



Product Guide

McAfee SaaS Endpoint Protection 5.2.0

COPYRIGHT

Copyright © 2010 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

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 MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

Preface	9
About this guide	9
Audience	9
Conventions	9
Finding product documentation	10
1 Introducing McAfee SaaS Endpoint Protection	11
How McAfee SaaS Endpoint Protection works	12
Types of protection	13
Core protection services	13
Additional protection services	13
Core product strengths	14
New features for this release	15
The role of the client software	17
Updates to the client software	17
Overview of update methods	18
Simple updates through direct connections	19
Updates using Rumor technology	19
Updates through relay servers	19
Management with the SecurityCenter	20
Create user groups	21
Customize policies	23
Check reports	25
2 Using the Client Software	27
How to access the client software	27
About the icon	28
About the console	29
Types of client software updates	29
Terminal server support	31
Specifying when computers check for updates	31
Updating client computers manually	32
Disabling updates for non-logged on users	32
Performing setup and maintenance tasks	32
Testing virus protection	33
Changing the language for the software	33
Viewing information about the client software	34
Logging on as a site administrator	34
Configuring notifications	35
Configuring what users see	35
Uninstalling the client software	35
3 Using the SecurityCenter	37
The SecurityCenter	37
Logging on to the SecurityCenter	38

Accessing data on SecurityCenter pages	39
Protection status at a glance	40
Viewing protection at a glance	42
Working with widgets	42
Management of client computers	43
Working with computers	45
Working with an individual computer	46
Identifying duplicate computers	47
Identifying Microsoft product versions on computers	47
Upgrading the client software	48
Management of computer groups	48
Working with groups	49
Management of Active Directory groups	50
Downloading the Active Directory synchronization utility	51
Importing Active Directory groups	51
Installing on Active Directory groups	51
Synchronizing Active Directory groups	52
Viewing the synchronization status	52
Viewing the Active Directory tree in the SecurityCenter	53
Management of group administrators	53
Working with group administrators	55
Management of security policies	56
McAfee Default policy	56
Working with policies	59
Generation of security reports	60
Scheduling reports	63
Adding your logo to reports	64
Management of your account	65
Configuring your account profile	65
Signing up for email notifications	65
Viewing and updating subscription information	66
Buying and renewing subscriptions and licenses	66
Locating or creating keys for your account	67
Merging accounts	68
Utilities	68
Getting assistance	70
4 Using the Virus and Spyware Protection Service	71
How detections are handled	72
Spyware protection mode and detections	72
Use learn mode to discover programs	73
Types of scans	73
On-access (automatic) scans	74
On-demand scans	74
Email scans	75
Spyware scans	76
Scanning on client computers	77
Scanning on demand from the console	77
Scanning on demand from Windows Explorer	78
Scanning email on client computers	78
Viewing scheduled scans	78
Enabling and disabling on-access scanning	79
Configuring scanning policy options	80
Scheduling a scan	80
Enabling optional types of virus scans	80
Excluding files and folders from virus scans	82

Selecting spyware scanning options	82
Approving and unapproving programs in a policy	82
Managing detections	83
Viewing scan results on client computers	84
Managing potentially unwanted program detections	84
Managing quarantined files	85
Viewing user-approved programs and applications	86
Viewing threats detected on the account	87
Viewing unrecognized programs detected on the account	87
Viewing historical information about detections	88
Reports for virus and spyware protection	89
Best practices (virus and spyware protection)	89
5 Using the Firewall Protection Service	91
Connection type and detections of incoming communications	92
Custom connections	93
Firewall protection mode and detections of unknown applications	94
Use learn mode to discover Internet applications	95
The role of IP addresses	95
The role of system service ports	96
Standard assignments for system service ports	97
Configuration of the firewall protection service	97
Interaction between user and administrator policy settings	99
Configuring policy options	99
Selecting general firewall settings	99
Configuring options for Internet applications	100
Tracking blocked communications	101
Configuring custom connections	101
Configuring system services and port assignments	102
Configuring IP addresses	103
Installing and enabling firewall protection at the policy level	104
Installing firewall protection during policy updates	104
Enabling and disabling firewall protection	104
Managing detections	105
Viewing unrecognized programs detected on the account	105
Viewing user-approved programs and applications	106
Viewing blocked communications	106
Reports for the firewall protection service	107
Best practices (firewall protection)	108
6 Using the Browser Protection Service and Web Filtering	109
Browser protection features	110
How safety ratings are compiled	110
Safety icons and balloons protect during searches	111
Using site safety balloons	111
Testing communication problems	111
SiteAdvisor menu protects while browsing	112
Using the SiteAdvisor menu	113
Safety reports provide details	113
Viewing safety reports	115
Information that browser protection sends to McAfee	115
Installing browser protection during policy updates	116
Web filtering features	116
Enabling and disabling browser protection via policy	117
Enabling and disabling browser protection at the client computer	117
Block and warn sites by safety ratings	118

Blocking or warning site access based on safety ratings	119
Blocking or warning file downloads based on safety ratings	119
Blocking phishing pages	120
Block and warn sites by content	121
Blocking or warning site access based on content	121
Authorize and prohibit sites by URL or domain	122
How site patterns work	122
Adding authorized and prohibited sites	123
Customizing messages for users	124
Viewing browsing activity	125
Web Filtering report	125
Best practices (browser protection)	126
7 Using the SaaS Email Protection Service	127
Core SaaS email protection features	127
Additional SaaS email protection services	128
The SaaS email protection widget and portal	129
Account activation and setup	130
Activating and setting up your account	131
Accessing the SaaS email and web protection portal	132
Configuring policy settings for the SaaS email protection service	132
Checking quarantined messages	133
Reading encrypted messages	133
Reports and statistics for SaaS email protection	134
Viewing email activity for the week	134
Viewing reports	134
Getting more information	135
8 Using the SaaS Web Protection Service	137
SaaS web protection features	137
Multiple layers of protection against web-based threats	138
The SaaS web protection widget and portal	138
Account activation and setup	139
Activating and setting up your account	140
Accessing the SaaS email and web protection portal	140
Configuring policy settings for SaaS web protection	141
Reports for SaaS web protection	141
Viewing reports	141
Getting more information	142
9 Using the Email Server Protection Service	143
Email server protection features	143
The installation and setup process	145
Installing email server protection	145
The email server protection widget and management console	146
Managing the email server protection service	147
Checking notifications and action items	148
Viewing detection and status information	148
Accessing the management console on the server	149
Where to find more information	150
10 Using the SaaS Vulnerability Scanning Service	151
Vulnerability scanning features	151
Certification programs	153
The SaaS vulnerability scanning widget and portal	153
Accessing the SaaS vulnerability scanning portal	154

Overview of scanning process	155
Overview of the certification process	155
Types of devices to scan	156
Types of scans	157
Managing scan devices	158
Discovering IP addresses in a domain	159
Discovering IP addresses in a network	159
Adding devices to scan	160
Configuring devices to accept scans	161
Creating device groups	161
Changing device groups	162
Deleting devices	162
Performing scans	163
Starting a scan	163
Scheduling scans for devices	164
How detections are reported	165
Viewing scan results	165
Viewing results for audit scans	166
Viewing results for DNS discovery on domains	166
Viewing results for network discovery scans	167
11 Troubleshooting	169
Frequently asked questions	169
Error messages	174
Index	177

Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

Contents

- ▶ [About this guide](#)
- ▶ [Finding product documentation](#)

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses the following typographical conventions and icons.

