COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

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

**McAfee Endpoint Security**

1. **Introduction**
   - Endpoint Security modules .................................................. 7
   - How Endpoint Security protects your computer .......................... 8
     - How your protection stays up to date .................................. 8
   - Interacting with Endpoint Security ........................................ 9
     - About the McAfee system tray icon .................................... 10
     - About notification messages ............................................. 10
     - About the Endpoint Security Client .................................... 11

2. **Using the Endpoint Security Client**
   - Open the Endpoint Security Client ....................................... 15
   - Get help .............................................................................. 16
   - Respond to prompts ................................................................ 16
     - Respond to a threat-detection prompt .................................. 16
     - Respond to a scan prompt .................................................. 16
   - Get information about your protection ................................... 17
     - Management types ............................................................. 18
   - Update protection and software manually ............................... 18
   - View the Event Log ................................................................ 19
     - About log files .................................................................... 20
   - Managing Endpoint Security ................................................ 22
     - Log on as administrator ....................................................... 22
     - Unlock the client interface ............................................... 22
     - Disable and enable features .............................................. 23
     - Change the AMCore content version ................................. 23
     - Use Extra.DAT files ............................................................ 24
     - Configure common settings .............................................. 25

3. **Using Threat Prevention**
   - Scan your computer for malware .......................................... 33
     - Types of scans .................................................................... 33
     - Run a Full Scan or Quick Scan .......................................... 34
     - Scan a file or folder ............................................................. 36
   - Manage threat detections ..................................................... 37
   - Manage quarantined items .................................................... 37
   - Detection names .................................................................... 39
   - Managing Threat Prevention ................................................ 40
     - Excluding items from scans .............................................. 40
     - Detecting potentially unwanted programs ............................ 41
     - Configure Access Protection settings .................................. 43
     - Configure Exploit Prevention settings ............................... 45
     - Configure On-Access Scan settings ..................................... 47
     - Configure On-Demand Scan settings ................................... 52
Contents

Schedule Full Scan and Quick Scan tasks ........................................ 56
Configure common scan settings .............................................. 56

4 Using the Firewall ............................................................................. 59
How the Firewall works ........................................................................ 59
Managing Firewall ........................................................................... 59
Modify Firewall options ...................................................................... 60
Configure Firewall rules and groups .............................................. 62

5 Using Web Control ................................................................................ 73
About Web Control features .............................................................. 73
Web Control button identifies threats while browsing ......................... 74
Safety icons identify threats while searching ......................................... 75
Site reports provide details .................................................................. 75
How safety ratings are compiled .................................................... 76
Access Web Control features ............................................................... 76
Access features while browsing .......................................................... 77
View site report while searching ......................................................... 77
View site reports .............................................................................. 78
Troubleshoot communication problems ............................................ 78
Managing Web Control ................................................................. 79
Configure Web Control options ...................................................... 79
Specify rating actions and block site access based on web category .......... 82

Index ...................................................................................................... 127
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 7
- How Endpoint Security protects your computer on page 8
- Interacting with Endpoint Security on page 9

**Frequently performed tasks**
- Open the Endpoint Security Client on page 15
- Update protection and software manually on page 18
- Scan your computer for malware on page 33
- Unlock the client interface on page 22

**More information**
To access additional information about this product, see:
- *McAfee Endpoint Security Installation Guide*
- *McAfee Endpoint Security Release Notes*
- Endpoint Security Threat Prevention Help
- Endpoint Security Firewall Help
- Endpoint Security Web Control Help
- *McAfee support*
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)
- McAfee® SecurityCenter

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.

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, McAfee ePO Cloud, or SecurityCenter.

See also
Get information about your protection on page 17

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.

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

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 Update Now.

See also
Update protection and software manually on page 18
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 any of the installed content files, the scan engine can't detect and clean that virus.

New threats appear regularly. McAfee Labs releases engine updates and new content files that incorporate the results of ongoing threat research almost every day at about 6:00 PM (GMT).

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.

Exploit Prevention content

The Exploit Prevention content includes:

- Memory protection signatures — Generic Buffer Overflow Protection (GBOP) and Kevlar.
- Application Protection List — Processes that Exploit Prevention protects.

McAfee releases new Exploit Prevention content files once a month.

Interacting with Endpoint Security

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

- McAfee icon in the Windows system tray — Enables you to launch the Endpoint Security Client and view security status.
- Notification messages — Alerts you to scan and firewall intrusion detections 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

About the McAfee system tray icon on page 10
About notification messages on page 10
Manage threat detections on page 37
About the Endpoint Security Client on page 11
About the McAfee system tray icon
The McAfee icon in the Windows system tray provides access to the Endpoint Security Client.

The McAfee icon might not be available, depending on how the settings are configured.

Use the system tray icon to:

- Check the security status — Right-click the icon and select View Security Status to display the McAfee Security Status page.
- Open Endpoint Security Client — Right-click the icon and select McAfee Endpoint Security.

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.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Endpoint Security is protecting your system and no issues exist.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Endpoint Security detects an issue with your security, such as a module or technology is disabled.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>• Firewall is disabled.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>• Threat Prevention — Exploit Prevention, On-Access Scan, or ScriptScan is disabled.</td>
</tr>
</tbody>
</table>

Endpoint Security reports issues differently, depending on the management type.

**Self-managed**
One or more technologies is disabled.

**Managed**
One or more technologies has been disabled manually, not as a result of a policy enforcement from the management server.

When an issue is detected, the McAfee Security Status page indicates which module or technology is disabled.

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.

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.

In Windows 8 Metro mode, toast notifications appear in the upper-right corner of the screen to notify you of both alerts and prompts. Click the toast notification to display the notification in Desktop mode.

The McTray.exe process must be running for Endpoint Security to display alerts and prompts.
About the Endpoint Security Client

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

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

• Buttons on the right of the page provide quick access to frequent tasks.
  - Scan System: 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.
  - Update Now: Updates content files and software components on your computer.
    - This button might not appear, depending on how settings are configured.

• Buttons on the left side of the page provide information about your protection.
  - Status: Returns you to the main Status page.
  - Event Log: Displays the log of all protection and threat events on this computer.
  - Quarantine: Opens the Quarantine Manager.
    - This button is available only if the Threat Prevention module is installed.

• The Threat Summary gives you information about threats that Endpoint Security detected on your system in the last 30 days.
See also
- Load an Extra.DAT file on page 24
- Log on as administrator on page 22
- Scan your computer for malware on page 33
- Update protection and software manually on page 18
- View the Event Log on page 19
- Manage quarantined items on page 37
- Managing Endpoint Security on page 22
- About the Threat Summary on page 12

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

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

The Threat Summary includes:
- Date of the last eliminated threat
- Top two threat vectors, by category:
  - Web: Threats from webpages or downloads.
  - External Device or Media: Threats from external devices, such as USB, 1394 firewire, eSATA, tape, CD, DVD, or disk.
  - Network: Threats from the network (not network file share).
  - Local System: Threats from the local boot file system drive (usually C:) or drives other than those classified as External Device or Media.
  - File Share: Threats from a network file share.
  - Email: Threats from email messages.
  - Instant Message: Threats from instant messaging.
  - Unknown: Threats where attack vector isn't determined (due to error condition or other failure case).
- Number of threats per threat vector

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

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

Change the Client Interface Mode in the Common settings.

For managed systems, policy changes from McAfee ePO, McAfee ePO Cloud, or the SecurityCenter 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.

This mode is the default setting for self-managed systems.

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.

This mode is the default setting for managed systems.

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.
The default password is mcafee.

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

Configure settings for client interface security on page 27

How installed modules affect the client

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

These features are available only if Threat Prevention is installed:

• Scan System button
• Quarantine button

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

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

<table>
<thead>
<tr>
<th>Module</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
<td>Appears if any module is installed.</td>
</tr>
<tr>
<td>Threat Prevention</td>
<td>Appears only if Threat Prevention is installed.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Appears only if Firewall is installed.</td>
</tr>
<tr>
<td>Web Control</td>
<td>Appears only if Web Control is installed.</td>
</tr>
</tbody>
</table>

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 12
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

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, start the McAfee Endpoint Security app.
     1. Press the Windows key to display the Start screen.
     2. Enter McAfee Endpoint Security, 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 22
Get help

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

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.

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 16
  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 16
  When a scheduled on-demand scan is about to start, Endpoint Security might prompt you for input to continue. The prompt appears only if the scan is configured to allow you to defer, pause, resume, or cancel the scan.

Respond to a threat-detection prompt

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

In Windows 8 Metro mode, toast notifications appear in the upper-right corner of the screen to notify you of threat detections. Click the toast notification to display the prompt in Desktop mode.

Task

For option definitions, click ? in the interface.

- 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 37

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.

In Windows 8 Metro mode, toast notifications appear in the upper-right corner of the screen to prompt you for input. Click the toast notification to display the prompt in Desktop mode.

**Task**
For option definitions, click ? in the interface.

- At the prompt, select one of these options.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Now</strong></td>
<td>Starts the scan immediately.</td>
</tr>
<tr>
<td><strong>View Scan</strong></td>
<td>Views detections for a scan in progress.</td>
</tr>
<tr>
<td><strong>Pause Scan</strong></td>
<td>Pauses the scan. Depending on the configuration, clicking <strong>Pause Scan</strong> might reset the scan to run only when you’re idle. Click <strong>Resume Scan</strong> to resume the scan where it left off.</td>
</tr>
<tr>
<td><strong>Resume Scan</strong></td>
<td>Resumes a paused scan.</td>
</tr>
<tr>
<td><strong>Cancel Scan</strong></td>
<td>Cancels the scan.</td>
</tr>
<tr>
<td><strong>Defer Scan</strong></td>
<td>Delays the scan for the specified number of hours.</td>
</tr>
</tbody>
</table>

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.

**See also**
*Respond to a threat-detection prompt on page 16*

---

### 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 18*
*Open the Endpoint Security Client on page 15*
Management types

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

For managed systems, policy changes from McAfeee PO, McAfeee PO Cloud, or the SecurityCenter might overwrite changes from the Settings page.

<table>
<thead>
<tr>
<th>Management type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfeee PO</td>
<td>An administrator manages Endpoint Security using McAfeee PO (on-premise).</td>
</tr>
<tr>
<td>McAfeee PO Cloud</td>
<td>An administrator manages Endpoint Security using McAfeee PO Cloud.</td>
</tr>
<tr>
<td>Self-Managed</td>
<td>Endpoint Security is managed locally using Endpoint Security Client. This mode is also called unmanaged or standalone.</td>
</tr>
</tbody>
</table>

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 on your computer.

If doesn’t appear in the client, you can enable it in the settings. See Configure update behavior on page 29 for information.

Manual updates are called *on-demand updates*.

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

For option definitions, click ? in the interface.

**Task**

1. Open the Endpoint Security Client.
2. Click ![Update Now](update_icon). 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
How your protection stays up to date on page 8
About log files on page 20
Open the Endpoint Security Client on page 15
Configure update behavior on page 29

View the Event Log

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

For help, from the Action menu, select Help.

Task
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 your 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 your 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.

Sort events by date, features, action taken, and severity
Click the table column heading.

Search the event log
Enter the search text in the Search field and press Enter, or click Search.
The search is case-insensitive and searches all fields of the event log for the search text. The event list shows all elements with matching text.
To cancel the search and display all events, click x in the Search field.

Filter events by severity or module
From the filter drop-down list, select an option.
To remove the filter and display all events, select Show all events from the drop-down list.

Refresh the Event Log display with any new events
Click .

Open the folder that contains the log files
Click View Logs Folder.

5 Navigate the Event Log.

Display the previous page of events
Click Previous page.

Display the next page of events
Click Next page.

Display a specific page in the log
Enter a page number and press Enter or click Go.

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

See also
About log files on page 20
Open the Endpoint Security Client on page 15

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

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.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Default location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 8.1 (Blue)</td>
<td>%ProgramData%\McAfee\Endpoint Security\Logs</td>
</tr>
<tr>
<td>Microsoft Windows 8</td>
<td>%ProgramData%\McAfee\Endpoint Security\Installer\Logs</td>
</tr>
<tr>
<td>Microsoft Windows 7</td>
<td></td>
</tr>
<tr>
<td>Microsoft Vista</td>
<td>C:\Documents and Settings\All Users\Application Data\McAfee\Endpoint Security\Logs</td>
</tr>
<tr>
<td>Microsoft Windows XP</td>
<td>McAfee\Endpoint Security\Logs folder under the Application Data folder</td>
</tr>
</tbody>
</table>
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.

---

![Warning icon] Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.

### Table 2-1 Log files

<table>
<thead>
<tr>
<th>Module</th>
<th>Feature or technology</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common</strong></td>
<td></td>
<td><strong>EndpointSecurityPlatform_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>EndpointSecurityPlatform_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Self Protection</strong></td>
<td></td>
<td><strong>SelfProtection_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>SelfProtection_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Updates</strong></td>
<td></td>
<td><strong>PackageManager_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>PackageManager_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Errors</strong></td>
<td></td>
<td><strong>EndpointSecurityPlatform_Errors.log</strong></td>
</tr>
<tr>
<td><strong>Threat Prevention</strong></td>
<td></td>
<td><strong>ThreatPrevention_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ThreatPrevention_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Access Protection</strong></td>
<td></td>
<td><strong>AccessProtection_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>AccessProtection_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Exploit Prevention</strong></td>
<td></td>
<td><strong>ExploitPrevention_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ExploitPrevention_Debug.log</strong></td>
</tr>
<tr>
<td><strong>On-access scanner</strong></td>
<td></td>
<td><strong>OnAccessScan_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OnAccessScan_Debug.log</strong></td>
</tr>
<tr>
<td><strong>On-demand scanner</strong></td>
<td></td>
<td><strong>OnDemandScan_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OnDemandScan_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Access Protection</strong></td>
<td></td>
<td><strong>AccessProtection_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>AccessProtection_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Exploit Prevention</strong></td>
<td></td>
<td><strong>ExploitPrevention_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ExploitPrevention_Debug.log</strong></td>
</tr>
<tr>
<td><strong>On-access scanner</strong></td>
<td></td>
<td><strong>OnAccessScan_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>OnAccessScan_Debug.log</strong></td>
</tr>
<tr>
<td><strong>On-demand scanner</strong></td>
<td></td>
<td><strong>OnDemandScan_Activity.log</strong></td>
</tr>
<tr>
<td><strong>Quick Scan</strong></td>
<td></td>
<td><strong>OnDemandScan_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Full Scan</strong></td>
<td></td>
<td><strong>OnDemandScan_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Right-Click Scan</strong></td>
<td></td>
<td><strong>OnDemandScan_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Endpoint Security Client</strong></td>
<td></td>
<td><strong>MFEConsole_Debug.log</strong></td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td></td>
<td><strong>Firewall_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Firewall_Debug.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>FirewallEventMonitor.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logs blocked and allowed traffic events, if configured.</td>
</tr>
<tr>
<td><strong>Web Control</strong></td>
<td></td>
<td><strong>WebControl_Activity.log</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>WebControl_Debug.log</strong></td>
</tr>
</tbody>
</table>
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, and configuring common settings.

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

See also

- Log on as administrator on page 22
- Unlock the client interface on page 22
- Disable and enable features on page 23
- Change the AMCore content version on page 23
- Use Extra.DAT files on page 24
- Configure common settings on page 25

Log on as administrator

If the interface mode for Endpoint Security Client is set to Standard access, you can log on as administrator to access all settings.

**Before you begin**

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

For help, from the Action menu, select Help.

**Task**

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.

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 must be set to **Full access** or you are logged on as administrator.

The **Status** page shows the enabled status of the module of feature, which might not reflect the actual status of the feature. 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 option definitions, click ? in the interface.

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 22*

**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 must be 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 option definitions, click ? in the interface.

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 9*

*Log on as administrator on page 22*
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 24
  To download an Extra.DAT file, click the download link supplied by McAfee Labs.
- Load an Extra.DAT file on page 24
  To install the downloaded Extra.DAT file, use Endpoint Security Client.

See also
About Extra.DAT files on page 24

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 must be set to Full access or you are logged on as administrator.
Task
For option definitions, click ? in the interface.

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 22

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 26
  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 26
  Configure Endpoint Security logging in the Common settings.
- Configure settings for client interface security on page 27
  Configure the interface password and display options for Endpoint Security Client in the Common settings.
- Configure proxy server settings for McAfee GTI on page 28
  Specify proxy server options for retrieving McAfee GTI reputation in the Common settings.
- Configure update behavior on page 29
  Specify the behavior for updates initiated from the Endpoint Security Client in the Common settings.
- Configure source sites for client updates on page 29
  For self-managed systems, you can configure the sites from which Endpoint Security Client gets updated security files in the Common settings.
- Schedule the Default Client Update task on page 31
  You can modify or schedule the Default Client Update task from the Endpoint Security Client 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 must be set to Full access or you are logged on as administrator.

Users, administrators, developers, or security professionals should never need to disable Endpoint Security protection on their systems.

**Task**
For option definitions, click ? in the interface.

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 22

Configure logging settings
Configure Endpoint Security logging in the Common settings.

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

**Task**
For option definitions, click ? in the interface.

1. Open the Endpoint Security Client.
2. From the Action menu, select Settings.
3. Click Show Advanced.
5. Click Apply to save your changes or click Cancel.
See also
About log files on page 20
Log on as administrator on page 22

Configure settings for client interface security
Configure the interface password and display options for Endpoint Security Client in the Common settings.

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

Modify these settings with caution because they can allow users to change their security configuration, which can leave systems unprotected from malware attacks.

Task
For option definitions, click ? in the interface.

1. Open the Endpoint Security Client.
2. From the Action menu, select Settings.
3. Configure Client Interface Mode settings on the page.
4. Click Apply to save your changes or click Cancel.

See also
Effects of setting an administrator password on page 27
Log on as administrator on page 22

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 must be set to Full access or you are logged on as administrator.

Task
For option definitions, click ? in the interface.

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 28
Log on as administrator on page 22

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 heuristics to check for suspicious files.

The scanner submits fingerprints of samples, or hashes, to a central database server hosted by McAfee Labs to determine if they are malware. By submitting hashes, detection might be made available sooner than the next content file update, when McAfee Labs publishes the update.
You can configure the sensitivity level that McAfee GTI uses when it determines if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections can result in more false positive results. The McAfee GTI sensitivity level is set to Medium by default. Configure the sensitivity level for each scanner in the Threat Prevention settings. 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.

