dynamic Application Containment trigger threshold [165](#)
  - content file updates [11](#)
  - debug log [25](#)
  - Dynamic Application Containment technology [166](#)
  - Endpoint Security [157](#)
  - Endpoint Security Client [16](#)
  - log files [25](#)
  - managing [156](#)
  - scenarios [155](#)
  - workflow examples [160](#)
- Threat Intelligence Exchange server, *See* TIE servers
- Threat Prevention
  - about [9](#)
  - Access Protection feature [66](#)
  - Endpoint Security Client [16](#)
  - Exploit Prevention feature [73](#)
  - managing [62](#)
  - on-access scans, about [77](#)
  - on-access scans, configuring [77](#)
  - on-demand scans, about [82](#)

- Threat Prevention (*continued*)
  - on-demand scans, configuring [81](#)
  - Options, unwanted programs [74](#)
  - potentially unwanted programs, detecting [74](#)
  - scanning files before downloading [147](#), [149](#)
- Threat Summary, about [15](#)
- threats
  - access point violations [65](#)
  - Access Protection process [65](#)
  - AMCore content files [11](#)
  - and safety ratings [144](#)
  - detections while scanning [58](#)
  - getting more information from McAfee Labs [59](#)
  - managing detections [59](#)
  - Quarantine folder [59](#)
  - rescanning quarantined items [62](#)
  - responding to detections [20](#)
  - types [61](#)
  - Windows Store apps [77](#), [82](#)
- thresholds
  - enabling the Dynamic Application Containment trigger threshold [165](#)
- throttling, configuring [85](#)
- TIE servers
  - about [158](#)
  - bridging [158](#)
- timed groups
  - managing from McAfee system tray icon [12](#)
- timed groups, Firewall
  - about [116](#)
  - creating [129](#)
  - managing from the system tray icon [116](#)
- toast notifications, Windows 8 and 10 [13](#), [20](#)
- traffic
  - allowing outgoing until firewall services start [117](#)
  - scanned by Firewall [115](#)
- trojans
  - about [61](#)
  - detections while scanning [56](#), [58](#)
- trust logic, optimizing on-access scans [77](#)
- trusted executables
  - configuring [120](#)
  - defining [120](#)
- trusted installers, scanning [77](#)
- trusted networks, *See* networks

## U

- unmanaged, *See* self-managed, about
- Update page [23](#)
- updates
  - canceling [23](#)
  - Update Now button, Endpoint Security Client [23](#)
  - Update Security option [12](#)
- updates, Endpoint Security
  - configuring and scheduling from client [37](#)

- updates, Endpoint Security (*continued*)
  - configuring behavior [34](#)
  - configuring source sites for updates [34](#)
  - Default Client Update task, about [37](#)
  - Default Client Update, configuring [36](#)
- updates, Firewall
  - checking for manually [23](#)
- updates, Threat Prevention
  - checking for manually [12](#), [23](#)
  - content files [10](#)
  - Extra.DAT files [30](#)
  - overview [11](#)
- upgrades, client software components [10](#)
- URLs
  - excluding from script scanning [63](#), [77](#)
- user accounts, controlling access to client [33](#)
- User added rules group, Firewall [126](#)
- user-defined rules, Access Protection
  - configuring [70](#)

## V

- View Detections button [59](#)
- View Scan button [56](#)
- viruses
  - about [61](#)
  - detections while scanning [56](#), [58](#)
  - responding to detections [20](#)
  - signatures [11](#)
- vulnerabilities, *See* threats

## W

- web categories, blocking or warning based on [150](#), [151](#)
- Web Control
  - about [9](#)
  - activity log [25](#)
  - and blocked sites [142](#)
  - and warned sites [142](#)
  - balloons and icons [147](#)
  - buttons, description [142](#)
  - configuring [147](#)
  - debug log [25](#)
  - enabling [147](#)
  - enabling the plug-in [145](#)
  - Endpoint Security Client [16](#)
  - features [141](#)
  - how file downloads are scanned [149](#)
  - icons, description [143](#)
  - log files [25](#)
  - managing [147](#)

- Web Control (*continued*)
  - menu [142](#)
  - search engines and safety icons [143](#)
  - site reports [144](#)
  - viewing information about a site [146](#)
  - viewing site reports [146](#)
- websites
  - browsing protection [142](#)
  - protection while searching [143](#)
  - safety ratings [144](#)
  - viewing Web Control site reports [146](#)
- websites, blocking
  - based on ratings [150](#)
  - based on safety ratings [151](#)
  - based on web category [150](#), [151](#)
  - risky sites from search results [147](#)
  - unrated or unknown [147](#)
- websites, controlling access
  - with safety ratings [151](#)
  - with web categories [150](#), [151](#)
- websites, warning
  - based on ratings [150](#)
  - based on safety ratings [151](#)
- wildcards
  - in exclusions [64](#)
  - in root-level exclusions [64](#)
  - using in exclusions [64](#)
  - using in firewall rules [128](#)
- Windows 8 and 10
  - about notification messages [13](#)
  - opening Endpoint Security Client [19](#)
  - responding to threat detection prompts [20](#)
- Windows Set Priority setting [85](#)
- Windows Store apps, detecting threats [77](#), [82](#)
- workflow examples [160](#)
  - build file prevalence and observe [160](#)
  - monitoring and adjusting [160](#)
  - submit files for further analysis [161](#)

## Y

- Yahoo
  - default search engine [147](#)
  - safety icons [143](#)
  - supported search engine [143](#)

## Z

- zero-impact scans [83](#)