Book title or Emphasis Title of a book, chapter, or topic; introduction of a new term; emphasis.

Bold Text that is strongly emphasized.

User input or Path Commands and other text that the user types; the path of a folder or program.

Code

A code sample.

User interface Words in the user interface including options, menus, buttons, and dialog boxes.

Hypertext blue A live link to a topic or to a website.



Note: Additional information, like an alternate method of accessing an option.



Tip: Suggestions and recommendations.



Important/ Caution: Valuable advice to protect your computer system, software installation, network, business, or data.



Warning: Critical advice to prevent bodily harm when using a hardware product.

Finding product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	<ol style="list-style-type: none">1 Click Product Documentation.2 Select a Product, then select a Version.3 Select a product document.
KnowledgeBase	<ul style="list-style-type: none">• Click Search the KnowledgeBase for answers to your product questions.• Click Browse the KnowledgeBase for articles listed by product and version.

1

Introducing McAfee SaaS Endpoint Protection

McAfee SaaS Endpoint Protection provides a "hands-off" solution to safeguard the computers on your network automatically by keeping itself up-to-date and checking for threats contained in files and programs, in email messages, in communications from inside and outside the network, and on websites.

When you purchase a subscription to McAfee SaaS Endpoint Protection, an account is created for you, and you become the account administrator (referred to as the *site administrator*). When you install the McAfee SaaS Endpoint Protection client software on computers, they are added to your account. A weekly email alerts you to any problems detected for computers on your account.



In some organizations, another person, such as a purchasing department representative, purchases the subscription and then designates you to be the site administrator.

For a more "hands-on" approach, use the SecurityCenter to view and manage computers and detections on your network. Your service provider sends you a unique URL and login credentials for your account, which you can use to access the SecurityCenter. This is a pre-configured website that provides a simple-to-use management console for monitoring the protection status of computers on your account. Use the SecurityCenter to view reports on detections and activities and to configure security settings that address the specific needs of your account.

This section provides an overview of the product and its features.

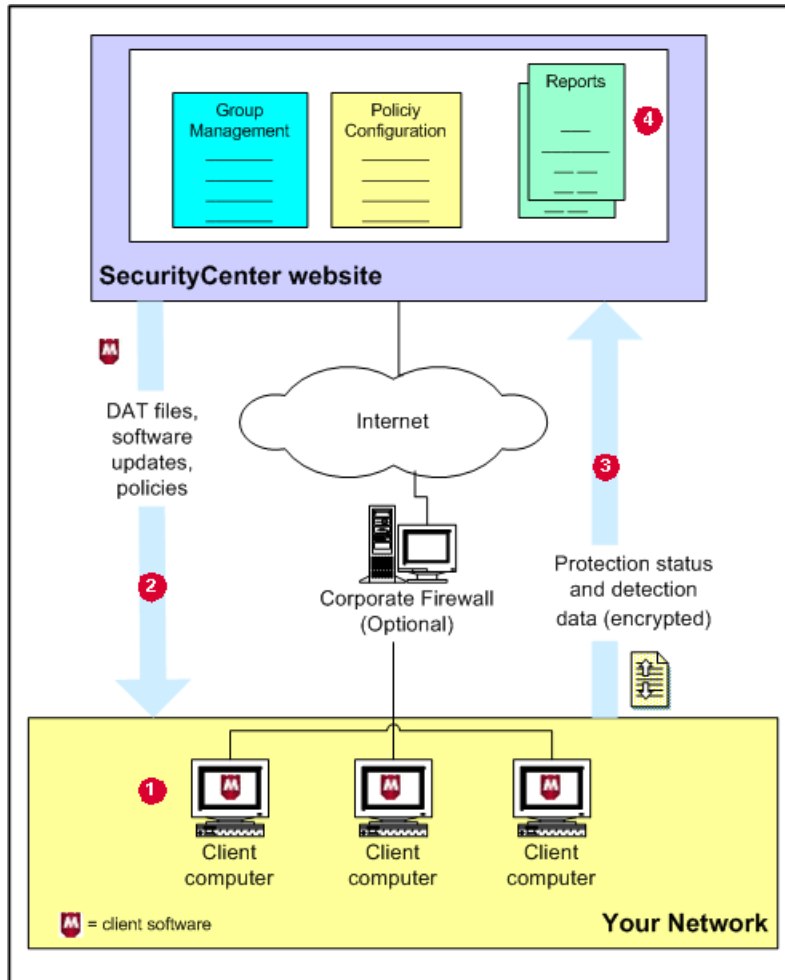
Contents

- ▶ *How McAfee SaaS Endpoint Protection works*
- ▶ *Types of protection*
- ▶ *Core protection services*
- ▶ *Additional protection services*
- ▶ *Core product strengths*
- ▶ *New features for this release*
- ▶ *The role of the client software*
- ▶ *Updates to the client software*
- ▶ *Management with the SecurityCenter*

How McAfee SaaS Endpoint Protection works

McAfee SaaS Endpoint Protection delivers comprehensive security as a service for all the computers on your account.

It automatically checks for threats, intercepts them, takes the appropriate action to keep your data and your network safe, and tracks detections and security status for reports.



1	Client software runs on each computer where it is installed.
2	The client software updates itself — automatically and silently — by downloading the latest detection definition (DAT) files from your account's administrative website, the SecurityCenter. DAT files define the threats that the client software detects.
3	The client software uploads security information about each computer to the SecurityCenter for use in administrative reports.
4	As your account's administrator, you can use a web browser to visit the SecurityCenter, where you can access reports that detail the status of client computers and use tools for customizing and managing security.

Types of protection

McAfee SaaS Endpoint Protection uses three basic methodologies for protection services. All are managed through the SecurityCenter administrative website.

- *Client-based protection services* are installed on client computers. They check for threats, download updates that add protection against the latest types of threats, and send status information to the SecurityCenter.
- *Server-based protection services* are installed on a server, such as an email server. Threats are detected at the server, rather than on client computers, and reported to the SecurityCenter.
- *SaaS protection services* reside "in the clouds." Incoming and outgoing content is routed through dedicated McAfee servers to check for threats, and the servers report data to the SecurityCenter. No associated software is installed on your network.

Core protection services


The core protection services in McAfee SaaS Endpoint Protection are client based.