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

You can configure these settings on self- and McAfee ePO-managed systems only.

Use these settings to configure whether to show the **Update Now** button in the client and what to update when the user clicks the button or the Default Client Update task runs.

- **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 option definitions, click ? in the interface.

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 22
- Configure source sites for client updates on page 29
- Schedule the Default Client Update task on page 31

**Configure source sites for client updates**
For self-managed systems, 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 must be set to Full access or you are logged on as administrator.

You can configure these settings on self-managed systems only.
Task
For option definitions, click ? in the interface.

1 Open the Endpoint Security Client.

2 From the Action menu, select Settings.

3 Click Show Advanced.

4 Configure Source Sites for Updates settings on the page.

You can enable and disable the two default backup source sites (NAIFtp and NAIHttp), but you can’t otherwise modify, delete, or move them in the list.

<table>
<thead>
<tr>
<th>To...</th>
<th>Follow these steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a site to the list.</td>
<td>1 Click Add.</td>
</tr>
<tr>
<td></td>
<td>2 Specify the site settings.</td>
</tr>
<tr>
<td></td>
<td>3 Click OK to save your changes.</td>
</tr>
<tr>
<td></td>
<td>The rule appears at the beginning of rule list.</td>
</tr>
<tr>
<td>Delete a site.</td>
<td>Select the site, then click Delete.</td>
</tr>
<tr>
<td>Modify an existing site.</td>
<td>1 Double-click the site name.</td>
</tr>
<tr>
<td></td>
<td>2 Change the settings.</td>
</tr>
<tr>
<td></td>
<td>3 Click OK to save your changes.</td>
</tr>
<tr>
<td>Reorder sites in the list.</td>
<td>To move elements:</td>
</tr>
<tr>
<td></td>
<td>1 Select elements to move.</td>
</tr>
<tr>
<td></td>
<td>The grip appears to the left of elements that can be moved.</td>
</tr>
<tr>
<td></td>
<td>2 Drag-and-drop the elements to the new location.</td>
</tr>
<tr>
<td></td>
<td>A blue line appears between elements where you can drop the dragged elements.</td>
</tr>
<tr>
<td></td>
<td>The order determines the order Endpoint Security uses to search for the update site.</td>
</tr>
</tbody>
</table>

5 Click Apply to save your changes or click Cancel.

See also

How the Default Client Update task works on page 31
Log on as administrator on page 22
Configure update behavior on page 29
Schedule the Default Client Update task on page 31
Schedule the Default Client Update task
You can modify or schedule the Default Client Update task from the Endpoint Security Client in the Common settings.

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

- You can configure these settings on self-managed systems only.
- Use these settings to configure when the Default Client Update task runs. See Configure update behavior on page 29 to configure the default behavior for client updates initiated from the Endpoint Security Client.

**Task**
For option definitions, click ? in the interface.

1. Open the Endpoint Security Client.
2. From the Action menu, select Settings.
3. Click Show Advanced.
4. Click Tasks.
5. Double-click Default Client Update, edit the schedule, then click OK to save your changes or click Cancel.
6. Click Apply to save your changes or click Cancel.

**See also**
How the Default Client Update task works on page 31
Configure update behavior on page 29
Configure source sites for client updates on page 29

**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 AM and repeats every four hours until 11:59 PM.

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** | **Interrupted download**
---|---
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 client updates* on page 29
- *Schedule the Default Client Update task* on page 31
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

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 34
  Use Endpoint Security Client to perform a manual Full Scan or Quick Scan on your computer.
- Scan a file or folder on page 36
  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 33

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 you access files, folders, and programs, the on-access scanner intercepts the operation and scans the item, based on criteria defined by the administrator.

- On-demand scan
Manual
The administrator (or user, for self-managed systems) configures predefined 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 and 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.

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 or Quick Scan tab — Configures on-demand scans.
2 Settings | Common | Tasks — Schedules on-demand scans.

See also
Schedule Full Scan and Quick Scan tasks on page 56
Respond to a scan prompt on page 16

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 option definitions, click ? in the interface.

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. See Manage threat detections on page 37.

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

The AMCore content creation date indicates the last time the content was updated. If the content is more than two days old, McAfee recommends that you 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 any detections.

- **Detection Name** Identifies the name of the detected malware.
- **Type** Displays the threat type.
- **File Name** Identifies the infected file.
- **Action** 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 33
- Configure On-Demand Scan settings on page 52
- Schedule Full Scan and Quick Scan tasks on page 56
- Detection names on page 39
- Update protection and software manually on page 18
- Manage threat detections on page 37
Scan a file or folder
Right-click in Windows Explorer to immediately scan an individual file or folder that you suspect is infected.

Before you begin
The Threat Prevention module must be installed.

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

Task
1 In Windows Explorer, right-click the file or folder to scan and select Scan for threats from the pop-up menu.
   Endpoint Security Client displays the status of the scan in the Scan for threats page.
2 Click buttons at the top of the page to control the scan.
   - Pause Scan: Pauses the scan before it completes.
   - Resume Scan: Resumes a paused scan.
   - Cancel Scan: Cancels a running scan.
3 When the scan completes, the page displays any detections.
   - Detection Name: Identifies the name of the detected malware.
   - Type: Displays the threat type.
   - File Name: Identifies the infected file.
   - Action: Describes the last security action taken on the infected file:
     - Access Denied
     - Cleaned
     - Deleted
     - None

The on-demand scan detection list is cleared when the next on-demand scan starts.
4 Select a detection in the table, then click Clean or Delete to clean or delete the infected file.
   Depending on the threat type and scan settings, these actions might not be available.
5 Click Close to close the page.

See also
Types of scans on page 33
Configure On-Demand Scan settings on page 52
Detection names on page 39
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 option definitions, click ? in the interface.

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.
For help, from the Action menu select Help.

**Task**

1. Open the Endpoint Security Client.
2. Click Quarantine on the left side of the page.
   The page shows any items in the Quarantine.

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

   **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.

   **Delete items from the quarantine**
   Select items, click Delete, then click Delete again to confirm.
   Deleted items can't be restored.

   **Restore items from the quarantine**
   Select items, click Restore, then click Restore again to confirm.
   Endpoint Security restores items to the original location and removes them from the quarantine.

   If an item is still a valid threat, Endpoint Security returns it to the quarantine the next time the item is accessed.

   **Rescan items**
   Select items, then click Rescan.
   For example, you might rescan an item after updating your protection. If the item is no longer a threat, you can restore the item to its original location and remove it from the quarantine.

   **View an item in the Event Log**
   Select an item, then click the View in Event Log link in the details pane.
   The Event Log page opens, with the event related to the selected item highlighted.

   **Get more information about a threat**
   Select an item, then click the Learn more about this threat link in the details pane.
   A new browser window opens to the McAfee Labs website with more information about the threat that caused the item to be quarantined.

**See also**
Detection names on page 39
Open the Endpoint Security Client on page 15
Update protection and software manually on page 18
The Quarantine reports threats by detection name.

<table>
<thead>
<tr>
<th>Detection name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware</td>
<td>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.</td>
</tr>
<tr>
<td>Dialer</td>
<td>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.</td>
</tr>
<tr>
<td>Joke</td>
<td>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.</td>
</tr>
<tr>
<td>Keylogger</td>
<td>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.</td>
</tr>
<tr>
<td>Password Cracker</td>
<td>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.</td>
</tr>
<tr>
<td>Potentially unwanted program</td>
<td>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.</td>
</tr>
<tr>
<td>Remote Admin Tool</td>
<td>Gives an administrator remote control of a system. These tools can be a significant security threat when controlled by an attacker.</td>
</tr>
<tr>
<td>Spyware</td>
<td>Transmits personal information to a third party without the user's knowledge or consent. Spyware exploits infected computers for commercial gain by:</td>
</tr>
<tr>
<td></td>
<td>• Delivering unsolicited pop-up advertisements</td>
</tr>
<tr>
<td></td>
<td>• Stealing personal information, including financial information, such as credit card numbers</td>
</tr>
<tr>
<td></td>
<td>• Monitoring web-browsing activity for marketing purposes</td>
</tr>
<tr>
<td></td>
<td>• Routing HTTP requests to advertising sites</td>
</tr>
<tr>
<td></td>
<td>See also Potentially unwanted program.</td>
</tr>
<tr>
<td>Stealth</td>
<td>Is a type of virus that attempts to avoid detection from anti-virus software. Also known as interrupt interceptor. Many stealth viruses intercept disk-access requests. When an anti-virus application tries to read files or boot sectors to find the virus, the virus shows a &quot;clean&quot; image of the requested item. Other viruses hide the actual size of an infected file and display the size of the file before infection.</td>
</tr>
<tr>
<td>Detection name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>Is a malicious program that pretends to be a benign application. A trojan doesn't replicate but causes damage or compromises the security of your computer. Typically, a computer becomes infected: • When a user opens a trojan attachment in email. • When a user downloads a trojan from a website. • Peer-to-peer networking. Because they don't replicate themselves, trojans aren't considered viruses.</td>
</tr>
<tr>
<td>Virus</td>
<td>Attaches to disks or other files and replicates itself repeatedly, typically without user knowledge or permission. Some viruses attach to files, so when the infected file executes, the virus also executes. Other viruses reside in a computer's memory and infect files as the computer opens, modifies, or creates files. Some viruses exhibit symptoms, while others damage files and computer systems.</td>
</tr>
</tbody>
</table>

### 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, McAfee ePO Cloud, or the SecurityCenter might overwrite changes from the Settings page.

See also
- Excluding items from scans on page 40
- Detecting potentially unwanted programs on page 41
- Configure Access Protection settings on page 43
- Configure Exploit Prevention settings on page 45
- Configure On-Access Scan settings on page 47
- Configure On-Demand Scan settings on page 52
- Schedule Full Scan and Quick Scan tasks on page 56
- Configure common scan settings on page 56

#### Excluding items from scans

Threat Prevention enables you to fine-tune the list of scanned items 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.)

<table>
<thead>
<tr>
<th>For this feature...</th>
<th>Specify items to exclude</th>
<th>Where to configure</th>
<th>Exclude items by</th>
<th>Use wildcards?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Protection</td>
<td>Processes (for all rules or a specified rule)</td>
<td>Access Protection settings</td>
<td>Process name</td>
<td>No</td>
</tr>
<tr>
<td>Exploit Prevention</td>
<td>Processes</td>
<td>Exploit Prevention settings</td>
<td>Process name</td>
<td>No</td>
</tr>
<tr>
<td>On-access scan</td>
<td>Files, file types, and folders</td>
<td>On-Access Scan settings</td>
<td>Pattern, file type, or file age</td>
<td>Yes</td>
</tr>
<tr>
<td>Default</td>
<td>ScriptScan URLs</td>
<td>On-Access Scan settings</td>
<td>URL name</td>
<td>No</td>
</tr>
</tbody>
</table>
### Wildcards in scan exclusions

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

#### Table 3-1 Valid wildcards

<table>
<thead>
<tr>
<th>Wildcard character</th>
<th>Name</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Question mark</td>
<td>Single character.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>Multiple characters.</td>
</tr>
<tr>
<td>**</td>
<td>Double asterisk</td>
<td>Zero or more of any characters, including backslash ().</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This wildcard matches zero or more characters. For example: C:\ABC**\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\XYZ.</td>
</tr>
</tbody>
</table>

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

### 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 42
Enable and configure potentially unwanted program detection and responses on page 42
Configure On-Access Scan settings on page 47
Configure On-Demand Scan settings on page 52

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 must be 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 option definitions, click ? in the interface.

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 22

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 must be set to Full access or you are logged on as administrator.
**Task**
For option definitions, click ? in the interface.

   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 47
Configure On-Demand Scan settings on page 52
Log on as administrator on page 22

**Configure Access Protection settings**
Use rules in the Access Protection settings to protect your system’s access points.

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

You can enable, disable, and edit these rules, but you can’t delete them.

**Task**
For option definitions, click ? in the interface.

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 In the Exclusions section, add processes to exclude from all rules.

   Use the exact process name. For example, specify these exclusions: avtask.exe, cfgwiz.exe, fssm32.exe, kavsvc.exe, mmc.exe, navw32.exe, nmain.exe, rtvscan.exe.

   Access Protection allows access to the processes you specify.

7 In the Rules section, select Block, Report, or both for each rule.

   To block or report all, select Block or Report in the first row.

   To disable a rule, deselect both the Block and Report actions.

8 Select a rule, click Add, then enter a process to exclude from the selected rule.

9 Click Apply to save your changes or click Cancel.

See also

Log on as administrator on page 22

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 computer by restricting access to specified ports, files, shares, and registry and keys.

Access Protection uses rules to report or block access to items. The on-access scanner compares a requested action against the list of rules and takes the action specified by the rule.

The on-access scanner must be enabled to detect attempts to access ports, files, shares, and registry keys and values.

How threats gain access

Threats gain access to your system using various access points.

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

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 must be set to Full access or you are logged on as administrator.

Task
For option definitions, click ? in the interface.

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 22
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 Internet Explorer, Microsoft Outlook, Outlook Express, Microsoft Word, and MSN Messenger.

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 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 must be set to Full access or you are logged on as administrator.

Task
For option definitions, click ? in the interface.

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.
   • 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 22
Configure common scan settings on page 56

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 System 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.
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** — If the scanner detects a threat in the path of an installed Windows Store app, the scanner marks it as *tampered*. Windows 8 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.
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.

**Scanning scripts**

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

For example:

- 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 doesn't execute.

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.

Deselect this option to enable the client computer to use both the exclusions specified here and the exclusions that are specified locally on the client.

You can specify websites to exclude from inspection if they use scripts.

On Windows Server 2008 systems, ScriptScan URL exclusions don't work with Windows Internet Explorer unless you enable third-party browser extensions and restart the system. See the KnowledgeBase article KB69526.
How to determine scanning settings for processes

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

When balancing performance against security...

Do you need to scan some processes more or less thoroughly?

No

Yes

Identify processes for each risk category.

Configure Standard settings for all processes.

Risk Categories

Low-risk processes
Processes with a lower possibility of spreading or introducing potential threats.

High-risk processes
Processes with a higher possibility of spreading or introducing potential threats.

Unlisted processes
Any process not defined as low risk or high risk.
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 must be set to Full access or you are logged on as administrator.

See the Common settings for more configuration options.

**Task**
For option definitions, click ? in the interface.

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 22
Configure common scan settings on page 56
Schedule Full Scan and Quick Scan tasks on page 56

**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** — If the scanner detects a threat in the path of an installed Windows Store app, the scanner marks it as *tampered*. Windows 8 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.

![Warning]

McAfee recommends disabling 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 On-Demand Scan settings.

**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 On-Demand Scan settings:

- **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 On-Demand Scan settings.

**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 Timeout category for the On-Demand Scan task. See Schedule Full Scan and Quick Scan tasks on page 56.

**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 On-Demand Scan settings.

**See also**

Configure On-Demand Scan settings on page 52
Schedule Full Scan and Quick Scan tasks on page 56

**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

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

**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 Scan 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.
Schedule Full Scan and Quick Scan tasks

You can schedule the default Full Scan and Quick Scan tasks from the Endpoint Security Client in the Common module.

Before you begin

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

Task

For option definitions, click ? in the interface.

1. Open the Endpoint Security Client.
2. From the Action menu, select Settings.
3. Click Show Advanced.
4. Click Tasks.
5. Double-click Full Scan or Quick Scan, edit the schedule, then click OK to save your changes or click Cancel.
6. Click Apply to save your changes or click Cancel.

See also

Log on as administrator on page 22
Configure On-Demand Scan settings on page 52

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 must be 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
Task
For option definitions, click ? in the interface.

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 22
Configure On-Access Scan settings on page 47
Configure On-Demand Scan settings on page 52
Using the Firewall

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

Contents
- How the Firewall works
- Managing Firewall

How the 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 60
How firewall rules work on page 62
How firewall rule groups work on page 64

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, McAfee ePO Cloud, or the SecurityCenter might overwrite changes from the Settings page.

See also
Modify Firewall options on page 60
Create and manage Firewall rules and groups on page 67
Modify Firewall options
As administrator, you can modify Firewall options from the Endpoint Security Client.

Tasks
- Configure Firewall options on page 60
  Configure settings in Options to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options.
- Block DNS traffic on page 60
  To refine firewall protection, create a list of FQDNs to block. Firewall blocks connections to the IP addresses resolving to the domain names.

See also
FAQ — McAfee GTI and Firewall on page 61

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 must be set to Full access or you are logged on as administrator.

Task
For option definitions, click ? in the interface.

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.
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 22

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 must be set to Full access or you are logged on as administrator.
Task
For option definitions, click ? in the interface.

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.


4. Enter the FQDN of the domains to block.
   You can use the * and ? wildcards. For example, *domain.com.

   ! Any duplicate entries are removed automatically.

5. 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.

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 67
  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 70
  Create a connection isolation firewall rule group to establish a set of rules that apply only when connecting to a network with particular parameters.

See also

How firewall rules work on page 62
How firewall rule groups work on page 64

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.

**Figure 4-1  Rule precedence**

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 organized 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 its rules location-aware and 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

**Network:**

- Local IP address
- Media type

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.

<table>
<thead>
<tr>
<th>If this option is selected...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable location awareness</td>
<td>A location name is required.</td>
</tr>
<tr>
<td>Require that McAfee ePO is reachable</td>
<td>The McAfee ePO is reachable and the FQDN of the server has been resolved.</td>
</tr>
<tr>
<td>Local Network</td>
<td>The IP address of the adapter must match one of the list entries.</td>
</tr>
<tr>
<td>Connection-specific DNS Suffix</td>
<td>The DNS suffix of the adapter must match one of the list entries.</td>
</tr>
<tr>
<td>Default gateway</td>
<td>The default adapter gateway IP address must match at least one of the list entries.</td>
</tr>
<tr>
<td>If this option is selected...</td>
<td>Then...</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>DHCP server</td>
<td>The adapter DHCP server IP address must match at least one of the list entries.</td>
</tr>
<tr>
<td>DNS server</td>
<td>The adapter DNS server IP address must match any of the list entries.</td>
</tr>
<tr>
<td>Primary WINS server</td>
<td>The adapter primary WINS server IP address must match at least one of the list entries.</td>
</tr>
<tr>
<td>Secondary WINS server</td>
<td>The adapter secondary WINS server IP address must match at least one of the list entries.</td>
</tr>
<tr>
<td>Domain reachability (HTTPS)</td>
<td>The specified domain must be reachable using HTTPS.</td>
</tr>
</tbody>
</table>

**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:

- Media 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:

- Media 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.

**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 must be 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 option definitions, click ? in the interface.

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, then click *Apply* to save changes to Firewall Rules.

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Follow these steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the rules in a firewall group.</td>
<td>Click ➔.</td>
</tr>
<tr>
<td>Collapse a firewall group.</td>
<td>Click ☑.</td>
</tr>
</tbody>
</table>
| Modify an existing rule.           | 1. Expand the *User added* group.  
                                       2. Double-click the rule.  
                                       3. Change the rule settings.  
                                       4. Click OK to save your changes. |
| View an existing rule in any group. | 1. Expand the group.  
                                           2. Select the rule to view its details in the bottom pane. |
| Create a rule.                     | 1. Click *Add Rule*.  
                                           2. Specify the rule settings.  
                                           3. Click OK to save your changes.  
                                           The rule appears at the end of the *User added* group. |
| Create copies of rules.            | 1. Select the rule or rules and click *Duplicate*.  
                                           Copied rules appear with the same name at the end of the *User added* group.  
                                           2. Modify the rules to change the name and settings. |
| Delete rules.                      | 1. Expand the group.  
                                           2. Select the rule or rules and click *Delete*. |
To do this... | Follow these steps
---|---
Create a group. | 1 Click **Add Group**.
| 2 Specify the group settings.
| 3 Click **OK** to save your changes.
The group appears in the **User added** group.

Move rules and groups within and between groups. | To move elements:
---|---
You can move rules and groups in the **User added** group only. | 1 Select elements to move.
The grip appears to the left of elements that can be moved.
2 Drag-and-drop the elements to the new location.
A blue line appears between elements where you can drop the dragged elements.

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

**See also**
*Wildcards in firewall rules* on page 69
*Allowing FTP connections* on page 70
*Log on as administrator* on page 22
*Create connection isolation groups* on page 70

**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 must be set to Full access or you are logged on as administrator.

**Task**
For option definitions, click ? in the interface.

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.
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 Network Options, for Media 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 Apply to save your changes or click Cancel.
8. Create new rules within this group, or move existing rules into it from the firewall rule list.

**See also**
- Firewall rule groups and connection isolation on page 65
- How firewall rule groups work on page 64

**Allowing FTP connections**
To allow active mode FTP connections, create firewall rules to allow incoming and outgoing connections on specific ports.

The FTP protocol uses two connections: control for commands and data for the information.

Because Firewall doesn't inspect FTP protocol packets, FTP connections aren't allowed by default. To allow FTP connections, create firewall rules to allow connections for specific ports.

**Active mode FTP**
When a client connects to an FTP server in active mode:

- The control channel is established on TCP port 21.
- The data channel is established on TCP port 20.
To enable an FTP client to connect and download/upload data to an FTP server using active mode, create the following firewall rules on the client:

- Allow outgoing connections for TCP port 21 on the server.
- Allow incoming connections for TCP port 20 on the server.

To enable an FTP server to allow an FTP client to connect and download/upload data, create the following firewall rules on the server:

- Allow incoming connections for TCP port 21 on the server.
- Allow outgoing connections for TCP port 20 on the server.

**Passive mode FTP**

Passive mode FTP requires that you open a range of ports for the data channel on the FTP server.

When a client connects to an FTP server in passive mode:

- The control channel is established on TCP port 21.
- The data channel is established on the TCP port range 1025–5000.

To enable an FTP client to connect and download/upload data to an FTP server using passive mode, create the following firewall rules on the client:

- Allow outgoing connections for TCP port 21 on the server.
- Allow outgoing and incoming connections for the TCP port range 1025–5000 on the server.

To enable an FTP server to allow an FTP client to connect and download/upload data, create the following firewall rules on the server:

- Allow incoming connections for TCP port 21 on the server.
- Allow outgoing and incoming connections for the TCP port range 1025–5000 on the server.

See also

*Create and manage Firewall rules and groups on page 67*
Access Web Control protection features from your browser while browsing or searching.

**Contents**
- About Web Control features
- Access Web Control features
- Managing 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 upper-right corner. 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 software and 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, and prevent or allow the disabling the software and 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.

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

Firefox doesn't allow you to check file downloads or to hide the Web Control button with the View | Toolbars command.

Chrome doesn't support file download enforcement or the Show Balloon option.

See also
Web Control button identifies threats while browsing on page 74
Safety icons identify threats while searching on page 75
Site reports provide details on page 75
How safety ratings are compiled on page 76

Web Control button identifies threats while browsing

When you browse to a website, a color-coded button appears in the upper-right corner of the browser. The color of the button corresponds to the safety rating for the site.

The Chrome browser window displays a small button in the address bar.

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>This site is tested daily and certified safe by McAfee SECURE™.</td>
</tr>
<tr>
<td>Green</td>
<td>This site is safe.</td>
</tr>
<tr>
<td>Yellow</td>
<td>This site might have some issues.</td>
</tr>
<tr>
<td>Red</td>
<td>This site might have some serious issues.</td>
</tr>
<tr>
<td>Gray</td>
<td>No rating is available for this site.</td>
</tr>
<tr>
<td>Orange</td>
<td>A communication error occurred with the McAfee GTI server that contains rating information.</td>
</tr>
<tr>
<td>Blue</td>
<td>No information is available to rate this site. The reason might be that the site is internal or in a private IP address range.</td>
</tr>
<tr>
<td>Black</td>
<td>This site is a phishing site.</td>
</tr>
<tr>
<td>White</td>
<td>A setting allows this site.</td>
</tr>
<tr>
<td>Silver</td>
<td>A setting disabled Web Control.</td>
</tr>
</tbody>
</table>

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.

See also
Access features while browsing on page 77
Troubleshoot communication problems on page 78
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 77

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.

<table>
<thead>
<tr>
<th>This item...</th>
<th>Indicates...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>The overall rating for the website, determined from these tests:</td>
</tr>
<tr>
<td></td>
<td>• Evaluation of a website's email and download practices using proprietary data collection and analysis techniques.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Analysis of the website's online affiliations to see if it associates with other suspicious sites.</td>
</tr>
<tr>
<td></td>
<td>• Combination of the McAfee review of suspicious sites with feedback from our Threat Intelligence services.</td>
</tr>
<tr>
<td>Online Affiliations</td>
<td>How aggressively the site tries to get you to go to other sites that McAfee flagged with a red rating.</td>
</tr>
<tr>
<td></td>
<td>Suspicious sites often associate with other suspicious sites. The primary purpose of feeder sites is to get you to visit the suspicious site. A site can receive a red rating if, for example, it links too aggressively to other red sites. In this case, Web Control considers the site red by association.</td>
</tr>
<tr>
<td>Web Spam Tests</td>
<td>The overall rating for a website's email practices, based on the test results.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Download Tests</td>
<td>The overall rating about the impact a site's downloadable software had on our test computer, based on the test results.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
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

- Access features while browsing on page 77
  Access Web Control features from the button on the browser. The button works differently depending on the browser.
- View site report while searching on page 77
  Use the safety icon on a search results page to view more information about the site.
- View site reports on page 78
  To get more information about a site’s safety rating, view the site reports.
- Troubleshoot communication problems on page 78
  On the client computer, run tests from the browser to determine the reason for problems communicating with the McAfee GTI safety ratings server.
Access features while browsing

Access Web Control features from the button on the browser. The button works differently depending on the browser.

**Internet Explorer and Firefox**

- Hold the cursor over this button to display a balloon with a summary of the safety report for the site.
- Click the button to display the detailed safety report.
- Click the button next to the icon to display a menu of features.

**Chrome** — Click the button to display a menu of features.

In Chrome, you can’t display balloons with the menu button. Balloons are available only from search results pages.

**Task**

1. From the menu, select options.

<table>
<thead>
<tr>
<th>Option</th>
<th>To do...</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>View Site Report</strong></td>
<td>View the safety report for the current site.</td>
<td>Available only when Web Control is enabled.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="McAfee" /> You can also click Read site report in the site balloon.</td>
<td></td>
</tr>
<tr>
<td><strong>Show Balloon</strong></td>
<td>Display the balloon for the current site.</td>
<td>Available only when Web Control is enabled, and for browsers other than Chrome.</td>
</tr>
</tbody>
</table>

2. If the communication error button ![McAfee](image) appears, show the balloon for the site, and click **Troubleshoot**.

The connection status page indicates the possible cause of the communication error.

**See also**

*Web Control button identifies threats while browsing on page 74*

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 75*

*Site reports provide details on page 75*
**View site reports**
To get more information about a site’s safety rating, view the site reports.

**Task**
- View the report for a site.

<table>
<thead>
<tr>
<th>From this location...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Website               | • Select View Site Report from the Web Control menu.  
                        • Click the balloon.  
                        • Click Read site report in the balloon. |
| Search results page   | Click the safety icon following the webpage link. |

**See also**
*Site reports provide details on page 75*

**Troubleshoot communication problems**
On the client computer, run tests from the browser to determine the reason for problems communicating with the McAfee GTI safety ratings server.

An orange button [McAfee](image) in the upper right corner of the browser indicates communication problems with the McAfee GTI server.

- Communication troubleshooting isn’t available in Chrome. To perform these tests, use Internet Explorer or Firefox.

**Task**
1. In Internet Explorer or Firefox, hold the cursor over the orange button to display the balloon.
2. Click Troubleshoot to run tests and display the results.
   - A connection status page displays the reason for the communication error and possible resolutions after these tests are completed.

<table>
<thead>
<tr>
<th>Test</th>
<th>Checks for...</th>
<th>A failed test means...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Access</td>
<td>Does the browser have Internet access?</td>
<td>Your computer can't access the Internet. This failure might mean that your network connection is down or the proxy settings are configured incorrectly. Contact your administrator.</td>
</tr>
<tr>
<td>McAfee GTI Server</td>
<td>Is the McAfee GTI server down?</td>
<td>The McAfee GTI servers are down.</td>
</tr>
</tbody>
</table>

3. Check the results when they are displayed and follow any instructions to resolve the problem.
4. Retest the connection by clicking Repeat Tests.
   - The Repeat Tests button enables you to see if the error persists or is corrected while the page is open.

**See also**
*Web Control button identifies threats while browsing on page 74*
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, McAfee ePO Cloud, or the SecurityCenter might overwrite changes from the Settings page.

See also
Configure Web Control options on page 79
Specify rating actions and block site access based on web category on page 82

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 must be set to Full access or you are logged on as administrator.

Task
For option definitions, click ? in the interface.

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.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide the Web Control toolbar on the browser without disabling protection.</td>
<td>Select Hide the toolbar on the client browser.</td>
<td>Use this setting to resolve third-party compatibility issues.</td>
</tr>
<tr>
<td>Track browser events to use for reports.</td>
<td>Configure settings in the <strong>Event Logging</strong> section.</td>
<td>Configure Web Control events sent from client systems to the management server to use for queries and reports.</td>
</tr>
<tr>
<td>Block or warn unknown URLs.</td>
<td>In <strong>Action Enforcement</strong>, select the action (Block, Allow, or Warn) for sites not yet verified by McAfee GTI.</td>
<td></td>
</tr>
<tr>
<td>Scan files before downloading.</td>
<td>Select <strong>Enable file scanning for file downloads</strong>, then select the McAfee GTI risk level to block.</td>
<td></td>
</tr>
<tr>
<td>Block risky sites from appearing in search results.</td>
<td>In <strong>Secure Search</strong>, select <strong>Enable Secure Search</strong>, select the search engine, then specify whether to block links to risky sites.</td>
<td>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. If you change the default search engine, restart the browser for the changes to take effect.</td>
</tr>
</tbody>
</table>

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 81*
*Log on as administrator on page 22*
**How file downloads are scanned**

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

1. **User clicks a link to download a file.**
2. **Web Control checks the rating for the URL.**
3. **Does the rating allow the file download?**
   - **Yes:**
     - **Is Threat Prevention installed and ODS enabled?**
       - **Yes:**
         - **Web Control sends the file to Threat Prevention for scanning.**
       - **No:**
         - **File download is blocked.**
   - **No:**
     - **File download is blocked.**

4. **Does the rating allow the file download?**
   - **Yes:**
     - **Threat Prevention checks the file against the AMCore content files.**
     - **Web Control performs a McAfee GTI file reputation lookup on the file.**
     - **A**
     - **Does the file match a signature or hash in the AMCore content files?**
       - **Yes:**
         - **File download is blocked.**
       - **No:**
         - **Threat Prevention performs a McAfee GTI file reputation lookup on the file.**

5. **Does McAfee GTI allow the file download?**
   - **Yes:**
     - **File is downloaded**
   - **No:**
     - **File download is blocked.**
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 must be set to Full access or you are logged on as administrator.

Web Control applies the rating actions to sites in the unblocked categories specified in the Web Category Blocking section under Advanced.

Task
For option definitions, click ? in the interface.

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 82
Using safety ratings to control access on page 83
Log on as administrator on page 22

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.

By default, most of the web categories that McAfee gives a green rating are allowed, yellow are warned, and red are blocked. However, some unrated content categories are warned or blocked by default, based on McAfee GTI recommendation. Use the settings for Content Actions to block or allow web categories. Use the Rating Actions settings to specify the actions for sites and downloads in unblocked 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

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

Contents

- Event Log page
- Quarantine page
- Common — Options
- Common — Tasks
- Threat Prevention — Access Protection
- Threat Prevention — Exploit Prevention
- Threat Prevention — On-Access Scan
- Threat Prevention — On-Demand Scan
- Scan Locations
- McAfee GTI
- Actions
- Add or Edit exclusions
- Threat Prevention — Options
- Roll Back AMCore Content
- Firewall — Options
- Firewall — Rules
- Web Control — Options
- Web Control — Content Actions

Event Log page

Displays the activity and debug events in the Event Log.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of events</td>
<td>Indicates the number of events that Endpoint Security logged on the system in the last 30 days.</td>
</tr>
<tr>
<td></td>
<td>Refreshes the Event Log display with any new event data.</td>
</tr>
<tr>
<td>View Logs Folder</td>
<td>Opens the folder that contains the log files in Windows Explorer.</td>
</tr>
<tr>
<td>Show all events</td>
<td>Removes any filter.</td>
</tr>
<tr>
<td>Filter by Severity</td>
<td>Filters events by a severity level:</td>
</tr>
<tr>
<td></td>
<td>Critical: Shows level 1 severity events only.</td>
</tr>
<tr>
<td></td>
<td>Major and greater: Shows levels 1 and 2 severity events only.</td>
</tr>
<tr>
<td></td>
<td>Minor and greater: Shows levels 1, 2, and 3 severity events only.</td>
</tr>
<tr>
<td></td>
<td>Warning and greater: Shows levels 1, 2, 3, and 4 severity levels.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Filter by Module</strong></td>
<td>Filters events by module:</td>
</tr>
<tr>
<td>Common</td>
<td>Shows Common events only.</td>
</tr>
<tr>
<td>Threat Prevention</td>
<td>Shows Threat Prevention events only.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Shows Firewall events only.</td>
</tr>
<tr>
<td>Web Control</td>
<td>Shows Web Control events only.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Search</th>
<th>Searches the Event Log for a string.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events per page</td>
<td>Selects the number of events to display on a page. (By default, 20 events per page)</td>
</tr>
<tr>
<td>Previous page</td>
<td>Displays the previous page in the Event Log.</td>
</tr>
<tr>
<td>Next page</td>
<td>Displays the next page in the Event Log.</td>
</tr>
<tr>
<td>Page x of x</td>
<td>Selects a page in the Event Log to navigate to.</td>
</tr>
<tr>
<td></td>
<td>Enter a number in the Page field and press Enter or click Go to navigate to the page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Sorts the event list by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Date the event occurred.</td>
</tr>
<tr>
<td>Feature</td>
<td>Feature that logged the event.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that Endpoint Security took, if any, in response to the event.</td>
</tr>
<tr>
<td></td>
<td>The action is configured in the settings.</td>
</tr>
<tr>
<td>Allowed</td>
<td>Allowed access to file.</td>
</tr>
<tr>
<td>Access Denied</td>
<td>Prevented access to file.</td>
</tr>
<tr>
<td>Deleted</td>
<td>Deleted file automatically.</td>
</tr>
<tr>
<td>Continue</td>
<td></td>
</tr>
<tr>
<td>Cleaned</td>
<td>Removed the threat from the file automatically.</td>
</tr>
<tr>
<td>Moved</td>
<td>Moved the file into the Quarantine.</td>
</tr>
<tr>
<td>Blocked</td>
<td>Blocked access to the file.</td>
</tr>
<tr>
<td>Would Block</td>
<td>An Access Protection rule would have blocked access to the file if the rule was being enforced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity</th>
<th>Severity level of the event.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>1</td>
</tr>
<tr>
<td>Major</td>
<td>2</td>
</tr>
<tr>
<td>Minor</td>
<td>3</td>
</tr>
<tr>
<td>Warning</td>
<td>4</td>
</tr>
<tr>
<td>Informational</td>
<td>5</td>
</tr>
</tbody>
</table>

**See also**

*View the Event Log on page 19*
Quarantine page

Manages items in the Quarantine.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Deletes selected items from the Quarantine.</td>
</tr>
<tr>
<td></td>
<td>Deleted items can't be restored.</td>
</tr>
<tr>
<td>Restore</td>
<td>Restores items from the Quarantine. Endpoint Security restores items to the original location and removes them from the Quarantine.</td>
</tr>
<tr>
<td></td>
<td>If an item is still a valid threat, Endpoint Security immediately returns it to the Quarantine.</td>
</tr>
<tr>
<td>Rescan</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Sorts the quarantine list by...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection Name</td>
<td>Name of the detection.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of threat, for example, Trojan or Adware.</td>
</tr>
<tr>
<td>Time quarantined</td>
<td>The length of time the item has been quarantined.</td>
</tr>
<tr>
<td>Number of objects</td>
<td>The number of objects in the detection.</td>
</tr>
<tr>
<td>AMCore content version</td>
<td>The version number of AMCore content that identified the threat.</td>
</tr>
</tbody>
</table>