Service	Description
Virus and spyware protection	Checks for viruses, spyware, unwanted programs, and other potential threats borne on removable media or brought in from your network, including via email. Every time a file on your computer is accessed, virus and spyware protection scans the file to make sure it is free of viruses and spyware.
Firewall protection	Establishes a barrier between each computer and the Internet or other computers on your local network. It silently monitors communications traffic for suspicious activity and takes appropriate action, such as blocking.
Browser protection	Displays information to safeguard client computer users against web-based threats. Users can view website safety ratings and safety reports as they browse or search with Microsoft Internet Explorer or Mozilla Firefox.

Additional protection services

Some versions of McAfee SaaS Endpoint Protection include additional protection services.

Feature	Description
Client-based	
Web filtering	Works within the browser protection service to expand the policy and reporting options available. Enables administrators to control access to websites based on their safety rating or category of content. Based on McAfee®SiteAdvisor® Enterprise Plus.
Web-based	

Feature	Description
SaaS email protection (includes NEW module)	<p>Protects against email threats by scanning messages before they reach your network. Blocks or quarantines detections of directory harvest attacks, spam, phishing scams, viruses, and other email-borne threats in messages and attachments. Based on McAfee SaaS Email Protection and can be enhanced with these additional services:</p> <ul style="list-style-type: none"> • McAfee SaaS Email Archiving — Stores email messages in a centralized, secure location. • McAfee SaaS Email Protection & Continuity — Enables web-based email access during outages. • SaaS Email Intelligent Routing — Routes filtered email to distributed email systems. • SaaS Email Encryption (NEW) — Encrypts the content of outgoing messages, then requires account credentials to retrieve them. <p> If you have subscribed to email protection previously, your account will be migrated to SaaS email protection. McAfee will notify you when this occurs and provide instructions for setting up the new account.</p>
SaaS vulnerability scanning (includes NEW services)	<p>Analyzes your domains and IP addresses, then reports vulnerability detections and recommends steps for correcting them. Based on McAfee®SECURE™ and can be enhanced with these additional services:</p> <ul style="list-style-type: none"> • PCI Certification (NEW) — Ensures that your websites always comply with the Payment Card Industry Data Security Standard (PCI DSS) by providing the tools needed to complete the PCI certification process, remain in compliance, and create quarterly validation reports. • Trustmark module (NEW) — Adds the McAfee®SECURE™ Trustmark to your website as proof that it meets the rigorous certification requirements for compliance with the McAfee®SECURE™ data security standard.
Email server protection	<p>Provides comprehensive virus and spam protection for the email and other content entering and leaving your environment. Proactive anti-virus scanning and an automatic outbreak manager prevent malicious code from disrupting the system, while advanced content filtering allows administrators to set up rules for inappropriate content, sensitive information, and adding disclaimers to messages.</p> <ul style="list-style-type: none"> • McAfee® Security Service for Exchange protects your Microsoft Exchange Server 2003/2007 environment and includes McAfee® Anti-Spam for Mail Servers. Documentation is bundled with the downloaded software. • McAfee®GroupShield® for Lotus Domino protects your Lotus Domino Windows edition version 6.0.2/7.0.2/8.0 environment and includes Anti-Spam for Mail Servers. Documentation is available on the CD or in the downloadable installer accessible from the McAfee download center.

Core product strengths

McAfee SaaS Endpoint Protection safeguards your computers with a robust set of core features.

- **Continuous protection** — From the time a client computer is turned on until it is turned off, McAfee SaaS Endpoint Protection silently monitors all file input and output, downloads, program executions, inbound and outbound communications, and other system-related activities.
- **Instant discovery for virus threats** — When McAfee SaaS Endpoint Protection detects a virus threat, it attempts to clean the item containing the threat before further damage can occur. If an item cannot be cleaned, a copy of it is placed in a quarantine folder and the original item is deleted.

- **Customized threat response for program detections** — By default, McAfee SaaS Endpoint Protection provides a high degree of protection against threats. You can also configure the response to detections of potentially unwanted programs and suspicious activity to suit your needs: take immediate action to clean, quarantine, or block the detection; prompt users for a response; or only log the detection for administrative reports.
- **Preemptive safety notifications for web-based threats** — Threats reported on websites are communicated to users through color-coded icons and safety reports, enabling them to minimize exposure to dangerous websites.
- **Automatic updates** — McAfee SaaS Endpoint Protection checks for product updates at regular intervals throughout the day, comparing security components against the latest releases. When a computer needs a newer version, the client software retrieves it automatically.
- **Early Warning system and outbreak response** — McAfee SaaS Endpoint Protection uses the latest information about threats and outbreaks as soon as they are discovered by McAfee Labs, a research division of McAfee. Whenever McAfee Labs releases an outbreak detection definition (DAT) file, computers on your account receive it promptly.

New features for this release

This release of McAfee SaaS Endpoint Protection includes these new features.

Core features

All versions of McAfee SaaS Endpoint Protection include these new features to facilitate account management.

Now you can do this...	Details
Import the Active Directory organizational unit (OU) structure into the SecurityCenter, then install the client software, assign policies, and view reports based on the imported groups of computers.	Administrators who use Active Directory to define group hierarchies in their networks can also: <ul style="list-style-type: none"> • Download and run a synchronization utility to import Active Directory information from your network to the SecurityCenter. • "Push" the client software to computers in the Active Directory tree by using the Push Install utility. • Schedule the synchronization utility to run at regular intervals to keep the Active Directory information up-to-date in the SecurityCenter. • Select either a flat list view or a tree view of groups created in the SecurityCenter and Active Directory groups. A tree view icon appears to the right of the Groups filter, and icons for flat list and tree views appear at the top of listings.
Schedule a date and time for some or all computers to be upgraded to a new version of the product.	This allows administrators to: <ul style="list-style-type: none"> • Select a time when the upgrade would be least disruptive to computer users. • Test a new version of the product on a small number of computers before deploying it company-wide.

Now you can do this...	Details
Use a variety of web browsers.	<p>Access the SecurityCenter and perform a URL or push installation with these browsers:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer (versions 6, 7, and 8) • Mozilla Firefox (versions 2.0, 3.0, and 3.5) • Google Chrome (version 4.1) • Apple Safari for Windows (version 4.0)
Reduce the number of steps required for installing the client software.	<p>All methods for installing the client software include these new options:</p> <ul style="list-style-type: none"> • Assign a policy during installation. • Perform a full scan on the client computer when installation is complete.
Increase protection and ease-of-use with new virus and spyware protection features.	<p>The virus and spyware protection service includes these enhancements:</p> <ul style="list-style-type: none"> • Script scanning support for Firefox browser pages. • Addition of identification information to alerts and reports. The IP address or name of the source machine is provided when an infection originates from a remote source. • Addition of status information for the last client scan and client update tasks on the Computer Details page of the SecurityCenter.
Install the firewall protection service more easily and increase the level of protection.	<p>The firewall protection service includes these enhancements:</p> <ul style="list-style-type: none"> • No reboot is necessary after installing the firewall protection service (unless installing over an existing installation). • Notification alert when the network connection changes.