See also

Manage quarantined items on page 37
Detection names on page 39

Common — Options


Table 6-1

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Interface</td>
<td>Full access</td>
<td>Allows access to all features. (Default for self-managed systems)</td>
</tr>
<tr>
<td>Mode</td>
<td>Standard access</td>
<td>Displays protection status and allows access to most features, such as run updates and scans.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Standard access</strong> mode requires a password to view and modify settings on the Endpoint Security Client Settings page. The default password is <strong>mcafee</strong>.</td>
</tr>
<tr>
<td></td>
<td>Lock client interface</td>
<td>Requires a password to access the Endpoint Security Client.</td>
</tr>
</tbody>
</table>
Table 6-1  *(continued)*

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set Administrator password</td>
<td>For <strong>Standard access</strong> and <strong>Lock client interface</strong>, specifies the administrator password for accessing all features of the Endpoint Security Client interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Password</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Confirm password</strong></td>
</tr>
<tr>
<td>Uninstallation</td>
<td>Require password to uninstall the client</td>
<td>Requires a password to uninstall the Endpoint Security Client and specifies the password. (Disabled by default for self-managed systems)</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Password</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Confirm password</strong></td>
</tr>
</tbody>
</table>

Table 6-2  Advanced options

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Client Interface Language</td>
<td>Automatically selects the language to use for Endpoint Security Client interface text based on the language on the client system.</td>
</tr>
<tr>
<td></td>
<td>Language</td>
<td><strong>Language</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For managed systems, changes made from the client system affect the Endpoint Security Client interface. The language change is applied after</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the Endpoint Security Client restarts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>The client language doesn't affect the log files. Log files always appear in the language specified by the default system locale.</strong></td>
</tr>
<tr>
<td></td>
<td>Self Protection</td>
<td>Enable Self Protection</td>
</tr>
<tr>
<td></td>
<td>Action</td>
<td>Specifies the action to take when malicious activity occurs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Block and report</strong> — Blocks and reports to McAfee ePO. (Default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Block only</strong> — Blocks but doesn't report to McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Report only</strong> — Reports to McAfee ePO but doesn't block activity.</td>
</tr>
<tr>
<td></td>
<td>Files and folders</td>
<td>Prevents modifying or deleting McAfee system files and folders.</td>
</tr>
<tr>
<td></td>
<td>Registry</td>
<td>Prevents modifying or deleting McAfee registry keys and values.</td>
</tr>
<tr>
<td></td>
<td>Processes</td>
<td>Prevents stopping McAfee processes.</td>
</tr>
<tr>
<td></td>
<td>Exclude these processes</td>
<td>Allows access to the specified processes.</td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Adds a process to the exclusion list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>Add</strong>, then enter the exact resource name, such as avtask.exe.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Deletes a process from the exclusion list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the resource, then click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
## Table 6-2 Advanced options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Logging</strong></td>
<td><strong>Log files location</strong></td>
<td>Specifies the location for the log files. The default location is: <code>&lt;SYSTEM_DRIVE&gt;:\ProgramData\McAfee\Endpoint\Logs</code> Enter or click <strong>Browse</strong> to navigate to a location.</td>
</tr>
<tr>
<td><strong>Activity Logging</strong></td>
<td><strong>Enable activity logging</strong></td>
<td>Enables logging of all Endpoint Security activity.</td>
</tr>
<tr>
<td></td>
<td><strong>Limit size (MB) of each of the activity log files</strong></td>
<td>Limits each activity log file to the specified maximum size (between 1 MB and 999 MB). The default is 10 MB. Disable this option to allow log files to grow to any size. If the log file exceeds this size, new data replaces the oldest 25 percent of the entries in the file.</td>
</tr>
<tr>
<td><strong>Debug Logging</strong></td>
<td><img src="https://example.com/warning.png" alt="Warning" /></td>
<td>Enabling debug logging for any module also enables debug logging for the Common module features, such as Self Protection.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable for Firewall</strong></td>
<td>Enables verbose logging of Firewall activity.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable for Web Control</strong></td>
<td>Enables verbose logging of Web Control activity.</td>
</tr>
<tr>
<td></td>
<td><strong>Limit size (MB) of each of the debug log files</strong></td>
<td>Limits each debug log file to the specified maximum size (between 1 MB and 999 MB). The default is 50 MB. Disable this option to allow log files to grow to any size. If the log file exceeds this size, new data replaces the oldest 25 percent of the entries in the file.</td>
</tr>
<tr>
<td><strong>Event Logging</strong></td>
<td><strong>Send events to McAfee ePO</strong></td>
<td>Sends all events logged to the <strong>Event Log</strong> on the Endpoint Security Client to McAfee ePO. This option is available on systems managed by McAfee ePO or McAfee ePO Cloud only.</td>
</tr>
<tr>
<td></td>
<td><strong>Log events to Windows Application log</strong></td>
<td>Sends all events logged to the <strong>Event Log</strong> on the Endpoint Security Client to the Windows Application log. The Windows Application log is accessible from the Windows **Event Viewer</td>
</tr>
</tbody>
</table>
### Table 6-2  Advanced options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Severity levels</strong></td>
<td></td>
<td>Specifies the severity level of events to log to the Event Log on the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Endpoint Security Client:</td>
</tr>
<tr>
<td></td>
<td>None</td>
<td>Sends no alerts</td>
</tr>
<tr>
<td></td>
<td>Critical only</td>
<td>Sends alert level 1 only</td>
</tr>
<tr>
<td></td>
<td>Major and Critical</td>
<td>Sends alert levels 1 and 2</td>
</tr>
<tr>
<td></td>
<td>Minor, Major, and Critical</td>
<td>Sends alert levels 1–3</td>
</tr>
<tr>
<td></td>
<td>All except Informational</td>
<td>Sends alert levels 1–4</td>
</tr>
<tr>
<td></td>
<td>All</td>
<td>Sends alert levels 1–5</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Major</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Minor</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Informational</td>
</tr>
<tr>
<td>Threat Prevention events to log</td>
<td></td>
<td>Specifies the severity level of events for each Threat Prevention feature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to log:</td>
</tr>
<tr>
<td></td>
<td>• Access Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Exploit Prevention</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On-Access Scanner</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On-Demand Scanner</td>
<td></td>
</tr>
<tr>
<td>Firewall events to log</td>
<td></td>
<td>Specifies the severity level of Firewall events to log.</td>
</tr>
<tr>
<td>Web Control events to log</td>
<td></td>
<td>Specifies the severity level of Web Control events to log.</td>
</tr>
<tr>
<td>Proxy Server for McAfee GTI</td>
<td>No proxy server</td>
<td>Specifies that the managed systems retrieve McAfee GTI reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>information directly over the Internet directly, not through a proxy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server. (Default)</td>
</tr>
<tr>
<td>Use system proxy settings</td>
<td></td>
<td>Specifies to use the proxy settings from the client system, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>optionally enable HTTP proxy authentication.</td>
</tr>
<tr>
<td>Configure proxy server</td>
<td></td>
<td>Customizes proxy settings.</td>
</tr>
<tr>
<td></td>
<td>• Address</td>
<td>Specifies the IP address or fully qualified domain name of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTP proxy server.</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
<td>Limits access through the specified port.</td>
</tr>
<tr>
<td></td>
<td>• Exclude these addresses</td>
<td>Don't use the HTTP proxy server for websites or IP addresses that begin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with the specified entries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click Add, then enter the address name to exclude.</td>
</tr>
<tr>
<td>Section</td>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Enable HTTP proxy authentication</td>
<td>Specifies that the HTTP proxy server requires authentication. (This option is available only when you have selected an HTTP proxy server.) Enter HTTP proxy credentials:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User name — Specifies the user account with permissions to access the HTTP proxy server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Password — Specifies the password for User name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Confirm password — Confirms the specified password.</td>
</tr>
<tr>
<td>Default Client Update</td>
<td>Enable the Update Now button in the client</td>
<td>Enables the 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can configure these settings on self- and McAfee ePO-managed systems only.</td>
</tr>
<tr>
<td></td>
<td>What to update</td>
<td>Specifies what to update when the Update Now button is clicked.</td>
</tr>
<tr>
<td></td>
<td>Security content, hotfixes, and patches</td>
<td>Updates all security content (including engine, AMCore and Exploit Prevention content), as well as any hotfixes and patches, to the latest versions.</td>
</tr>
<tr>
<td></td>
<td>Security content</td>
<td>Updates security content only (default).</td>
</tr>
<tr>
<td></td>
<td>Hotfixes and patches</td>
<td>Updates hotfixes and patches only.</td>
</tr>
<tr>
<td></td>
<td>Source Sites for Updates</td>
<td>Configures sites from which to get updates to content files and software components.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can configure these settings on self-managed systems only.</td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Adds a site to the source site list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Add or Edit source sites on page 92 for information.</td>
</tr>
<tr>
<td></td>
<td>Import</td>
<td>Imports a list of sites from an XML file.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Deletes the selected site from the source site list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can enable and disable the two default backup source sites (NAIFtp and NAIHttp), but you can’t otherwise modify, delete, or move them in the list.</td>
</tr>
<tr>
<td>Proxy server for Source Sites</td>
<td>No proxy server</td>
<td>Specifies that the managed systems retrieve McAfee GTI reputation information directly over the Internet directly, not through a proxy server. (Default)</td>
</tr>
<tr>
<td></td>
<td>Use system proxy settings</td>
<td>Specifies to use the proxy settings from the client system, and optionally enable HTTP or FTP proxy authentication.</td>
</tr>
</tbody>
</table>
### Table 6-2 Advanced options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure proxy server</td>
<td>Configure proxy server</td>
<td>Customizes proxy settings.</td>
</tr>
<tr>
<td></td>
<td>HTTP/FTP address</td>
<td>Specifies the DNS, IPv4, or IPv6 address of the HTTP or FTP proxy server.</td>
</tr>
<tr>
<td></td>
<td>Port</td>
<td>Limits access through the specified port.</td>
</tr>
<tr>
<td></td>
<td>Exclude these addresses</td>
<td>Specifies the addresses for Endpoint Security Client systems that you don't want to use the proxy server for obtaining McAfee GTI ratings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click Add, then enter the address name to exclude.</td>
</tr>
<tr>
<td></td>
<td>Enable HTTP/FTP proxy</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>proxy authentication</td>
<td>User name — Specifies the user account with permissions to access the proxy server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password — Specifies the password for the specified User name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Confirm password — Confirms the specified password.</td>
</tr>
</tbody>
</table>

See also
- Protect Endpoint Security resources on page 26
- Configure logging settings on page 26
- Configure settings for client interface security on page 27
- Configure proxy server settings for McAfee GTI on page 28
- Configure update behavior on page 29
- Configure source sites for client updates on page 29
- Add or Edit source sites on page 92

### Add or Edit source sites

Adds or edits a site in the source site list.

### Table 6-3 Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Indicates the name of the source site containing the update files.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enables or disables use of the source site for downloading update files.</td>
</tr>
<tr>
<td>Retrieve files from</td>
<td>Specifies where to retrieve the files from.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HTTP repository</td>
<td>Retrieves files from the designated HTTP repository location.</td>
</tr>
<tr>
<td></td>
<td>HTTP offers updating independent of network security, but supports higher levels of concurrent connections than FTP.</td>
</tr>
<tr>
<td>URL</td>
<td>• DNS name — Indicates that the URL is a domain name.</td>
</tr>
<tr>
<td></td>
<td>• IPv4 — Indicates that the URL is an IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>• IPv6 — Indicates that the URL is an IPv6 address.</td>
</tr>
<tr>
<td></td>
<td>http:// — Specifies the address of the HTTP server and folder where the update files are located.</td>
</tr>
<tr>
<td></td>
<td>Port — Specifies the port number for the HTTP server.</td>
</tr>
<tr>
<td>Use authentication</td>
<td>Selects to use authentication and specifies the credentials for accessing the update file folder.</td>
</tr>
<tr>
<td></td>
<td>• User name — Specifies the user account with read permissions to the update file folder.</td>
</tr>
<tr>
<td></td>
<td>• Password — Specifies the password for the specified User name.</td>
</tr>
<tr>
<td></td>
<td>• Confirm password — Confirms the specified password.</td>
</tr>
</tbody>
</table>
Table 6-3  Option definitions (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP repository</td>
<td>Retrieves files from the designated FTP repository location.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>URL</td>
<td>• DNS name — Indicates that the URL is a domain name.</td>
</tr>
<tr>
<td></td>
<td>• IPv4 — Indicates that the URL is an IPv4 address.</td>
</tr>
<tr>
<td></td>
<td>• IPv6 — Indicates that the URL is an IPv6 address.</td>
</tr>
<tr>
<td>ftp://</td>
<td>ftp:// Specifies the address of the FTP server and folder where the update files are located.</td>
</tr>
<tr>
<td>Port</td>
<td>Port Specifies the port number for the FTP server.</td>
</tr>
<tr>
<td></td>
<td>Selects to use anonymous FTP to access the update file folder.</td>
</tr>
<tr>
<td></td>
<td>Deselect this option to specify access credentials.</td>
</tr>
<tr>
<td></td>
<td>• User name — Specifies the user account with read permissions to the update file folder.</td>
</tr>
<tr>
<td></td>
<td>• Password — Specifies the password for the specified User name.</td>
</tr>
<tr>
<td></td>
<td>• Confirm password — Confirms the specified password.</td>
</tr>
<tr>
<td>UNC path or Local path</td>
<td>Retrieves files from the designated UNC or local path location.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Path</td>
<td>• UNC path — Specifies the path using UNC notation (\servername\path).</td>
</tr>
<tr>
<td></td>
<td>• Local path — Specifies the path of a folder on a local or network drive.</td>
</tr>
<tr>
<td>Use logged on account</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Domain — Specifies the domain for the user account.</td>
</tr>
<tr>
<td></td>
<td>• User name — Specifies the user account with read permissions to the update file folder.</td>
</tr>
<tr>
<td></td>
<td>• Password — Specifies the password for the specified User name.</td>
</tr>
<tr>
<td></td>
<td>• Confirm password — Confirms the specified password.</td>
</tr>
</tbody>
</table>
# Common — Tasks

Schedules Endpoint Security Client tasks.

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>Name</td>
<td>Name of the scheduled task.</td>
</tr>
<tr>
<td></td>
<td>Feature</td>
<td>Module or feature that the task is associated with.</td>
</tr>
<tr>
<td></td>
<td>Schedule</td>
<td>When the task is scheduled to run and if it's disabled.</td>
</tr>
<tr>
<td></td>
<td>Status</td>
<td>Status of the last time the task ran:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (no status) — Never run</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Running — Current running or resumed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Paused — Paused by the user (such as a scan)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deferred — Deferred by the user (such as a scan)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Finished — Completed running without errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Finished (errors) — Finished running with errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failed — Failed to complete</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deferred (errors) — Deferred running with errors</td>
</tr>
<tr>
<td></td>
<td>Last Run</td>
<td>Date and time the task last ran.</td>
</tr>
<tr>
<td>Run Now</td>
<td></td>
<td>Opens the dialog associated with the selected task.</td>
</tr>
<tr>
<td>Quick Scan</td>
<td></td>
<td>Opens the Quick Scan dialog and starts the scan.</td>
</tr>
<tr>
<td>Full Scan</td>
<td></td>
<td>Opens the Full Scan dialog and starts the scan.</td>
</tr>
<tr>
<td>Default Client Update</td>
<td></td>
<td>Opens the Update dialog and starts the update.</td>
</tr>
<tr>
<td>Delete</td>
<td></td>
<td>Deletes the selected task.</td>
</tr>
<tr>
<td>Add</td>
<td></td>
<td>Adds a new scheduled task.</td>
</tr>
</tbody>
</table>

See also
- Run a Full Scan or Quick Scan on page 34
- Update protection and software manually on page 18
- Edit Full Scan or Edit Quick Scan tasks on page 95
- Edit Default Client Update task on page 96

## Edit Full Scan or Edit Quick Scan tasks

Schedules and edits the Full Scan or Quick Scan task.

See Configure On-Demand Scan settings on page 52 for information on configuring the Full Scan and Quick Scan settings.

By default, both the Full Scan and Quick Scan are scheduled to run every day at 11:59 PM. The schedules are disabled.

You can configure these settings on self-managed systems only.
## Table 6-4

<table>
<thead>
<tr>
<th>Category</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Schedule | Enable schedule | Schedules the task to run at a specified time. (Disabled by default)  
This option must be selected to schedule the task. |
| Repeats  |              | Specifies the task frequency.                                                                                                               |
|          | Daily        | Runs the task every day at the specified **Start time**.                                                                                   |
|          | Weekly       | Runs the task weekly:  
• On the weeks specified in **Frequency**  
• On the days specified in **Runs on** |
|          | Monthly      | Runs the task monthly on either:  
• The specified day of the month  
• The specified days of the week — first, second, third, fourth, or last |
| Start time |              | Specifies the time to start the task.                                                                                                      |
|          | Run once at that time | Runs the task once at the specified **Start time**.                                                                                       |
|          | Run at that time, and then repeat until | Runs the task at the specified **Start time**. Then, it runs the task every specified number of hours/minutes until the specified end time. |
|          | Run at that time, and then repeat for | Runs the task at the specified **Start time**. Then, it runs the task every specified number of hours/minutes until it has run for the specified amount of time. |
| Timeout  | Stop this task if it runs longer than | Stops the task after the specified number of **Hours** and **Minutes**.  
If the task is interrupted before completing, the next time the task starts, it resumes where it left off. |
| Account  |              | Specifies the credentials to use for running the task.                                                                                     |
|          | User name    | Specifies the user account.                                                                                                                |
|          | Password     | Specifies the password for the specified user account.                                                                                     |
|          | Confirm password | Confirms the password for the specified user account.                                                                                      |
|          | Domain       | Specifies the domain for the specified user account.                                                                                       |

### See also
- Configure On-Demand Scan settings on page 52
- Run a Full Scan or Quick Scan on page 34
- Schedule Full Scan and Quick Scan tasks on page 56

### Edit Default Client Update task

Schedules and edits the **Default Client Update** task.  
See Configure update behavior on page 29 for information on configuring the **Default Client Update** settings.
By default, the Default Client Update task runs every day at 1:00 AM and repeats every four hours until 11:59 PM.

![Information icon] You can configure these settings on self-managed systems only.

| Table 6-5 |

<table>
<thead>
<tr>
<th>Category</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Schedule | Enable schedule | Schedules the task to run at a specified time. (Enabled by default)  
**This option must be selected to schedule the task.** |
| Repeats  |        | Specifies the task frequency.  
**Daily** Runs the task every day at the specified **Start time**.  
**Weekly** Runs the task weekly on:  
- The weeks specified in **Frequency**  
- The days specified in **Runs on**  
**Monthly** Runs the task monthly on either:  
- The specified day of the month  
- The specified days of the week — first, second, third, fourth, or last  
| Start time |        | Specifies the time to start the task.  
**Run once at that time** Runs the task once at the specified **Start time**.  
**Run at that time, and then repeat until** Runs the task at the specified **Start time**. Then, it runs the task every specified number of hours/minutes until the specified end time.  
**Run at that time, and then repeat for** Runs the task at the specified **Start time**. Then, it runs the task every specified number of hours/minutes until it has run for the specified amount of time. |
| Timeout  | Stop this task if it runs longer than | Stops the task after the specified number of **Hours** and **Minutes**.  
**If the task is interrupted before completing, the next time the task starts, it resumes where it left off.** |
| Account  |        | Specifies the credentials to use for running the task.  
**If no credentials are specified, the task runs as the local system Administrator account.** |
|          | User name | Specifies the user account. |
|          | Password  | Specifies the password for the specified user account. |
|          | Confirm password | Confirms the password for the specified user account. |
|          | Domain    | Specifies the domain for the specified user account. |

**See also**
- Configure update behavior on page 29
- Schedule the Default Client Update task on page 31
- Common — Tasks on page 95
Threat Prevention — Access Protection

Protects your system's access points based on configured rules.

See Common — Options on page 87 settings for logging configuration.

Access Protection compares a requested action against the list of configured rules and acts according to the rule.

<table>
<thead>
<tr>
<th>Table 6-6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
</tr>
<tr>
<td>ACCESS PROTECTION</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 6-7  Advanced options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
</tr>
<tr>
<td>Exclusions</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Rules</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Exclusions</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Installing new CLSIDs, APPIDs, and TYPELIBs</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Disabling Registry Editor and Task Manager</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Section</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Altering user rights policies</td>
</tr>
<tr>
<td>Altering any file extension registrations</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Remotely creating or modifying Portable Executable, .INI, .PIF file types, and core system locations</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Remotely creating autorun files</td>
</tr>
<tr>
<td>Running files from any temp folder</td>
</tr>
<tr>
<td>Executing scripts by Windows script host (CScript.exe or Wscript.exe) from any temp folder</td>
</tr>
<tr>
<td>Accessing or modifying Remote Access Phonebook files</td>
</tr>
</tbody>
</table>
### Table 6-7 Advanced options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executing and reading</td>
<td>tftp.exe</td>
<td>Prevents use of TFTP (Trivial File Transfer Protocol), a file transfer protocol with no user authentication. This rule blocks malware from using TFTP to download more malware to the system, preventing further infection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Because Windows requires access to tftp.exe when installing Windows Service Packs, disable this rule when installing patches and Service Packs.</td>
</tr>
<tr>
<td>Reading Internet Explorer</td>
<td>cached files</td>
<td>Limits access to items in the Internet Explorer cache to Internet Explorer only. This rule prevents malware from searching the Internet Explorer cache for email addresses and website passwords.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any process that uses the WinInet library or hosts an Internet Explorer control in a window can access the cache. If enabled, you might need to add processes to this rule.</td>
</tr>
<tr>
<td>Remotely accessing local</td>
<td>files or folders</td>
<td>Prevents read and write access from remote computers to the computer. This rule prevents a share-hopping worm from spreading. In a typical environment, this rule is suitable for workstations, but not servers, and is only useful when computers are actively under attack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Remotely creating or modifying files or folders</td>
<td></td>
<td>Blocks write access to all shares. This rule is useful in an outbreak by preventing write access to limit the spread of infection. The rule blocks malware that would otherwise severely limit use of the computer or network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In a typical environment, this rule is suitable for workstations, but not servers, and is only useful when computers are actively under attack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Hijacking .EXE and other</td>
<td>executable extensions</td>
<td>Protects .EXE, .BAT, and other executable registry keys under HKEY_CLASSES_ROOT. This rule prevents malware from modifying registry keys to run the virus when another executable runs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This rule is a less restrictive alternative to Altering all file extension registrations.</td>
</tr>
<tr>
<td>Executing potentially</td>
<td>malicious executables by</td>
<td>Prevents svchost.exe from loading DLLs other than Windows service .DLLs. This rule prevents malware from using svchost.exe to register .DLLs that aren't part of Windows.</td>
</tr>
<tr>
<td></td>
<td>Svchost</td>
<td></td>
</tr>
</tbody>
</table>
### Table 6-7  Advanced options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifying core Windows processes</td>
<td></td>
<td>Prevents files from being created or executed with the most commonly spoofed names. This rule prevents viruses and trojans from running with the name of a Windows process. This rule excludes authentic Windows files.</td>
</tr>
<tr>
<td>Modifying Mozilla files and settings</td>
<td></td>
<td>Blocks processes from modifying favorites and settings in Firefox. This rule prevents start-page trojans, adware, and spyware from modifying browser settings, such as changing the start page or installing favorites.</td>
</tr>
<tr>
<td>Modifying Internet Explorer settings</td>
<td></td>
<td>Blocks processes from modifying settings in Internet Explorer. This rule prevents start-page trojans, adware, and spyware from modifying browser settings, such as changing the start page or installing favorites.</td>
</tr>
<tr>
<td>Installing Browser Helper Objects or Shell Extensions</td>
<td></td>
<td>Prevents adware, spyware, and trojans that install as Browser Helper Objects from installing on to the host computer. This rule prevents adware and spyware from installing on systems.</td>
</tr>
<tr>
<td>Executing Windows Help and Support Center (HCP) URLs in Internet Explorer or Windows Media Player</td>
<td></td>
<td>Prevents Internet Explorer and Media Player from executing Help Center and Support (HCP) URLs (hcp://). This rule prevents an attacker from using an hcp:// URL to execute arbitrary code on the computer, with the user’s permissions.</td>
</tr>
<tr>
<td>Modifying Internet Explorer favorites or settings</td>
<td></td>
<td>Blocks processes from modifying Internet Explorer configurations and files. This rule prevents start-page trojans, adware, and spyware from modifying browser settings, such as changing the start page or installing favorites.</td>
</tr>
</tbody>
</table>

See also

*Configure Access Protection settings on page 43*

---

### Threat Prevention — Exploit Prevention

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

See Common — Options on page 87 settings for logging configuration.

### Table 6-8

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXPLOIT PREVENTION</td>
<td>Enable Exploit Prevention</td>
<td>Enables the Exploit Prevention feature. Failure to enable this feature leaves your system unprotected from malware attacks.</td>
</tr>
</tbody>
</table>
## Table 6-9  Advanced options

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Data Execution Prevention</td>
<td>Use Windows Data Execution Prevention</td>
<td>Enables Windows Data Execution Prevention (DEP). (Disabled by default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabling this option doesn’t affect any processes that have DEP enabled as a result of the Windows DEP policy.</td>
</tr>
<tr>
<td>Protection Level</td>
<td></td>
<td>Specifies the Exploit Prevention protection level.</td>
</tr>
<tr>
<td></td>
<td>Standard</td>
<td>Detects and blocks only high-severity buffer overflow exploits identified in the Exploit Prevention content file and stops the detected thread. Use the feature in Standard mode for a short while. Review the log file during that time to determine whether to change to Maximum protection.</td>
</tr>
<tr>
<td></td>
<td>Maximum</td>
<td>Detects and blocks high- and medium-severity buffer overflow exploits identified in the Exploit Prevention content file and stops the detected threat. This setting can result in false positives.</td>
</tr>
<tr>
<td>Exclusions</td>
<td>Exclude these processes</td>
<td>Specifies the process name that owns the writable memory that is making the call. Enter the process name to exclude. Exploit Prevention excludes the process wherever it is located.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exclusions are case-insensitive and wildcards aren’t allowed.</td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Adds a process to the exclusion list. Enter the process name or process name with its path.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Deletes the selected process from the exclusion list.</td>
</tr>
</tbody>
</table>

See also

Configure Exploit Prevention settings on page 45

### Threat Prevention — On-Access Scan

Enables and configures the on-access scan settings.

See Common — Options on page 87 settings for logging configuration.

#### Table 6-11

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON-ACCESS SCAN</td>
<td>Enable On-Access Scan</td>
<td>Enables the On-Access Scan feature. Enabled by default.</td>
</tr>
<tr>
<td></td>
<td>Enable On-Access Scan on system startup</td>
<td>Enables the On-Access Scan feature each time you start the computer. Enabled by default.</td>
</tr>
<tr>
<td></td>
<td>Specify maximum number of seconds for each file scan</td>
<td>Limits each file scan to the specified number of seconds. Enabled by default. If a scan exceeds the time limit, the scan stops cleanly and logs a message.</td>
</tr>
</tbody>
</table>
### Table 6-11 (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Scan boot sectors</td>
<td>Examines the disk boot sector. Enabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⚠️ When a disk contains a unique or abnormal boot sector that can’t be scanned, disable boot sector scanning.</td>
</tr>
<tr>
<td></td>
<td>Scan processes on enable</td>
<td>Rescans all processes that are currently in memory each time:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You disable and re-enable on-access scans.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The system starts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⚠️ Because some programs or executables start automatically when you start your system, enabling this option can slow your system and increase system startup time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When the on-access scanner is enabled, it always scans all processes when they are executed.</td>
</tr>
<tr>
<td></td>
<td>Scan trusted installers</td>
<td>Scans MSI files (installed by msiexec.exe and signed by McAfee or Microsoft) or Windows Trusted Installer service files. Disabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⚠️ Disable this option to improve the performance of large Microsoft application installers.</td>
</tr>
<tr>
<td></td>
<td>Scan when copying</td>
<td>Scans files whenever the user copies from one local folder to another.</td>
</tr>
<tr>
<td></td>
<td>between local folders</td>
<td>If this option is:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Disabled</strong> — Only items in the destination folder are scanned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Enabled</strong> — Items in both source (read) and destination (write) folders are scanned.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled by default.</td>
</tr>
</tbody>
</table>

**McAfee GTI**

See McAfee GTI on page 110 for information.

### Table 6-12  Advanced options

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Detection</td>
<td>Display the On-Access Scan page</td>
<td>Displays the On-Access Scan page with the specified message to client users when a detection occurs. Enabled by default.</td>
</tr>
<tr>
<td>User Messaging</td>
<td>when a threat is detected</td>
<td>When this option is selected, users can open this page from the Scan Now page at any time the detection list includes at least one threat.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The on-access scan detection list is cleared when the Endpoint Security service restarts or the system reboots.</td>
</tr>
<tr>
<td></td>
<td>Message</td>
<td>Specifies the message to display to client users when a detection occurs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default message is: <strong>McAfee Endpoint Security detected a threat.</strong></td>
</tr>
<tr>
<td>Processes Settings</td>
<td>Use Standard settings for all processes</td>
<td>Applies the same configured settings to all processes when performing an on-access scan.</td>
</tr>
</tbody>
</table>
### Table 6-12 Advanced options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Configure different settings for High Risk and Low Risk processes** | Configures different scanning settings for each process type that you identify.  
- Standard — Processes that aren't identified as either high risk or low risk. Enabled by default.  
- High Risk — Processes that are high risk.  
- Low Risk — Processes that are low risk. |  
| Add | Adds a process to the High Risk or Low Risk list. |  
| Delete | Removes a process from the High Risk or Low Risk list. |  

<table>
<thead>
<tr>
<th>Scanning</th>
<th>Specify when to scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>When writing to disk</td>
<td>Scans all files as they are written to or modified on the computer or other data storage device.</td>
</tr>
<tr>
<td>When reading from disk</td>
<td>Scans all files as they are read from the computer or other data storage device. McAfee strongly recommends enabling this option.</td>
</tr>
<tr>
<td>Let McAfee decide</td>
<td>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.</td>
</tr>
<tr>
<td>Do not scan when reading from or writing to disk</td>
<td>Specifies to not scan Low Risk processes only.</td>
</tr>
</tbody>
</table>
| On network drives | Scans resources on mapped network drives.  
*Scanning network resources might affect performance.* |  
| Opened for backups | Examines files that are open for backup operations. |  
| File types to scan |  
| All files | Scans all files, regardless of extension. McAfee strongly recommends enabling this option.  
*Failure to enable this option leaves your system unprotected from malware attacks.* |  
| Default and specified file types | Scans:  
- Default list of extensions in the current AMCore content file.  
- (Optional) Known macro threats.  
- Any additional extensions that you specify.  
- (Optional) Files with no extension. |  
| Specified file types only | Scans only files with the extensions that you specify, and optionally, files with no extension. |  

<table>
<thead>
<tr>
<th>Specify what to scan</th>
</tr>
</thead>
</table>
| Compressed archive files | Examines the contents of archive (compressed) files, including .jar files.  
Because scanning compressed files negatively affect system performance, McAfee recommends scanning inside archives when the system isn't in use. |  
| Compressed MIME-encoded files | Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files. |
### Table 6-12 Advanced options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect unwanted</td>
<td>programs</td>
<td>Specifies that the on-access scanner detects potentially unwanted programs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The scanner uses the information you configured in the Options settings to detect potentially unwanted programs.</td>
</tr>
<tr>
<td>Actions</td>
<td></td>
<td>See Actions on page 111 for information.</td>
</tr>
<tr>
<td>Exclusions</td>
<td></td>
<td>Specifies files, folders, and drives to exclude from scanning. See Add or Edit exclusions on page 112 for information.</td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Adds an item to the Default, High Risk, or Low Risk exclusion list.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes an item from the Default, High Risk, or Low Risk exclusion list.</td>
</tr>
<tr>
<td>ScriptScan</td>
<td>Enable ScriptScan</td>
<td>Enables scanning JavaScript and VBScript scripts to prevent unwanted scripts from executing. Enabled by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You must restart Internet Explorer after enabling ScriptScan for it to detect malicious scripts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deselect this option to enable the client computer to use both the exclusions specified here and the exclusions that are specified locally on the client.</td>
</tr>
<tr>
<td>Exclude these URLs</td>
<td></td>
<td>Specifies ScriptScan exclusions by URL.</td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Adds a URL to the exclusion list.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes a URL from the exclusion list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="http://weather.msn.com">http://weather.msn.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="http://music.msn.com">http://music.msn.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>On Windows Server 2008, ScriptScan URL exclusions don't work with Windows Internet Explorer unless you select Enable third-party browser extensions and restart the system. For details, see the ScriptScan URL exclusions KB article.</td>
</tr>
</tbody>
</table>

**See also**
- Configure On-Access Scan settings on page 47
- McAfee GTI on page 110
- Actions on page 111
- Add or Edit exclusions on page 112
Threat Prevention — On-Demand Scan

Configures the On-Demand Scan settings for the preconfigured scans that run on your system.

See Common — Options on page 87 settings 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.
- Right-click a file or folder and select Scan for threats from the pop-up menu.

### Table 6-14

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan type</td>
<td>Scan boot sectors</td>
<td>Examines the disk boot sector. When a disk contains a unique or abnormal boot sector that can’t</td>
</tr>
<tr>
<td></td>
<td></td>
<td>be scanned, you might choose to disable boot sector scanning.</td>
</tr>
<tr>
<td>Detect unwanted programs</td>
<td></td>
<td>Enables the scanner to detect potentially unwanted programs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The scanner uses the information you configured in the Common settings to detect potentially unwanted programs.</td>
</tr>
<tr>
<td>Decode MIME-encoded files</td>
<td></td>
<td>Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.</td>
</tr>
<tr>
<td>Scan inside archives</td>
<td></td>
<td>Examines the contents of archive (compressed) files, including .jar files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Because scanning compressed files can negatively affect system performance, McAfee recommends using this option in scans during off hours when the system isn't being used.</td>
</tr>
<tr>
<td>Scan files that have been migrated to storage</td>
<td></td>
<td>Scans files that Remote Storage manages. When the scanner encounters a file with migrated content, it restores the file to the local system before scanning.</td>
</tr>
<tr>
<td>Find unknown program threats</td>
<td></td>
<td>Uses McAfee GTI to detect executable files that have code resembling malware.</td>
</tr>
<tr>
<td>Find unknown macro threats</td>
<td></td>
<td>Uses McAfee GTI to detect unknown macro viruses.</td>
</tr>
<tr>
<td>Scan subfolders</td>
<td></td>
<td>Examines all subfolders of the specified folder.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This option applies to the Right-Click Scan settings only.</td>
</tr>
<tr>
<td>Scan Locations</td>
<td></td>
<td>See Scan Locations on page 108 for information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>These options apply to Full Scan and Quick Scan only.</td>
</tr>
<tr>
<td>File Types to Scan</td>
<td>All files</td>
<td>Scans all files, regardless of extension. McAfee strongly recommends enabling All files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure to enable this option leaves your system unprotected from malware attacks.</td>
</tr>
</tbody>
</table>
## Table 6-14  (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default and specified</td>
<td>Scans:</td>
<td>• Default list of extensions in the current AMCore content file.</td>
</tr>
<tr>
<td>file types</td>
<td></td>
<td>• (Optional) Known macro threats.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Any additional extensions that you specify.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Optional) Files with no extension.</td>
</tr>
<tr>
<td>Specified file types</td>
<td>Scans only files with the extensions that you</td>
<td>Specify files, folders, and drives to exclude from scanning. See Add or Edit exclusions on page 112 for information.</td>
</tr>
<tr>
<td>only</td>
<td>specify, and optionally, files with no</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extension.</td>
<td></td>
</tr>
<tr>
<td>McAfee GTI</td>
<td>See McAfee GTI on page 110 for information.</td>
<td></td>
</tr>
<tr>
<td>Exclusions</td>
<td>Specifying files, folders, and drives to</td>
<td>Specifies files, folders, and drives to exclude from scanning. See Add or Edit exclusions on page 112 for information.</td>
</tr>
<tr>
<td></td>
<td>exclude from scanning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Adds an item to the exclusion list.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes an item from the exclusion list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the item in the table, then click Delete.</td>
</tr>
<tr>
<td>Actions</td>
<td>See Actions on page 111 for information.</td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td>Use the scan cache</td>
<td>Enables the scanner to use the existing clean scan results. Select this option to reduce duplicate scanning and improve performance.</td>
</tr>
<tr>
<td>System utilization</td>
<td>Enabling the operating system to specify the</td>
<td>Enables the operating system to specify the amount of CPU time that the scanner receives during the scan.</td>
</tr>
<tr>
<td></td>
<td>amount of CPU time</td>
<td>Each task runs independently, unaware of the limits for other tasks.</td>
</tr>
<tr>
<td></td>
<td>Enables the scan to complete faster.</td>
<td>Enables the scan to complete faster. Select this option for systems that have large volumes and little end-user activity.</td>
</tr>
<tr>
<td></td>
<td>Below normal</td>
<td>Sets the system utilization for the scan to the McAfee ePO default.</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Provides improved performance for other running applications.</td>
</tr>
<tr>
<td>Scheduled Scan Options</td>
<td>These options apply to <strong>Full Scan</strong> and <strong>Quick Scan</strong> only.</td>
<td>These options apply to <strong>Full Scan</strong> and <strong>Quick Scan</strong> only.</td>
</tr>
</tbody>
</table>