Additional types of protection

Some versions of McAfee SaaS Endpoint Protection offer additional types of protection that extend coverage to other network assets.

Now you can do this...	Details
Use encryption to secure the content of email messages.	<p>The SaaS email encryption module lets users encrypt the content of outgoing messages. Requires account credentials to retrieve encrypted messages. Based on McAfee® SaaS Email Encryption.</p> <p>Requires an active subscription to the SaaS email protection service.</p>
Route browser requests through McAfee servers to scan for threats and inappropriate content.	<p>The SaaS web protection service checks all websites that client computers attempt to access, then blocks those that violate standards defined in policy settings. Based on McAfee® SaaS Web Protection.</p>

Now you can do this...	Details
Participate in the McAfee PCI Certification program.	Ensures that websites always comply with the Payment Card Industry Data Security Standard (PCI DSS) by providing the tools needed to complete the PCI certification process, remain in compliance, and create quarterly validation reports. Requires an active subscription for the SaaS vulnerability scanning service.
Add the McAfee®SECURE™ Trustmark to your website as proof that it meets the rigorous certification requirements for compliance with the McAfee®SECURE™ data security standard.	Scans run automatically and results are displayed in SecurityCenter. The Trustmark is visible on a customer site as long as the site meets certification requirements; when vulnerabilities are detected, recommendations are given for resolving them. Requires an active subscription for the SaaS vulnerability scanning service.

The role of the client software

The McAfee SaaS Endpoint Protection software installed on client computers implements a three-prong approach to security

It does this by:

- 1 Silently monitoring all file input and output, downloads, program executions, inbound and outbound communications, and other system-related activities on client computers. As a result of this monitoring, the client software automatically:
 - Deletes or quarantines detected viruses.
 - Removes potentially unwanted programs, such as spyware or adware, unless you select a different response.
 - Blocks suspicious activity unless you specify a different response.
 - Indicates unsafe websites with a color-coded button or icon in the browser window or search results page. These indicators provide access to safety reports that detail site-specific threats.
- 2 Regularly updating detection definition (DAT) files and software components to ensure that you are always protected against the latest threats.
- 3 Uploading security information for each client computer to the SecurityCenter, then using this information to send emails and create reports that keep you informed about your account's status.

Updates to the client software

Regular updates are the cornerstone of McAfee SaaS Endpoint Protection.

The client software periodically checks a site on the Internet for newer versions of these software components.

- Regular DAT files, which contain the latest definitions for viruses, potentially unwanted programs, and cookies and registry keys that might indicate spyware. These are updated regularly to add protection against new threats.
- Outbreak DAT files, which are high-priority detection definition files released in an emergency situation in response to a specific new threat.

- Software components running on client computers.
- Policy settings configured for your account.

At the same time, the client software sends information about its detections and protection status, to update the security data maintained on the SecurityCenter website and used in administrative reports.

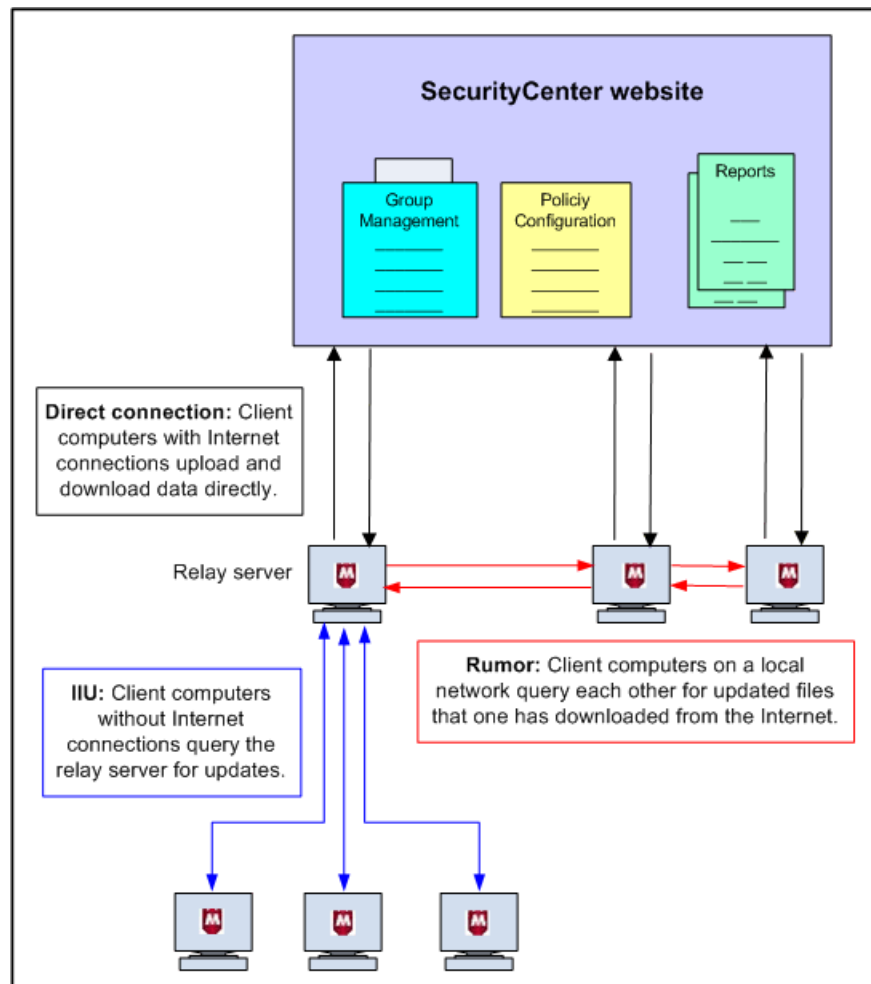
Overview of update methods

The client software uses several methods to check for and retrieve updates.

Five minutes after a client computer connects to the network, and at regular intervals throughout the day, the client software checks for updates. If updates are available, the client computer retrieves them.

In addition, users can check for updates manually at any time by clicking the product icon in the system tray, then selecting **Update Now**.

Updates can occur in three ways. You can implement one method or a combination of methods, which enables you to control the impact updates have on network resources.



- 1 For simple updates, each client computer on your account has a direct connection to the Internet and checks for new updates.
- 2 Rumor technology enables all computers in a workgroup to share downloaded files, which controls Internet traffic and minimizes expensive downloads.
- 3 Internet Independent Updating (IIU) enables any computer on the network to get information from the update site, even if that computer does not have an Internet connection, by communicating with the update site through a network computer that is configured as a relay server.

Simple updates through direct connections

Each client computer that has a direct Internet connection can check for updates and download them from the update site on the Internet. This is the simplest method of retrieving updates.

Updates using Rumor technology

When one computer shares updates with other computers on the local area network (LAN), rather than requiring each computer to retrieve updates from the update website individually, the Internet traffic load on the network is reduced. This process of sharing updates is called Rumor.