---

**Notes:**
- Each task runs independently, unaware of the limits for other tasks.
- Enables the scan to complete faster. Select this option for systems that have large volumes and little end-user activity.
- Sets the system utilization for the scan to the McAfee ePO default.
- Provides improved performance for other running applications. Select this option for systems with end-user activity.
### Table 6-14 (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan only when the system is idle</td>
<td>Runs the scan only when the system is idle. 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.</td>
<td>McAfee recommends disabling 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.</td>
</tr>
<tr>
<td>Scan anytime</td>
<td>Runs the scan even if the user is active and specifies options for the scan.</td>
<td></td>
</tr>
<tr>
<td>User can defer scans</td>
<td>Allows the user to defer scheduled scans, and specifies options for scan deferral.</td>
<td></td>
</tr>
<tr>
<td>Maximum number of times user can defer for one hour</td>
<td>Specifies the number of times (1–23) that the user can defer the scan for one hour.</td>
<td></td>
</tr>
<tr>
<td>User message</td>
<td>Specifies the message to display when a scan is about to start. The default message is: McAfee Endpoint Security is about to scan your system.</td>
<td></td>
</tr>
<tr>
<td>Message duration (seconds)</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Do not scan when the system is in presentation mode</td>
<td>Postpones the scan while the system is presentation mode.</td>
<td></td>
</tr>
<tr>
<td>Do not scan when the system is on battery power</td>
<td>Postpones the scan when the system is using battery power.</td>
<td></td>
</tr>
</tbody>
</table>

#### See also
- Configure On-Demand Scan settings on page 52
- Run a Full Scan or Quick Scan on page 34
- Scan a file or folder on page 36
- Scan Locations on page 108
- McAfee GTI on page 110
- Actions on page 111
- Add or Edit exclusions on page 112

### Scan Locations

Specifies the locations to scan.

> These options apply to Full Scan and Quick Scan only.
Table 6-15

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Locations</td>
<td>Scan subfolders</td>
<td>Examines all subfolders in the specified volumes when any of these options are selected:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Home folder</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User profile folder</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Program files folder</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deselect this option to scan only the root level of the volumes.</td>
</tr>
<tr>
<td></td>
<td>Specify locations</td>
<td>Specifies the locations to scan.</td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Adds a location to the scan. Click Add, then select the location from the drop-down.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes a location from the scan. Select the location and click Delete.</td>
</tr>
<tr>
<td>Memory for rootkits</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure to enable this option leaves your system unprotected from malware attacks.</td>
</tr>
<tr>
<td>Running processes</td>
<td></td>
<td>Scans the memory of all running processes. Actions other than Clean files are treated as Continue scanning.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Failure to enable this option leaves your system unprotected from malware attacks.</td>
</tr>
<tr>
<td>Registered files</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>My computer</td>
<td></td>
<td>Scans all drives physically attached to your computer or logically mapped to a drive letter on your computer.</td>
</tr>
<tr>
<td>All local drives</td>
<td></td>
<td>Scans all drives and their subfolders on the computer.</td>
</tr>
<tr>
<td>All fixed drives</td>
<td></td>
<td>Scans all drives physically connected to the computer.</td>
</tr>
<tr>
<td>All removable drives</td>
<td></td>
<td>Scans all removable drives or other storage devices connected to the computer.</td>
</tr>
<tr>
<td>All mapped drives</td>
<td></td>
<td>Scans network drives logically mapped to a network drive on the computer.</td>
</tr>
<tr>
<td>Home folder</td>
<td></td>
<td>Scans the home folder of the user who starts the scan.</td>
</tr>
<tr>
<td>User profile folder</td>
<td></td>
<td>Scans the profile of the user who starts the scan, including the user’s My Documents folder.</td>
</tr>
<tr>
<td>Windows folder</td>
<td></td>
<td>Scans the contents of the Windows folder.</td>
</tr>
<tr>
<td>Program Files folder</td>
<td></td>
<td>Scans the contents of the Program Files folder.</td>
</tr>
<tr>
<td>Temp folder</td>
<td></td>
<td>Scans the contents of the Temp folder.</td>
</tr>
<tr>
<td>Recycle bin</td>
<td></td>
<td>Scans the contents of the recycle bin.</td>
</tr>
<tr>
<td>File or folder</td>
<td></td>
<td>Scans the specified file or folder.</td>
</tr>
</tbody>
</table>
McAfee GTI

Enables and configures McAfee GTI settings.

### Table 6-16

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Enable McAfee GTI** |                         | Enables and disables heuristic checks.  
- When enabled, fingerprints of samples, or hashes, are submitted to McAfee Labs to determine if they are malware. By submitting hashes, detection might be made available sooner than the next AMCore content file release, when McAfee Labs publishes the update.  
- When disabled, no fingerprints or data is submitted to McAfee Labs. |
| **Sensitivity level** |                         | Configures the sensitivity level to use when determining if a detected sample is malware.  
The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections might result in more false positive results. |
| **Risk level**    |                         |                                                                                                                                                                                                                                                                                                                                 |
### Actions

Specifies how the scanner responds when it detects a threat.

**Table 6-17**

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
<th>On-Access Scan</th>
<th>On-Demand Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat detection first response</td>
<td>Deny access to files</td>
<td>Prevents users from accessing any files with potential threats.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continue scanning</td>
<td>Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Clean files</td>
<td>Removes the threat from the detected file, if possible.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Delete files</td>
<td>Deletes files with potential threats.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>If first response fails</td>
<td>Deny access to files</td>
<td>Prevents users from accessing files with potential threats.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Continue scanning</td>
<td>Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Delete files</td>
<td>Deletes files with potential threats.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unwanted program first response</td>
<td>Deny access to files</td>
<td>Prevents users from accessing files with potential threats.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Allow access to files</td>
<td>Allows users to access files with potential threats.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Continue scanning</td>
<td>Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Clean files</td>
<td>Removes the threat from the potentially unwanted program file, if possible.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Delete files</td>
<td>Deletes potentially unwanted program files.</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

*This option is available only if Detect unwanted programs is selected.*

---

**See also**

*Threat Prevention — On-Access Scan on page 102*

*Threat Prevention — On-Demand Scan on page 106*

*Web Control — Options on page 122*
Table 6-17 (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
<th>On-Access Scan</th>
<th>On-Demand Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>If first response fails</td>
<td>Deny access to files</td>
<td>Prevents users from accessing files with potential threats.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allow access to files</td>
<td>Allows users to access files with potential threats.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Continue scanning</td>
<td>Continues scanning files when a threat is detected. The scanner doesn't move items to the quarantine.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Delete files</td>
<td>Deletes potentially unwanted program files automatically.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See also

- Threat Prevention — On-Access Scan on page 102
- Threat Prevention — On-Demand Scan on page 106

---

Add or Edit exclusions

Adds or edits an exclusion definition.

Table 6-18

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
<th>On-Access Scan</th>
<th>On-Demand Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>What to exclude</td>
<td>Pattern</td>
<td>Specifies the pattern to exclude.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>File type</td>
<td>Specifies file types (file extensions) to exclude.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>File age</td>
<td>Specifies the access type (Modified, Accessed, or Created) of files to exclude and the Minimum age in days.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>When to exclude</td>
<td>When writing to or reading from disk</td>
<td>Excludes from scanning when files are being written to or read from disk or other data storage device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>When reading from disk</td>
<td>Excludes from scanning when files are being read from the computer or other data storage device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>When writing to disk</td>
<td>Excludes from scanning when files are being written to or modified on the disk or other data storage device.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Threat Prevention — Options

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

See Common — Options on page 87 settings for logging configuration.

This section includes only Advanced options.

Table 6-19

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine Manager</td>
<td>Quarantine directory</td>
<td>Specifies the location for the quarantine folder or accepts the default location: c:\Quarantine</td>
</tr>
<tr>
<td></td>
<td>Specify the maximum number of days to keep quarantine data</td>
<td>Specifies the number of days (1–999) to keep the quarantined items before automatically deleting. The default is 30 days.</td>
</tr>
<tr>
<td>Exclusion by Detection Name</td>
<td>Exclude these detection names</td>
<td>Specifies detection exclusions by detection name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, to specify that the on-access scanner and on-demand scanner not detect Installation Check threats, enter Installation Check.</td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Adds a detection name to the exclusion list.</td>
</tr>
<tr>
<td></td>
<td>Click Add, then enter the detection name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes a detection name from the exclusion list.</td>
</tr>
<tr>
<td></td>
<td>Select the name, then click Delete</td>
<td></td>
</tr>
<tr>
<td>Potentially Unwanted Program Detections</td>
<td>Exclude custom unwanted programs</td>
<td>Specifies individual files or programs to treat as potentially unwanted programs.</td>
</tr>
<tr>
<td></td>
<td>Add</td>
<td>Defines a custom unwanted program.</td>
</tr>
<tr>
<td></td>
<td>Click Add, enter the name, then press Tab to enter the description.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name — Specifies the file name of the potentially unwanted program.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description — Specifies the information to display as the detection name when a detection occurs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes a potentially unwanted program from the list.</td>
</tr>
<tr>
<td></td>
<td>Select the program in the table, then click Delete.</td>
<td></td>
</tr>
</tbody>
</table>
See also
Configure common scan settings on page 56

Roll Back AMCore Content
Changes the AMCore content to a previous version.

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

See also
Change the AMCore content version on page 23

Firewall — Options
Enables and disables the Firewall module and sets protection options.

See Common — Options on page 87 settings for logging configuration.

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

Table 6-21

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Enable Firewall</td>
<td>Enables and disables the Firewall module.</td>
</tr>
<tr>
<td>Options</td>
<td>Allow traffic for unsupported protocols</td>
<td>Allows all traffic that uses unsupported protocols. When disabled, all traffic using unsupported protocols is blocked.</td>
</tr>
<tr>
<td></td>
<td>Allow only outgoing traffic until firewall services have started</td>
<td>Allows outgoing traffic but no incoming traffic until the Firewall service starts. If this option disabled, Firewall allows all traffic before services are started.</td>
</tr>
<tr>
<td></td>
<td>Allow bridged traffic</td>
<td>Allows traffic with a local MAC address. The MAC address is an address in the list of VMs that Firewall supports, not the local system’s MAC address. Use this option to allow traffic through a bridged environment with virtual machines.</td>
</tr>
<tr>
<td></td>
<td>Enable IP spoof protection</td>
<td>Blocks network traffic from non-local host IP addresses or from local processes that attempt to spoof their IP address.</td>
</tr>
</tbody>
</table>
### Table 6-21  (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable firewall intrusion alerts</td>
<td>Displays alerts automatically when Firewall detects a potential attack.</td>
</tr>
<tr>
<td>DNS Blocking</td>
<td>Domain name</td>
<td>Defines domain names to block.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Add</strong> Adds a domain name to the blocked list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use the * and ? wildcards. For example, <code>*domain.com</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Separate multiple domains with a comma (,) or a carriage return.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Info] Any duplicate entries are removed automatically.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Delete</strong> Removes the selected domain name from the blocked list.</td>
</tr>
</tbody>
</table>

### Table 6-22  Advanced options

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuning Options</td>
<td>Enable Adaptive mode</td>
<td>Creates rules automatically to allow traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Warning] Enable this option temporarily while tuning a deployment.</td>
</tr>
<tr>
<td>Log all blocked traffic</td>
<td>Logs all blocked traffic (FirewallEventMonitor.log) on the Endpoint Security Client. (Enabled by default)</td>
<td></td>
</tr>
<tr>
<td>Log all allowed traffic</td>
<td>Logs all allowed traffic (FirewallEventMonitor.log) on the Endpoint Security Client. (Disabled by default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Warning] Enabling this option might negatively impact performance.</td>
</tr>
<tr>
<td>McAfee GTI Network Reputation</td>
<td>Send McAfee GTI events to Server</td>
<td>Sends events to the McAfee ePO server if the McAfee GTI block threshold setting for incoming or outgoing traffic matches. (Disabled by default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Info] Any IP address for a trusted network is excluded from McAfee GTI lookup.</td>
</tr>
</tbody>
</table>
Table 6-22  Advanced options (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incoming/Outgoing network-reputation threshold</td>
<td>Specifies the McAfee GTI rating threshold for blocking incoming or outgoing traffic from a network connection.</td>
</tr>
<tr>
<td></td>
<td>Do not block</td>
<td>This site is a legitimate source or destination of content/traffic.</td>
</tr>
<tr>
<td></td>
<td>High Risk</td>
<td>This source/destination sends or hosts potentially malicious content/traffic that McAfee considers risky.</td>
</tr>
<tr>
<td></td>
<td>Medium Risk</td>
<td>This source/destination shows behavior that McAfee considers suspicious. Any content/traffic from the site requires special scrutiny.</td>
</tr>
<tr>
<td></td>
<td>Unverified</td>
<td>This site appears to be a legitimate source or destination of content/traffic, but also displays properties suggesting that further inspection is necessary.</td>
</tr>
</tbody>
</table>

Stateful Firewall

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Number of seconds (1-240) before TCP connections time out</td>
<td>Specifies the time, in seconds, that an unestablished TCP connection remains active if no more packets matching the connection are sent or received. The default number is 30; the valid range is 1–240.</td>
</tr>
<tr>
<td></td>
<td>Number of seconds (1-300) before UDP and ICMP echo virtual connections time out</td>
<td>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 default number is 30; the valid range is 1–300.</td>
</tr>
</tbody>
</table>

See also
Configure Firewall options on page 60

Firewall — Rules

Manages firewall rules and groups.

You can add and delete rules and groups in the User added group only.

Table 6-23

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RULES</td>
<td>Add Rule</td>
<td>Adds a firewall rule.</td>
</tr>
<tr>
<td></td>
<td>See Add or Edit rules and groups on page 117 for information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add Group</td>
<td>Adds a firewall group.</td>
</tr>
<tr>
<td></td>
<td>Duplicate</td>
<td>Creates a copy of the selected item.</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>Removes a selected firewall item.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

See also
Create and manage Firewall rules and groups on page 67
Add or Edit rules and groups on page 117
Add or Edit rules and groups

Adds or edits firewall rules and groups.

**Table 6-24**

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
<th>Rule</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Name</td>
<td>Specifies the descriptive name of the item (required).</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Status</td>
<td></td>
<td>Enables or disables the item.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Specify actions</td>
<td>Allow — Allows traffic through the firewall if the item is matched.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Block — Stops traffic from passing through the firewall if the item is matched.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Treat match as intrusion — Treats traffic that matches the rule as an attack and generates an event that is sent to the McAfee ePO server. The Block action for the rule must be selected for an event to be generated.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Log matching traffic</td>
<td>Preserves a record of matching traffic in the Firewall activity log on the Endpoint Security Client.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Direction</td>
<td></td>
<td>Specifies the direction:</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In — Monitors incoming traffic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Out — Monitors outgoing traffic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Either — Monitors both incoming and outgoing traffic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td>Provides more information about the item.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Location</td>
<td>Enable location awareness</td>
<td>Enables or disables location information for the group.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Specifies the name of the location (required).</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Enable connection isolation</td>
<td>Blocks traffic on network adapters that don't match the group when an adapter is present that does match the group.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Settings for Transport and Executables aren't available for connection isolation groups.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Require that ePolicy Orchestrator be reachable</td>
<td>Enables the group to match only if there is communication with the McAfee ePO server and the FQDN of the server has been resolved.</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Table 6-24 (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
<th>Rule</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location criteria</td>
<td>Connection-specific DNS suffix</td>
<td>Specifies a connection-specific DNS suffix in the format: example.com.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default gateway</td>
<td>Specifies a single IP address for a default gateway in IPv4 or IPv6 format.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP server</td>
<td>Specifies a single IP address for a DHCP server in IPv4 or IPv6 format.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DNS server</td>
<td>Specifies a single IP address for a domain name server in IPv4 or IPv6 format.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Primary WINS</td>
<td>Specifies a single IP address for a primary WINS server in IPv4 or IPv6 format.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secondary WINS</td>
<td>Specifies a single IP address for a secondary WINS server in IPv4 or IPv6 format.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Domain reachability</td>
<td>Checks whether the specified domain is reachable.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For example:
- **IPv4** — 123.123.123.123

<table>
<thead>
<tr>
<th>Registry key</th>
<th>Specifies the registry key and key value.</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 In the first field, specify the registry key in the format: &lt;ROOT&gt;&lt;KEY&gt;[VALUE_NAME]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &lt;ROOT&gt; — Must use the full root name, such as HKEY_LOCAL_MACHINE, and not the shortened HKLM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &lt;KEY&gt; — Is the key name under the root.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• [VALUE_NAME] — is the name of the key value. If no value name is included, it is assumed to be the default value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 In the second field after the equal sign, enter the data for the key value.</td>
<td></td>
</tr>
</tbody>
</table>

To copy a registry key for pasting, right-click a key in the Registry Editor (run regedit) and select Copy Key Name.