- 1 Each client computer checks the version of the most recent catalog file on the Internet site. This catalog file contains information for every component in the client software, and is stored in a digitally signed, compressed .cab file format.
 - If the version is the same as the catalog file on the client computer, the process stops here.
 - If the version is different from the catalog file on the client computer, the client computer attempts to retrieve the latest catalog file from its peers. It queries if other computers on the LAN have already downloaded the new catalog file.
- 2 The client computer retrieves the required catalog file (directly from the Internet site or from one of its peers) and uses it to determine if new components are available.
- 3 If new components are available, the client computer attempts to retrieve them from its peers. It queries whether computers on the LAN have already downloaded the new components.
 - If so, the client computer retrieves the update from a peer. (Digital signatures are checked to verify that the computer is valid.)
 - If not, the client computer retrieves the update directly from the update site.
- 4 On the client computer, the catalog file is extracted and new components are installed.

Updates through relay servers

Internet Independent Updating (IIU) enables computers to update the client software when they are not connected to the Internet.

At least one computer on the subnet must have an Internet connection to be able to communicate with the update site. That computer is configured to act as a relay server, and computers without an Internet connection use this computer to connect with the Internet and retrieve updates directly from the McAfee update site.

- 1 When a computer without Internet access fails to connect directly to the update site, it requests a response from a relay server on the LAN and uses that computer to communicate with the update site.
- 2 The computer without an Internet connection downloads updates directly from the update site through the relay server.

You can specify which computers function as relay servers when you install the client software or at a later time. See the installation guide for more information.

Management with the SecurityCenter

Your service provider sends you a unique URL and login credentials for your account, which you can use to log on to the SecurityCenter, a pre-configured, web-based management console for your account.

From the SecurityCenter, you can access tools to monitor the status of computers on your account, view reports on detections and activities, and configure security settings that address the specific needs of your account.



The Dashboard page is the "home page" of the SecurityCenter. It shows summary information for your account at-a-glance.

- **Alerts and action items** — Indicate whether any action is required to address security issues, and links you to instructions for resolving them.
- **Product coverage and activity summaries** — Modular reports (known as *widgets*) illustrate the current status of your account. These include reports on protection coverage (such as computers where protection is installed and enabled) and activity (such as the number of detections, emails, and website visits). The type, size, and placement of widgets can be customized.
- **Subscription tracking** — Widgets are available to show subscription and licensing information for your account. Click a button to install protection, create a trial subscription, renew or purchase a subscription, or buy additional licenses.
- **Links to related portals** — Some widgets contain a link to a portal used for managing non-client-based protection, such as SaaS email protection and SaaS vulnerability scanning.

The SecurityCenter offers two powerful tools for protecting and monitoring displaying your computers and fine-tuning their security settings.

- **User groups** — Create groups for computers that have one or more common characteristics. This enables you to view and manage them as a single entity when needed.
- **Customized policies** — Select settings for protection features, save them in a policy, and assign the policy to computers or groups of computers. This enables you to configure settings targeted specifically for each computer's environment and risk factors.

From the SecurityCenter, access important information and additional management tools.

- Installation wizard and links to remote installation methods.
- Detailed identification, activity, and detection data for the groups and computers on your account.
- Administrative reports.
- Policy configuration tools.
- Account configuration data, reference information, subscription status, and tools for managing your accounts and subscriptions.
- Helpful utilities.
- Product documentation and links to product support and demos.

Create user groups

A group consists of one or more computers that share a particular feature. They are used to help you manage computers more easily. Each computer running the client software belongs to a group.

You can place a computer in a group in several ways.

- Specify a group during installation.
- Move a computer into a group on the **Computers** page of the SecurityCenter.
- Import groups and computers from your network Active Directory structure, then synchronize modifications made to the Active Directory structure with the SecurityCenter as needed.

By default, computers are placed in the Default Group.

To create a new group, use the **Computers** page of the SecurityCenter.


How to use groups

Groups let you manage computers collectively rather than individually. If there aren't many computers on your account, you probably don't need to create groups. You should create groups only if they help you manage your computers more easily.

In large accounts, groups are an essential tool for managing computers. You can view all the computers in a group, view detections and reports for the group, and assign security settings (called *policies*) to a group as a single entity. You can base groups on geographic location, department, computer type, user tasks, or anything meaningful to your organization.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. You can then view details about this group of computers separately from other computers in your account. You can easily check detections for these computers or customize their security settings to protect them from the risks specific to users of public networks.

The following example shows how an administrator might configure policies for client computers in three different groups. You should configure policies for your users to meet your own company's needs.

Policy setting			
	Home Office Group On-site client computers	Sales Team Group Laptops	Administrator Group Site and group administrators
On-Demand Scan	Weekly	Daily	Daily
Enable outbreak response	Enabled	Enabled	Enabled
Scan within archives during on-access scans	No	Enabled	Enabled
Check for updates every	12 hours	4 hours	4 hours
Spyware Protection Mode	Prompt	Protect	Prompt
Approved Programs	None	None	Nmap remote admin tool
Firewall Protection Mode	Protect	Protect	Prompt
Use Smart Recommendations to automatically approve common Internet applications	Enabled	No	Enabled
Connection Type	Trusted network	Untrusted network	Trusted network
Allowed Internet Applications	AOL Instant Messenger	None	<ul style="list-style-type: none"> AOL Instant Messenger GoogleTalk
Access to Sites, Access to Downloads (Web Filtering)	<ul style="list-style-type: none"> Red — Block Yellow — Warn Unrated — Warn 	<ul style="list-style-type: none"> Red — Block Yellow — Block Unrated — Warn 	<ul style="list-style-type: none"> Red — Warn Yellow — Allow Unrated — Allow
Block phishing pages (Web Filtering)	Enabled	Enabled	Enabled

Customize policies

A policy is a collection of security settings that define how the product features operate. A policy is assigned to each computer when it is added to your account.

Policies allow you to assign different levels and types of protection to different users. Although policies are assigned to computers, it is common practice to assign the same policy to all the computers in a group.

The McAfee Default policy is preconfigured in the SecurityCenter. You cannot modify it, but you can create other policies on the **Policies** page of the SecurityCenter.

You can assign a policy to a computer in two ways.

- Specify a policy during installation.
- Assign a different policy on the **Computers** page of the SecurityCenter.