<table>
<thead>
<tr>
<th>Networks</th>
<th>Specifies the network host options that apply to the item.</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network protocol</td>
<td>Specifies the network protocol that applies to the item.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Any protocol</td>
<td>Allows both IP and non-IP protocols.</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

If a transport protocol or an application is specified, only IP protocols are allowed.
<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
<th>Rule</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP protocol</td>
<td>Excludes non-IP protocols.</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>• IPv4 protocol</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IPv6 protocol</td>
<td>If neither checkbox is selected, any IP protocol applies. Both IPv4 and IPv6 can be selected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-IP protocol</td>
<td>Includes non-IP protocols only.</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>• Select etherType from list</td>
<td>— Specifies an etherType.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Specify custom etherType</td>
<td>— Specifies the four-characters of the hexadecimal etherType value of the non-IP protocol. See Ethernet Numbers for etherType values. For example, enter 809B for AppleTalk, 8191 for NetBEUI, or 8037 for IPX.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection types</td>
<td>Indicates if one or all connection types apply:</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>• Wired</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Wireless</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual</td>
<td>A Virtual connection type is an adapter presented by a VPN or a virtual machine application, such as VMware, rather than a physical adapter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specify the networks that apply to the item.</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>• Add — Creates and adds a network.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>See Add networks on page 121 for information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Import — Imports a list of network names from an XML file.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Delete — Removes the network from the list.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>Specifies transport options that apply to the item.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 6-24  (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>protocol</td>
<td>Specifies the transport protocol associated with the item.</td>
</tr>
<tr>
<td></td>
<td>All protocols</td>
<td>Allows IP, non-IP, and unsupported protocols.</td>
</tr>
<tr>
<td></td>
<td>TCP and UDP</td>
<td>Select from the drop-down:</td>
</tr>
<tr>
<td></td>
<td>Local port</td>
<td>Specifies the local traffic service or port to which the item applies.</td>
</tr>
<tr>
<td></td>
<td>Remote port</td>
<td>Specifies the traffic service or port on another computer to which the item applies.</td>
</tr>
<tr>
<td></td>
<td>All protocols</td>
<td>Allows IP, non-IP, and unsupported protocols.</td>
</tr>
<tr>
<td>ICMP and</td>
<td>ICMP and ICMPv6</td>
<td>In the Message type drop-down, specify an ICMP message type:</td>
</tr>
<tr>
<td>ICMPv6</td>
<td></td>
<td>• ICMP</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>Selects from a list of less common protocols.</td>
</tr>
</tbody>
</table>

**Executables**

- **Add** — Creates and adds an executable.
- **Import** — Imports a list of executable names from an XML file.
- **Delete** — Removes an executable from the list.

See also

Create and manage Firewall rules and groups on page 67
Add networks on page 121
Add or Edit executables on page 120

Add or Edit executables

Adds and edits an executable associated with a rule or group, or adds an executable to the Firewall Catalog.

Table 6-25

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name that you call the executable.</td>
</tr>
<tr>
<td>File path</td>
<td>Specifies the file path to the executable to add or edit. Click Browse to select the executable.</td>
</tr>
</tbody>
</table>

The file path can include wildcards.
### Table 6-25 (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
<th>Rule</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>File description</td>
<td>Indicates the description of the file.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>This field is populated automatically when you select an executable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Indicates the MD5 hash of the process.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>This field is populated automatically when you select an executable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable digital signature check</td>
<td>Enables or disables the digital signature check that guarantees code hasn't been altered or corrupted since it was signed with a cryptographic hash. If enabled, specify:</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>• Allow any signature — Allows files signed by any process signer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Signed by — Allows only files signed by the specified process signer.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Add networks

Adds or edits a network associated with a rule or group, or adds a network to the Firewall Catalog.

### Table 6-26

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
<th>Rule</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the network address name (required).</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Type</td>
<td>Selects either:</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>• Local network — Creates and adds a local network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote network — Creates and adds a remote network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Adds a network type to the network list.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected item.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Network type</td>
<td>Specifies the origin or destination of traffic. Select from the Address type drop-down list. See Address type on page 122 for the list of address types.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Address</td>
<td>Specifies the IP address to add to the network.</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

*Wildcards are valid.*

### See also

Address type on page 122
**Address type**

Specifies the address type.

**Table 6-27 Option definitions**

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single IP</td>
<td>Specifies a particular IP address. For example:</td>
</tr>
<tr>
<td></td>
<td>• IPv4 — 123.123.123.123</td>
</tr>
<tr>
<td></td>
<td>• IPv6 — 2001:db8::c0fa:f340:9219:bd20:9832:0ac7*</td>
</tr>
<tr>
<td>Subnet</td>
<td>Specifies the subnet address of any adapter on the network. For example:</td>
</tr>
<tr>
<td></td>
<td>• IPv4 — 123.123.123.0/24</td>
</tr>
<tr>
<td></td>
<td>• IPv6 — 2001:db8::0/32</td>
</tr>
<tr>
<td>Local subnet</td>
<td>Specifies the subnet address of the local adapter.</td>
</tr>
<tr>
<td>Range</td>
<td>Specifies a range of IP addresses. Enter the starting point and ending point of the range. For example:</td>
</tr>
<tr>
<td></td>
<td>• IPv4 — 123.123.1.0 — 123.123.255.255</td>
</tr>
<tr>
<td>Fully qualified domain name</td>
<td>Specifies the FQDN. For example, <a href="http://www.example.com">www.example.com</a>.</td>
</tr>
</tbody>
</table>

**Web Control — Options**

Configures general Web Control settings, which includes enabling, specifying action enforcement, Secure Search, and email annotations.

- **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)
  - Use this option to resolve third-party compatibility issues.

- **Event Logging**
  - **Log web categories for green rated sites**
    - Logs content categories for all green-rated sites.

  **Important**
  - 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.

---

*See Common — Options on page 87 settings for logging configuration.*
<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Enforcement</td>
<td>Apply this action to sites not yet verified by McAfee GTI</td>
<td>Specifies the default action to apply to sites that McAfee GTI hasn't yet rated. Use settings in Enforcement Messaging to customize the message.</td>
</tr>
<tr>
<td></td>
<td>Allow</td>
<td>Permits users to access the site.</td>
</tr>
<tr>
<td></td>
<td>Warn</td>
<td>Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before continuing.</td>
</tr>
<tr>
<td></td>
<td>Block</td>
<td>Prevents users from accessing the site and displays a message that the site download is blocked.</td>
</tr>
<tr>
<td>Enable HTML iFrames support</td>
<td>Blocks access to malicious (Red) and warn (Yellow) sites that appear in an HTML iframe. (Enabled by default)</td>
<td></td>
</tr>
<tr>
<td>Block sites by default if McAfee GTI ratings server is not reachable</td>
<td>Blocks access to websites by default if Web Control can't reach the McAfee GTI server.</td>
<td></td>
</tr>
<tr>
<td>Block phishing pages for all sites</td>
<td>Blocks all phishing pages, overriding content ratings actions. (Enabled by default)</td>
<td></td>
</tr>
<tr>
<td>Enable file scanning for file downloads</td>
<td>Scans all files (including .zip files) before downloading. (Enabled by default) This option prevents users from accessing a downloaded file until Threat Prevention marks the file as clean. Downloaded files are sent to Threat Prevention for scanning. Threat Prevention performs a McAfee GTI lookup on the file. If a downloaded file is detected as a threat, Endpoint Security takes action on the file and alerts the user.</td>
<td></td>
</tr>
<tr>
<td>Specify McAfee GTI risk level to block</td>
<td>Specifies the McAfee GTI risk level to block when the Threat Prevention on-demand scan feature isn't installed and enabled. See McAfee GTI on page 110 for information. Web Control uses the risk level to calculate the score when retrieving the checksum reputation from McAfee GTI.</td>
<td></td>
</tr>
<tr>
<td>Private IP Range</td>
<td>Configures Web Control to not rate or act on the specified private IP address range. Add</td>
<td>Adds a private IP address to the list of addresses to exclude from rating or blocking. Delete Deletes an IP address from the list of addresses to exclude from rating or blocking.</td>
</tr>
<tr>
<td>Secure Search</td>
<td>Enable Secure Search</td>
<td>Enables Secure Search, automatically blocking malicious sites in search results based on safety rating.</td>
</tr>
</tbody>
</table>
Table 6-28 (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
|                                      | Set the default search engine in supported browsers                    | Specifies the default search engine to use for supported browsers:  
|                                      |                                                                        | • Yahoo  
|                                      |                                                                        | • Google  
|                                      |                                                                        | • Bing  
|                                      |                                                                        | • Ask  
|                                      | Block links to risky sites in search results                           | Prevents users from clicking links to risky sites in search results.                                                                                                                                 |

Table 6-29 Advanced options

<table>
<thead>
<tr>
<th>Section</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Annotations</td>
<td>Enable annotations in browser-based email</td>
<td>Annotates URLs in browser-based email clients, such as Yahoo Mail and Gmail.</td>
</tr>
<tr>
<td></td>
<td>Enable annotations in non browser-based email</td>
<td>Annotates URLs in 32-bit email management tools, such as Microsoft Outlook or Outlook Express.</td>
</tr>
</tbody>
</table>

See also

Configure Web Control options on page 79
McAfee GTI on page 110

Web Control — Content Actions

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

ℹ️ For sites and file downloads in the unblocked categories, Web Control applies the rating actions.
### Table 6-31  
**Section** | **Option** | **Definition**  
--- | --- | ---  
Rating Actions | Rating actions for sites | Specifies actions for sites that are rated red, yellow, or unrated. Green-rated sites and downloads are allowed automatically.  
| Allow | Permits users to access the site. (Default for Unrated sites)  
| Warn | Displays a warning to notify users of potential dangers associated with the site. Users must dismiss the warning before canceling or proceeding to the site. (Default for Yellow sites)  
| Block | Prevents users from accessing the site and displays a message that the site is blocked. (Default for Red sites)  
Rating actions for file downloads | Specifies actions for file downloads that are rated red, yellow, or unrated.  
| Allow | Permits users to proceed with the download. (Default for Unrated sites)  
| Warn | Displays a warning to notify users of potential dangers associated with the download file. Users must dismiss the warning before ending or proceeding with the download. (Default for Yellow sites)  
| Block | Prevents users from downloading the file and displays a message that the download is blocked. (Default for Red sites)  
Use settings in Enforcement Messaging to customize the message.  

### Table 6-32  Advanced options  
**Section** | **Option** | **Definition**  
--- | --- | ---  
Web Category Blocking | Enable web category blocking | Enables blocking sites based on content category. The first 7 categories are considered high risk and are enabled by default. Subsequent categories appear in alphabetical order and are disabled by default.  
| 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, from highest to lowest risk.  

**See also**  
*Specify rating actions and block site access based on web category on page 82*  
*Using safety ratings to control access on page 83*  
*Using web categories to control access on page 82*
## Index

### A

**About page** 8, 17  
access modes, Endpoint Security Client 12  
Access Protection  
  about 44  
  configuring 43  
  examples 45  
  log files 20  
  processes, including and excluding 43  
Action menu, about 11  
actions, Threat Prevention  
  enabling users to clean and delete infected files 47, 52  
  performing on quarantined items 37  
  specifying what happens when threat is found 47, 52  
  unwanted programs 42  
active mode FTP protocol 70  
activity logs, Endpoint Security Client 20  
Adaptive mode  
  configuring in Firewall 60  
  rule precedence 62  
Adaptive rules group 67  
Administrator Log On page  
  unlocking the client interface 22  
  when opening Endpoint Security Client 15  
administrators  
  default password 11  
  defined 8  
  logging on to Endpoint Security Client 22  
  password 22  
adware, about 39  
alerts, Firewall 10  
alerts, Threat Prevention  
  on-access scan overview 47  
  on-demand scan overview 52  
AMCore content files  
  about 8  
  about signatures and updates 9  
  changing version 23  
  Extra.DAT files 24  
  on-access scan overview 47  
  on-demand scan overview 52  
apps, Windows Store 47, 52  
archives, specifying scan options 47, 52  
Ask search engine, and safety icons 75  
attacks, buffer overflow exploits 46

### B

backups, specifying scan options 47, 52  
balloons, Web Control 75, 77  
Bing search engine, and safety icons 75  
boot sectors, scanning 47, 52  
browsers  
  disabling Web Control plug-in 79  
  displaying Web Control menu options 77  
  supported 73, 77  
  troubleshooting communication problems 78  
buffer overflow exploits, about 46  
business  
  Scan Now 34  
  View Detections 37  
  View Scan 34  
business, Web Control buttons 74

### C

cache, global scan  
  on-access scans 47  
  on-demand scans 52  
Chrome  
  displaying Web Control menu options 77  
  supported browsers 73, 77  
  Web Control buttons 74  
client, See Endpoint Security Client  
Client Interface Mode, options 12  
client logging, configuring 26  
client software, defined 8  
colors, Web Control buttons 74  
Common module, configuring  
  client interface security 27  
  logging 26  
  McAfee GTI proxy server settings 28  
  Self Protection 26  
  settings 25  
  source sites for client updates 29  
  update settings 29  
Common module, Endpoint Security Client 7, 13  
communication problems, Web Control 78
Content Actions settings
  Web Control 82, 83
content categories, See web categories
content files
  about 8
  and detections 16
  changing AMCore version 23
  checking for updates manually 18
Extra.DAT files 24
  on-access scan overview 47
  on-demand scan overview 52
  scheduling updates 31
CPU time, on-demand scans 55
credentials, default administrator 11

D
debog logs, Endpoint Security Client 20
Default Client Update task
  about 31
  configuring 29
  configuring sites for updates 29
  scheduling with Endpoint Security Client 31
default password, Endpoint Security Client 11
Desktop mode, Windows 8
  responding to threat detection prompts 16
  Windows 8 10
detection definition files, See content files
detections
  displaying messages to users 47, 52
  excluding by name 56
  managing 34, 37
  names 39
  reporting to management server 8
  responding to 16
  types 34, 36
dialers, about 39
DNS traffic, blocking 60
domains, blocking 60
download requests, See file downloads

E
Endpoint Security
  managing 22
Endpoint Security Client
  about 11
  configuring security settings 27
  configuring sites for updates 29
  Default Client Update task, about 31
  Default Client Update task, configuring 29
  Default Client Update task, scheduling 31
  displaying help 16
  displaying protection information 17
  Full Scan and Quick Scan, scheduling 56
  interacting with 9

Endpoint Security Client (continued)
  logging on as administrator 22
  logs, about 20
  management types 8, 17
  managing threat detections 37
  modules 13
  opening 10, 15
  policy settings 12
  protecting with a password 27
  running scans 34
  scanning for malware 33
  system scans 33
  Threat Summary 12
  unlocking the interface 22
  updating protection 18
  viewing the Event Log 19
Endpoint Security, how it protects your computer 8
error logs, Endpoint Security Client 20
error messages, system tray icon states 10
event logs
  update failures 18
  viewing Event Log page 19
event logs, Endpoint Security Client 20
events, tracking Web Control browser events 79
exclusions
  detection name 56
  on-access scan, specifying files, folders, and drives 47
  on-demand scan, specifying 52
  specifying URLs for ScriptScan 47
  using wildcards 41
Exploit Prevention
  about 46
  configuring 45
  content file updates 9
  log files 20
exploits
  blocking buffer overflows 45, 46
  how buffer overflow exploits occur 46
Extra.DAT files
  about 24
  AMCore content files 9
  downloading 24
  loading 24
  on-access scan overview 47
  on-demand scan overview 52
  using 24

F
failures, update 18
features
  enabling and disabling 23
  Endpoint Security Client access based on policies 12
file downloads
  blocking from unknown sites 79
file downloads (continued)
  blocking or warning based on ratings 82
  scanning with Threat Prevention 81
files
  configuring for quarantine 56
  configuring log files 26
  Endpoint Security Client logs 19
  excluding specific types from scans 40
  log files 20
  managing in the Quarantine 37
  preventing from modification 26
  running scans 36
  wildcards in scan exclusions 41
files, content
  changing AMCore content version 23
  Exploit Prevention 9
  Extra.DAT and AMCore 9
  Extra.DAT files 24
  loading Extra.DAT files 24
  on-access scan overview 47
  on-demand scan overview 52
  signatures and updates 9
  using Extra.DAT files 24
Firefox
  displaying Web Control menu options 77
  supported browsers 73, 77
  testing communication problems 78
Firewall
  about 7
  activity log 20
  blocking DNS traffic 60
  debug log 20
  enabling and disabling protection 60
  Endpoint Security Client 13
  how firewall rules work 62
  how it works 59
  intrusion alerts 10
  location aware groups, about 64
  location-aware groups, creating 70
  log files 20
  managing 59
  managing rules and groups 67
  modifying options 60
  rules, See firewall rules
firewall groups
See also firewall rule groups
  configuring 62
firewall options
  modifying 60
firewall rule groups
  and connection isolation 65
  how the Firewall works 59
  location-aware, about 64
  location-aware, creating 70
  firewall rule groups (continued)
    precedence 64
firewall rules
  allow and block 62
  configuring 62
  for allowing FTP connections 70
  how the Firewall works 59
  how they work 62
  ordering and precedence 62
  using wildcards 69
folders
  configuring for quarantine 56
  managing in the Quarantine 37
  running scans 36
  wildcards in scan exclusions 41
frequently asked questions, McAfee GTI 61
FTP protocol 70
Full access mode
  modifying firewall options 60
  policy settings 12
Full Scan
  about 33
  configuring 52
  running from Endpoint Security Client 34
  scheduling on the client 56
G
global scan cache
  on-access scans 47
  on-demand scans 52
Google
  Chrome 73
  safety icons 75
  supported search engines 75
groups, firewall, See firewall rule groups
H
hashes, about 28
heap-based attacks, buffer overflow exploits 46
Help, displaying 11, 16
high-risk processes, specifying 47
I
icons, McAfee, See system tray icon, McAfee
icons, Web Control 75
incremental scans 54
information, displaying protection 17
installers, scanning trusted 47
interface modes
  configuring client security settings 27
  Standard access 22, 27
Internet Explorer
  and ScriptScan behavior 47
  displaying Web Control menu options 77
Internet Explorer (continued)
supported browsers 73, 77
testing communication problems 78
intrusions, enabling Firewall alerts 60
IP addresses
  location-aware groups 64
  rule groups 64