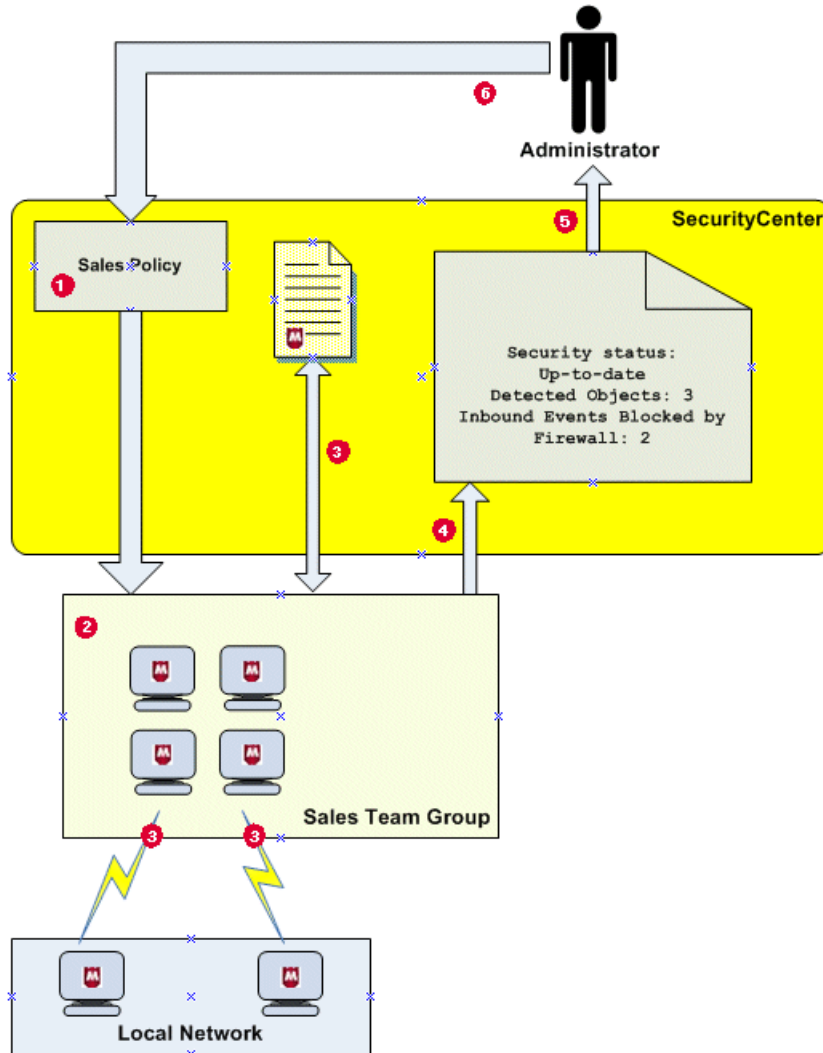
If you do not specify a different policy during installation, the default policy for your account is assigned. This is the McAfee Default policy, unless you have selected a different policy as the default for your account.

How to use policies

If there aren't many computers on your account, you probably don't need to create multiple policies. You should create policies only if they help you manage your computers more easily.

If computers on your account are used in different circumstances or for different purposes, creating different policies for them lets you change the way some settings are configured for them.

For example, you can assign a Sales policy to your mobile Sales Team group, with security settings that protect against threats in unsecured networks such as airports and hotels.



1	Create a Sales Team group and a Sales policy.
2	Assign the Sales policy to the computers in the Sales Team group.
3	Client software running on computers in the Sales Team group performs the tasks defined in the Sales policy: <ul style="list-style-type: none"> • Check for updates to software components and DAT files every 4 hours. • Check for an outbreak DAT file every hour. • Scan for viruses and potentially unwanted programs daily. • Block communication from computers on the local network (untrusted network).
4	Client software sends security data for each client computer to the SecurityCenter.
5	Administrator checks the security status for the Sales Team group in reports on the SecurityCenter.
6	The administrator adjusts the Sales policy. The modified policy is downloaded automatically to client computers in the Sales Team group the next time they check for updates.

Check reports

Whenever client computers check for updates, they upload information about their security status to the SecurityCenter.

This information includes the number and type of detections, the functional status of the client software, and any applications or communications that were approved by users or blocked. The method used to upload information is the same method used to retrieve updates (i.e., through a direct connection, Rumor technology, or a relay server).

A summary of this information is sent to you in a weekly status email (unless you or your service provider has disabled this feature). You can also retrieve detailed information in reports available on the SecurityCenter. Reports show the types of detections and activities occurring for computers on your account. Use them to evaluate the current policy options for your account and adjust them as needed.

You can also schedule these reports to run at regular intervals and be delivered to you or other specified persons as an email attachment.

2

Using the Client Software

McAfee SaaS Endpoint Protection client software is installed on each computer you want to protect. When installation is complete, the computer is added to your McAfee SaaS Endpoint Protection account automatically. The software then runs in the background to download updates to the computer, protect the computer from threats, and send detection data to the McAfee® SecurityCenter for use in administrative reports.

Typically, users have little interaction with the client software unless they want to manually scan for threats. User tasks are documented in the online user help on client computers.

As an administrator, you can use the SecurityCenter website to configure settings and monitor detections for the client computers on your account. Occasionally, you might work directly on a client computer by using the tasks described in this section.

Contents

- ▶ *How to access the client software*
- ▶ *Types of client software updates*
- ▶ *Performing setup and maintenance tasks*

How to access the client software

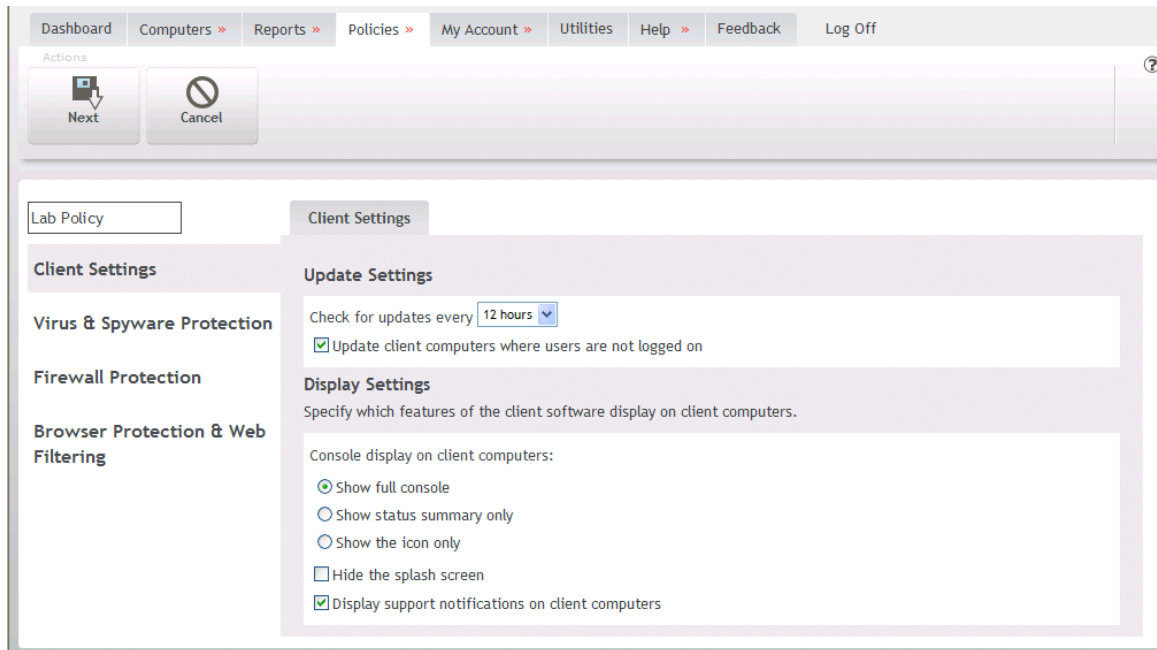
McAfee SaaS Endpoint Protection has two visual components for interacting with the client software.

- An icon that appears in the Windows system tray.
- A console that displays the current protection status and provides access to features.

The site administrator determines which components appear by configuring policy options and assigning them to client computers. The options are:

- Icon only, which allows access to only the menu options. They can view the status of the software (for example, when downloads are occurring) and perform manual updates.
- Icon and protection status summary, which allows access to a limited set of features.
- Icon and full console, which allows access to all features. This is the default setting.

Configure these policy options on the **Policies** page of the SecurityCenter, under **Client Settings**.



About the icon




The product icon appears in the Windows system tray. It provides access to the product's console and to some of the basic tasks performed on client computers.

Use the icon to:

- Check for product updates.
- Display online help.
- Open the console, to check the protection status and access features. (Available if the administrator configures this option for the computer.)
- Activate the copy of the software.
- Renew the subscription or buy more licenses.
- Log on as the site administrator. (Requires site administrator credentials.)

How the icon indicates the status of the client software

The appearance of the icon changes to indicate the status of the client software. Hold the cursor over the icon to display a message describing the current condition.

This icon...	...indicates:
	The product is active and there are no issues to be aware of.
	An update is in progress. Do not interrupt the Internet or LAN connection; do not log off the computer.
	One of these conditions exists: <ul style="list-style-type: none"> • The subscription for the product is expired. Renew it or contact the administrator. • The pre-installed or trial subscription is not activated. • The firewall protection service is disabled. • The last update failed to complete. Check the Internet or LAN connection and perform a manual update (click the icon, then select Update Now). • On-access scanning is disabled.

About the console

Check the protection status and access the features of the client software through the console. To display the console, use one of these methods:

- Double-click the product icon in the system tray.
- Click the icon, then select **Open Console**.
- Click **Start | Programs | McAfee | Managed Services | McAfee Security-as-a-Service**.

The basic console displays the status of the protection features installed on the computer.

- Detected risks are highlighted in red. Click **Fix** to resolve the risk.
- To access product features and perform tasks, click **Action Menu**, then select from the options:
 - **Product Details** — Display the full console with links to features and tasks.
 - **View Help** — Display online help.
 - **Scan Computer** — Select a scan target and begin scanning for threats.
 - **Set Connection Type** — Specify the type of network the computer connects to. This determines which communications firewall protection allows to access the computer.
 - **View Application List** — Specify applications that are allowed to access the Internet or blocked.



The client features that can be accessed are determined by policy options assigned to the computer.

Types of client software updates

Regular updates enable McAfee SaaS Endpoint Protection to ensure client computers are always protected from the latest threats.


To perform updates, the client software connects directly to a site on the Internet and checks for:

- Updates to the detection definition (DAT) files used to detect threats. DAT files contain definitions for threats such as viruses and spyware, and these definitions are updated as new threats are discovered.
- Upgrades to software components. (To simplify product terminology, both updates and upgrades are referred to as updates.)

Updates usually occur automatically in the background. Even computers without Internet access can retrieve updates through relay servers. In addition, users can perform on-demand (manual) updates at any time, and you can configure optional policy settings for updating tasks.

Client software is updated in these ways.

Type of update	Description
Automatic updates	<p>The software on each client computer automatically connects to the Internet directly or through a relay server and checks for updated components. McAfee SaaS Endpoint Protection checks for updates five minutes after a user logs on and at regular intervals thereafter.</p> <p>By default, computers check for new updates every 12 hours. You can change this interval by configuring a policy setting.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p>Automatic updates do not occur:</p> <ul style="list-style-type: none"> • On computers where a CHAP or NTML proxy is set up in Microsoft Internet Explorer. • When no user is logged on to a computer without an Internet connection that receives updates using a relay server. </div> <p>Pre-installed and CD-based versions of McAfee SaaS Endpoint Protection need to be activated before automatic updates occur. See the online user help for more information.</p>
Manual updates	<p>At times, users might want to check for updates manually. For example, when a computer appears to be out-of-date in your administrative reports, users might need to update manually as part of the troubleshooting process.</p>

Type of update	Description
Outbreak updates	<p>When an outbreak is identified by McAfee Labs, they issue an outbreak DAT, which is a special detection definition (DAT) file marked as Medium or High importance. It is specially encoded to inform the first computer receiving it to share the update immediately with other client computers on the network.</p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin: 10px 0;">  In rare cases, McAfee might send an EXTRA.DAT file with instructions for manually installing it. </div> <p>For maximum protection, configure your policies to check for an outbreak DAT file every hour. This feature is enabled by default.</p>
Updates when no user is logged on	<p>In most scenarios, McAfee SaaS Endpoint Protection supports terminal servers and the Windows fast user switching feature. When an update occurs, one session is designated as the primary update session. A pseudo user is defined, which enables automatic updates to occur on computers where no user is logged on.</p> <p>For certain configurations, automatic updates cannot occur. McAfee SaaS Endpoint Protection cannot create the pseudo user when:</p> <ul style="list-style-type: none"> • The computer is a domain controller. • Local security policies, including password restrictions, prevent the user's creation. • The computer receives updates through a relay server and no one is logged on. <p>When the pseudo user cannot be created, automatic updates do not occur. The pseudo user also cannot update if the computer is behind an authenticating proxy server or on computers where a CHAP or NTML proxy is set up in Internet Explorer.</p>

Terminal server support

McAfee SaaS Endpoint Protection supports updates for terminal servers and the Windows fast user switching feature.

These updates are supported in most scenarios, with these limitations:

- When an update occurs on a terminal server, one session is designated as the primary update session for restrictions that apply to automatic updates.
- For all user sessions, the product icon is removed from the system tray during the installation or update. The icon is restarted only for the user logged on to the primary update session. All user sessions are protected, and other users can manually redisplay their icons by clicking **Start | Programs | McAfee | Managed Services | McAfee Security-as-a-Service**.
- Detection notifications are not displayed on the desktop of all computer users if the fast user switching feature is enabled.

Specifying when computers check for updates

Use this task to select how often client computers check for updates to software components and DAT files. By default, they check every 12 hours.

For virus and spyware scans to detect all the latest threats, the detection definition (DAT) files must be kept up-to-date. DAT files are updated by McAfee Labs whenever new threats are discovered.

Task

For option definitions, click ? in the interface.

- 1 In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Client Settings**.
- 3 On the Client Settings tab, under Update Settings, select a frequency from the **Check for updates every** list.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Updating client computers manually

Use this task to check for and download updates to detection definition (DAT) files and software components on client computers.