J
jokes, about 39

K
keyloggers, about 39

L
location-aware groups
  about 64
  connection isolation 65
  creating 70
Lock client interface mode
  and policy settings 12
  unlocking the interface 22
  when opening Endpoint Security Client 15
log files
  configuring 26
  locations 20
  update failures 18
  viewing 19
low-risk processes, specifying 47

M
malware
  detections while scanning 34, 36
  responding to detections 16
  scanning for 33
management types
  about 18
  displaying 17
manual scans
  about scan types 33
  running from Endpoint Security Client 34, 36
manual updates, running 18
McAfee client, See Endpoint Security Client
McAfee Endpoint Security Client, See Endpoint Security Client
McAfee ePO
  and management types 18
  retrieving AMCore content files 9
  updating protection 8
McAfee ePO Cloud management type 18
McAfee GTI
  and web categories 82
  configuring sensitivity level 56
  firewall options, configuring 60
  frequently asked questions 61
McAfee GTI (continued)
  network reputation for firewall, configuring 60
  on-access scans, configuring 47
  on-access scans, how they work 47
  on-demand scans, configuring 52
  on-demand scans, how they work 52
  overview 28
  scanning files before downloading 79, 81
  sending block events to server 60
  specifying proxy server settings 28
  troubleshooting communication problems 78
  Web Control communication error 74
  Web Control safety ratings 76
  Web Control site reports 75
McAfee icon, See system tray icon, McAfee
McAfee Labs
  AMCore content file updates 9
  and McAfee GTI 28
  downloading Extra.DAT 24
  Extra.DAT 24
  getting more information on threats 37
McAfee protection client, See Endpoint Security Client
McAfee SECURE, Web Control button 74
McAfee Security Status page, displaying 10
McTray, starting 54
menus
  About 17
  Action 11, 23
  Help 11, 16
  Settings 11–13, 60, 67
messages, Endpoint Security
  about 10
  displaying when threat detected 47, 52
Metro mode, Windows 8
  notification messages 10
  responding to threat detection prompts 16
Microsoft Internet Explorer, See Internet Explorer
modules
  about Endpoint Security 7
  displaying information about 17
  Endpoint Security Client access based on policies 12
  installed in Endpoint Security Client 13
modules, Common
  client interface security, configuring 27
  client update settings, configuring 29
  configuring source sites for client updates 29
  how McAfee GTI works 28
  logging, configuring 26
  McAfee GTI proxy server settings, configuring 28
  Self Protection, configuring 26
  update settings, configuring 29
Mozilla Firefox, See Firefox

N
network adapters, allowing connection 64
network drives, specifying scan options 47
notification messages
  about 10
  interacting with Endpoint Security Client 9
Windows 8 10

O
On-Access Scan page 37
on-access scans
  about 33
  configuring 47, 56
  excluding items 40
  log files 20
  number of scanning policies 51
  optimizing with trust logic 47
  overview 47
  potentially unwanted programs, enabling detection 42
  scanning scripts 47
  ScriptScan 47
  threat detections 16
  writing to vs. reading from disk 47
on-demand scans
  about 33
  configuring 56
  deferring 54
  excluding items 40
  log files 20
  overview 52
  potentially unwanted programs, enabling detection 42
Remote Storage scans 55
responding to prompts 16
running Full Scan or Quick Scan 34
running Right-Click Scan 36
scanning files or folders 36
system utilization 55
zero impact 54
on-demand updates, See manual updates, running options
  configuring on-access scans 47
  configuring on-demand scans 52
  scanning for malware 33
Options, Common
  client interface security, configuring 27
  configuring 25
  logging settings, configuring 26
  proxy server settings, configuring 28
  scheduling on-demand scans 33
  Self Protection, configuring 26
  source sites for client updates, configuring 29
  update settings, configuring 29
Options, Threat Prevention
  common scan settings 56
  unwanted programs 42
P
pages
  About 8, 17
  Event Log 19
  McAfee Security Status 10
  On-Access Scan 16, 37
  Quarantine 37
  Roll Back AMCore Content 23
  Scan for threats 36
  Scan System 34, 37
  scan, displaying 34
  Settings 12, 26–29, 52, 60
  Update 18
passive mode FTP protocol 70
password crackers, about 39
passwords
  administrator 22
  configuring client security 27
  controlling access to client 27
  default administrator 11
phishing, reports submitted by site users 76
policies
  accessing Endpoint Security Client 12
  client features 9
  defined 8
policies, Common
  configuring 25
policies, Threat Prevention
  common scan settings 56
  on-access scans 51
  on-demand scans, deferring 54
pop-ups, and safety ratings 76
ports, FTP connections 70
potentially unwanted programs
  about 39
  configuring detection 41
  detections while scanning 34, 36
  enabling detection 42, 47, 52
  specifying 42
  specifying programs to detect 56
  wildcards in scan exclusions 41
precedence
  firewall groups 64
  firewall rules 62
priorities, on-access scans 55
process settings, on-demand scans 55
processes, Threat Prevention
  including and excluding in access protection 43
  scanning 47
  specifying high- and low-risk 47
product updates
  checking for manually 18
  scheduling 31
programs, enabling detection of potentially unwanted 47, 52
prompts, Endpoint Security
about 10
responding to scan 16
Windows 8 16
protection
configuring Self Protection 26
displaying information about 17
interacting with 9
keeping up to date 8
proxy server
configuring for McAfee GTI 28
how McAfee GTI works 28

Q
Quarantine page 37
Quarantine, Threat Prevention
configuring location and retention settings 56
Quick Scan
configuring 52
running from Endpoint Security Client 34
scheduling on the client 56
types of scans 33

R
ratings, safety, See safety ratings
ratings, Web Control, See safety ratings
remote admin tools, about 39
Remote Desktop, and scan on idle feature 54
Remote Storage scans, overview 55
reports, Web Control 75, 76
displaying 77
safety 73
viewing 78
website safety 75
responses, configuring for unwanted program detection 42
resumable scans, See incremental scans
Right-Click Scan
about 33
configuring 52
running from Windows Explorer 36
Roll Back AMCore Content page 23
rule groups, Firewall, See firewall rule groups
rules, firewall, See Firewall
rules, Threat Prevention
configuring 43
how Access Protection works 45

S
safety ratings
configuring actions for sites and downloads 82
controlling access to sites 83
how website ratings are derived 76
safety icons 75

safety ratings (continued)
Web Control and 73
safety reports, See reports, Web Control
scan avoidance 47
scan cache
on-access scans 47
on-demand scans 52
scan deferral, overview 54
scan engines, AMCore content file overview 9
Scan for threats page 36
Scan Now button 34
scan on idle feature 16, 54
scan page, displaying 16, 34
Scan System page 34, 37
scans
common settings for on-access and on-demand scans 56
deferring, pausing, resuming, and canceling 16
responding to prompts 16
running from Endpoint Security Client 34
running Right-Click Scan 36
scheduling with Endpoint Security Client 56
types 33
using wildcards in exclusions 41
Web Control 81
scans, on-access
configuring 47
detecting threats in Windows Store apps 47
excluding items 40
number of policies 51
optimizing with trust logic 47
overview 47
ScriptScan 47
threat detections, responding to 16
scans, on-demand
configuring 52
deferring 54
detecting threats in Windows Store apps 52
excluding items 40
overview 54
Remote Storage scans 55
running only when system is idle 54
scheduling on the client 56
system utilization 55
zero impact 54
schedules, on-demand scans, deferring 54
ScriptScan
about 47
enabling 47
searches
blocking risky sites from results 79
safety icons 75
Secure Search, configuring Web Control 79
security
configuring client interface security 27
SecurityCenter management type 18
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Protection, configuring</td>
<td>26</td>
</tr>
<tr>
<td>self-managed, about</td>
<td>18</td>
</tr>
<tr>
<td>sensitivity level, McAfee GTI 28</td>
<td>28</td>
</tr>
<tr>
<td>server systems, and scan on idle feature</td>
<td>54</td>
</tr>
<tr>
<td>settings</td>
<td></td>
</tr>
<tr>
<td>source sites, configuring for</td>
<td>29</td>
</tr>
<tr>
<td>updates, configuring for</td>
<td>29</td>
</tr>
<tr>
<td>Settings page</td>
<td></td>
</tr>
<tr>
<td>and Client Interface Mode</td>
<td>12</td>
</tr>
<tr>
<td>client interface security, configuring</td>
<td>27</td>
</tr>
<tr>
<td>logging, configuring</td>
<td>26</td>
</tr>
<tr>
<td>managing firewall rules and groups</td>
<td>67</td>
</tr>
<tr>
<td>modifying firewall options</td>
<td>60</td>
</tr>
<tr>
<td>on-access scan settings, configuring</td>
<td>47</td>
</tr>
<tr>
<td>on-demand scan settings, configuring</td>
<td>52</td>
</tr>
<tr>
<td>proxy server settings, configuring</td>
<td>28</td>
</tr>
<tr>
<td>Self Protection, configuring</td>
<td>26</td>
</tr>
<tr>
<td>source sites for client updates, configuring</td>
<td>29</td>
</tr>
<tr>
<td>update settings, configuring</td>
<td>29</td>
</tr>
<tr>
<td>settings, Threat Prevention</td>
<td></td>
</tr>
<tr>
<td>Access Protection feature</td>
<td>43</td>
</tr>
<tr>
<td>configuring potentially unwanted programs</td>
<td>42</td>
</tr>
<tr>
<td>on-access scans</td>
<td>42</td>
</tr>
<tr>
<td>on-demand scans</td>
<td>42</td>
</tr>
<tr>
<td>settings, Web Control</td>
<td></td>
</tr>
<tr>
<td>controlling access to websites</td>
<td>82</td>
</tr>
<tr>
<td>controlling access with safety ratings</td>
<td>83</td>
</tr>
<tr>
<td>controlling access with web categories</td>
<td>82</td>
</tr>
<tr>
<td>signatures, known threat information</td>
<td>9</td>
</tr>
<tr>
<td>site reports, See reports, Web Control</td>
<td></td>
</tr>
<tr>
<td>sites</td>
<td></td>
</tr>
<tr>
<td>browsing protection</td>
<td>74</td>
</tr>
<tr>
<td>protection while searching</td>
<td>75</td>
</tr>
<tr>
<td>safety ratings</td>
<td>76</td>
</tr>
<tr>
<td>viewing Web Control site reports</td>
<td>78</td>
</tr>
<tr>
<td>sites, blocking</td>
<td></td>
</tr>
<tr>
<td>based on ratings</td>
<td>82</td>
</tr>
<tr>
<td>based on safety ratings</td>
<td>83</td>
</tr>
<tr>
<td>based on web category</td>
<td>82</td>
</tr>
<tr>
<td>sites, controlling access</td>
<td></td>
</tr>
<tr>
<td>with safety ratings</td>
<td>83</td>
</tr>
<tr>
<td>with web categories</td>
<td>82</td>
</tr>
<tr>
<td>sites, warning</td>
<td></td>
</tr>
<tr>
<td>based on ratings</td>
<td>82</td>
</tr>
<tr>
<td>based on safety ratings</td>
<td>83</td>
</tr>
<tr>
<td>software updates</td>
<td></td>
</tr>
<tr>
<td>checking for manually</td>
<td>18</td>
</tr>
<tr>
<td>scheduling</td>
<td>31</td>
</tr>
<tr>
<td>source sites, configuring for client updates</td>
<td>29</td>
</tr>
<tr>
<td>spyware, about</td>
<td>39</td>
</tr>
<tr>
<td>stack-based attacks, buffer overflow exploits</td>
<td>46</td>
</tr>
<tr>
<td>standalone, See self-managed, about</td>
<td></td>
</tr>
<tr>
<td>Standard access mode</td>
<td></td>
</tr>
<tr>
<td>and policy settings</td>
<td>12</td>
</tr>
<tr>
<td>configuring client security settings</td>
<td>27</td>
</tr>
<tr>
<td>Standard access mode (continued)</td>
<td></td>
</tr>
<tr>
<td>effects of setting a password</td>
<td>27</td>
</tr>
<tr>
<td>logging on as administrator</td>
<td>22</td>
</tr>
<tr>
<td>managing firewall rules and groups</td>
<td>67</td>
</tr>
<tr>
<td>Start menu, opening Endpoint Security Client</td>
<td>15</td>
</tr>
<tr>
<td>Status page, viewing Threat Summary</td>
<td>12</td>
</tr>
<tr>
<td>status, Endpoint Security Client</td>
<td></td>
</tr>
<tr>
<td>stealth, about</td>
<td>39</td>
</tr>
<tr>
<td>system scans, types</td>
<td>33</td>
</tr>
<tr>
<td>system tray icon, McAfee</td>
<td></td>
</tr>
<tr>
<td>configuring access to Endpoint Security</td>
<td>27</td>
</tr>
<tr>
<td>defined</td>
<td>10</td>
</tr>
<tr>
<td>opening Endpoint Security Client</td>
<td>15</td>
</tr>
<tr>
<td>system utilization options, overview</td>
<td>55</td>
</tr>
<tr>
<td>T</td>
<td></td>
</tr>
<tr>
<td>tasks, Threat Prevention</td>
<td></td>
</tr>
<tr>
<td>Default Client Update, about</td>
<td>31</td>
</tr>
<tr>
<td>Default Client Update, scheduling</td>
<td>31</td>
</tr>
<tr>
<td>Full and Quick Scans, about</td>
<td>33</td>
</tr>
<tr>
<td>Full Scan and Quick Scan, scheduling</td>
<td>56</td>
</tr>
<tr>
<td>threads, priority</td>
<td>55</td>
</tr>
<tr>
<td>Threat Prevention</td>
<td></td>
</tr>
<tr>
<td>about</td>
<td>7</td>
</tr>
<tr>
<td>Access Protection feature</td>
<td>43</td>
</tr>
<tr>
<td>Endpoint Security Client</td>
<td>13</td>
</tr>
<tr>
<td>Exploit Prevention feature</td>
<td>45</td>
</tr>
<tr>
<td>managing</td>
<td>40</td>
</tr>
<tr>
<td>on-access scans, about</td>
<td>47</td>
</tr>
<tr>
<td>on-access scans, configuring</td>
<td>47</td>
</tr>
<tr>
<td>on-demand scans, about</td>
<td>52</td>
</tr>
<tr>
<td>on-demand scans, configuring</td>
<td>52</td>
</tr>
<tr>
<td>Options, unwanted programs</td>
<td>42</td>
</tr>
<tr>
<td>potentially unwanted programs, detecting</td>
<td>41</td>
</tr>
<tr>
<td>scanning files before downloading</td>
<td>79</td>
</tr>
<tr>
<td>81</td>
<td></td>
</tr>
<tr>
<td>Threat Summary, about</td>
<td>12</td>
</tr>
<tr>
<td>threats</td>
<td></td>
</tr>
<tr>
<td>access point violations</td>
<td>44</td>
</tr>
<tr>
<td>Access Protection process</td>
<td>45</td>
</tr>
<tr>
<td>AMCore content files</td>
<td>9</td>
</tr>
<tr>
<td>and safety ratings</td>
<td>76</td>
</tr>
<tr>
<td>detections while scanning</td>
<td>36</td>
</tr>
<tr>
<td>getting more information from McAfee Labs</td>
<td>37</td>
</tr>
<tr>
<td>managing detections</td>
<td>37</td>
</tr>
<tr>
<td>Quarantine folder</td>
<td>37</td>
</tr>
<tr>
<td>responding to detections</td>
<td>16</td>
</tr>
<tr>
<td>types</td>
<td>39</td>
</tr>
<tr>
<td>Windows Store apps</td>
<td>47</td>
</tr>
<tr>
<td>52</td>
<td></td>
</tr>
<tr>
<td>throttling, configuring</td>
<td>55</td>
</tr>
<tr>
<td>toast notifications, Windows 8 Metro mode</td>
<td>10</td>
</tr>
<tr>
<td>16</td>
<td></td>
</tr>
<tr>
<td>traffic</td>
<td></td>
</tr>
<tr>
<td>allowing outgoing until firewall services start</td>
<td>60</td>
</tr>
<tr>
<td>scanned by Firewall</td>
<td>59</td>
</tr>
</tbody>
</table>
trojans
  about 39
detections while scanning 34, 36
trust logic, optimizing on-access scans 47
trusted installers, scanning 47

U
unmanaged, See self-managed, about
Update page 18
updates
  canceling 18
  configuring sites for updates 29
  Update Now button, Endpoint Security Client 18
updates, Endpoint Security
  configuring behavior 29
  scheduling from client 31
updates, Threat Prevention
  checking for manually 18
  content files 8
  Default Client Update task, about 31
  Extra.DAT files 24
  overview 9
  scheduling automatic 31
upgrades, client software components 8
URLs
  blocking unknown 79
  excluding from script scanning 47
user accounts, controlling access to client 27
User added rules group 67

V
View Detections button 37
View Scan button 34
viruses
  about 39
detections while scanning 34, 36
  responding to detections 16
  signatures 9
vulnerabilities, See threats

W
web categories, blocking or warning based on 82
Web Control
  about 7
  activity log 20
  balloons and icons 77
  buttons, description 74
  configuring 79
  debug log 20
Web Control (continued)
  displaying menu options in browser 77
  enabling 79
  Endpoint Security Client 13
  features 73
  how file downloads are scanned 81
  icons, description 75
  log files 20
  managing 79
  menu 74
  search engines and safety icons 75
  site reports 75
  troubleshooting communication problems 78
  viewing site reports 78
websites
  browsing protection 74
  protection while searching 75
  safety ratings 76
  viewing Web Control site reports 78
websites, blocking
  based on ratings 82
  based on safety ratings 83
  based on web category 82
  risky sites from search results 79
  unrated or unknown 79
websites, controlling access
  with safety ratings 83
  with web categories 82
websites, warning
  based on ratings 82
  based on safety ratings 83
wildcards
  using in firewall rules 69
  using in scan exclusions 41
Windows 8
  about notification messages 10
  opening Endpoint Security Client 15
  responding to threat detection prompts 16
Windows Set Priority setting 55
Windows Store apps, detecting threats 47, 52

Y
Yahoo
  default search engine 79
  safety icons 75
  supported search engine 75

Z
zero-impact scans 54