Manual updates are also called *on-demand updates*.

Task

- Click the product icon in the system tray, then select **Update Now**.
 - A panel shows the progress of the update.
 - When the update is completed, the panel displays the date of the last update and a list of files that were downloaded.
 - The panel closes automatically after the update is completed.

Disabling updates for non-logged on users

Use this task to prevent failed automatic updates from being reported as errors when requirements cannot be met for updating computers where no user is logged on.

Task

For option definitions, click ? in the interface.

- 1 In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Client Settings**.
- 3 On the Client Settings tab, under Update Settings, deselect **Update client computers where users are not logged on**.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Performing setup and maintenance tasks

Use these tasks to set up and monitor the general features of the McAfee SaaS Endpoint Protection client software.

See the online help on the client computer for more information about performing tasks with the client software.

Tasks

- [Testing virus protection on page 33](#)
Use this task to test the virus-detection feature of the virus and spyware protection service by downloading the EICAR Standard AntiVirus Test File at the client computer
- [Changing the language for the software on page 33](#)
Use this task at the client computer to change the language at any time.
- [Viewing information about the client software on page 34](#)
Use this task to check general information for the client software.
- [Logging on as a site administrator on page 34](#)
Use this task to log in to a client computer as a site administrator, which makes the full console and some additional tasks available.
- [Configuring notifications on page 35](#)
Use this task to specify whether notifications display on client computers to let users know that support is ending for their operating system.
- [Configuring what users see on page 35](#)
Use this task to select which components of the client software are displayed on client computers.
- [Uninstalling the client software on page 35](#)
Use this task at a client computer to remove the client software.

Testing virus protection

Use this task to test the virus-detection feature of the virus and spyware protection service by downloading the EICAR Standard AntiVirus Test File at the client computer

Although it is designed to be detected as a virus, the EICAR test file is not a virus.

Task

- 1 Download the EICAR file from the following location:
<http://www.eicar.org/download/eicar.com>
If installed properly, the virus and spyware protection service interrupts the download and displays a threat detection dialog box.
- 2 Click **OK**, then select **Cancel**.



If installed incorrectly, the virus and spyware protection service does not detect the virus or interrupt the download process. In this case, use Windows Explorer to delete the EICAR test file from the client computer, then reinstall McAfee SaaS Endpoint Protection and test the new installation.

Changing the language for the software

Use this task at the client computer to change the language at any time.

By default, the client software uses the address that was submitted when the client software was purchased or activated to determine the language. (If that language is not supported on the computer, the one most closely matching is used.)

Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the **Action Menu**, select **Product Details**.
- 3 In the SecurityCenter Communication area, click **Select Console Language**.

- 4 Select **Use the specified custom language**, then select a language from the drop-down list.
- 5 Close the console, then re-open it (by repeating step 1).
The console appears in the selected language.

Viewing information about the client software

Use this task to check general information for the client software.

This information might also be required by product support for troubleshooting.

Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the Action Menu, select **Product Details**.
- 3 Under SecurityCenter Communication, check the details listed.

Detail	Description
Product version	The version of the client software.
Last update check	The last date when the computer checked for updated files.

- 4 View information about each protection service in its section of the console.
- 5 Click **Back** to return to the console.

Logging on as a site administrator

Use this task to log in to a client computer as a site administrator, which makes the full console and some additional tasks available.

- Viewing the status of scheduled scans that are in progress
- Disabling and enabling on-access scanning
- Synchronizing Active Directory information

Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the Action Menu, click **Product Details**.
- 3 From the SecurityCenter Communications section, select **Admin Login**.
- 4 Type your login credentials for the SecurityCenter, which were sent to you in a Welcome email when you purchased McAfee SaaS Endpoint Protection.
 - **Email address** — The email address used to sign up for McAfee SaaS Endpoint Protection.
 - **Password** — In most cases, the password you created when signing up.
- 5 Click **Submit**.

Options for performing administrative tasks appear in the console.

See also

Viewing scheduled scans on page 78

Enabling and disabling on-access scanning on page 79

Synchronizing Active Directory groups on page 52

Configuring notifications

Use this task to specify whether notifications display on client computers to let users know that support is ending for their operating system.

By default, the client software displays notifications:

- When upgrades to product components, such as the scanning engine, are scheduled to end or will end within 30 days.
- When updates to detection definition (DAT) files have ended or will end within 30 days.

Task

For option definitions, click ? in the interface.

- 1 In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Client Settings**.
- 3 On the Client Settings tab, under Display Settings, select or deselect **Display support notifications**.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Configuring what users see

Use this task to select which components of the client software are displayed on client computers.

Task

For option definitions, click ? in the interface.

- 1 In the SecurityCenter, click the **Policies** tab, then click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Client Settings**.
- 3 On the Client Settings tab, under Display Settings, select an option for **Console display on client computers**.
 - **Show full console** — All client software options are displayed.
 - **Show status summary only** — The tray icon and menu are displayed, and users can open the console to display only the status of protection features on their computer.
 - **Show the icon only** — The tray icon is displayed, and the tray menu lists only the **Update Now** option.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Uninstalling the client software

Use this task at a client computer to remove the client software.

You might need to do this for testing purposes or before reinstalling the client software. (Note that some protection services, such as the SaaS protection services, do not include a client software component.)



If you uninstall the client software, the computer is no longer protected. We recommend that you reinstall as soon as possible.

Task

- 1 Close the Microsoft Outlook and Internet Explorer applications.
- 2 In the Windows Control Panel, open **Add/Remove Programs** or **Programs and Features**.
- 3 Select the protection services uninstall, then click **Remove** or **Uninstall**.
 - **McAfee Virus and Spyware Protection Service**
 - **McAfee Firewall Protection Service**
 - **McAfee Browser Protection Service**



On computers running the Windows firewall, the setting for the Windows firewall is automatically restored to the setting that was in effect before the client software was installed. If the Windows firewall was enabled then, it is re-enabled automatically now.

3

Using the SecurityCenter

Use the McAfee® SecurityCenter administrative website to centrally manage all the client computers and protection information for your account.

After installing the software on client computers, you receive regular emails that summarize the security status of all client computers on your account, and notify you of actions required to address vulnerabilities. Status emails contain a link to the SecurityCenter, where you can view detailed reports and instructions for resolving problems.

McAfee SaaS Endpoint Protection is designed to protect your computers automatically with little or no hands-on management. In small organizations, status emails might be all that is needed to assure you that your computers are safe. If you manage a large account or want more proactive, hands-on involvement, you can take advantage of the management console available on the SecurityCenter.

Contents

- ▶ *The SecurityCenter*
- ▶ *Protection status at a glance*
- ▶ *Management of client computers*
- ▶ *Management of computer groups*
- ▶ *Management of Active Directory groups*
- ▶ *Management of group administrators*
- ▶ *Management of security policies*
- ▶ *Generation of security reports*
- ▶ *Management of your account*
- ▶ *Utilities*
- ▶ *Getting assistance*

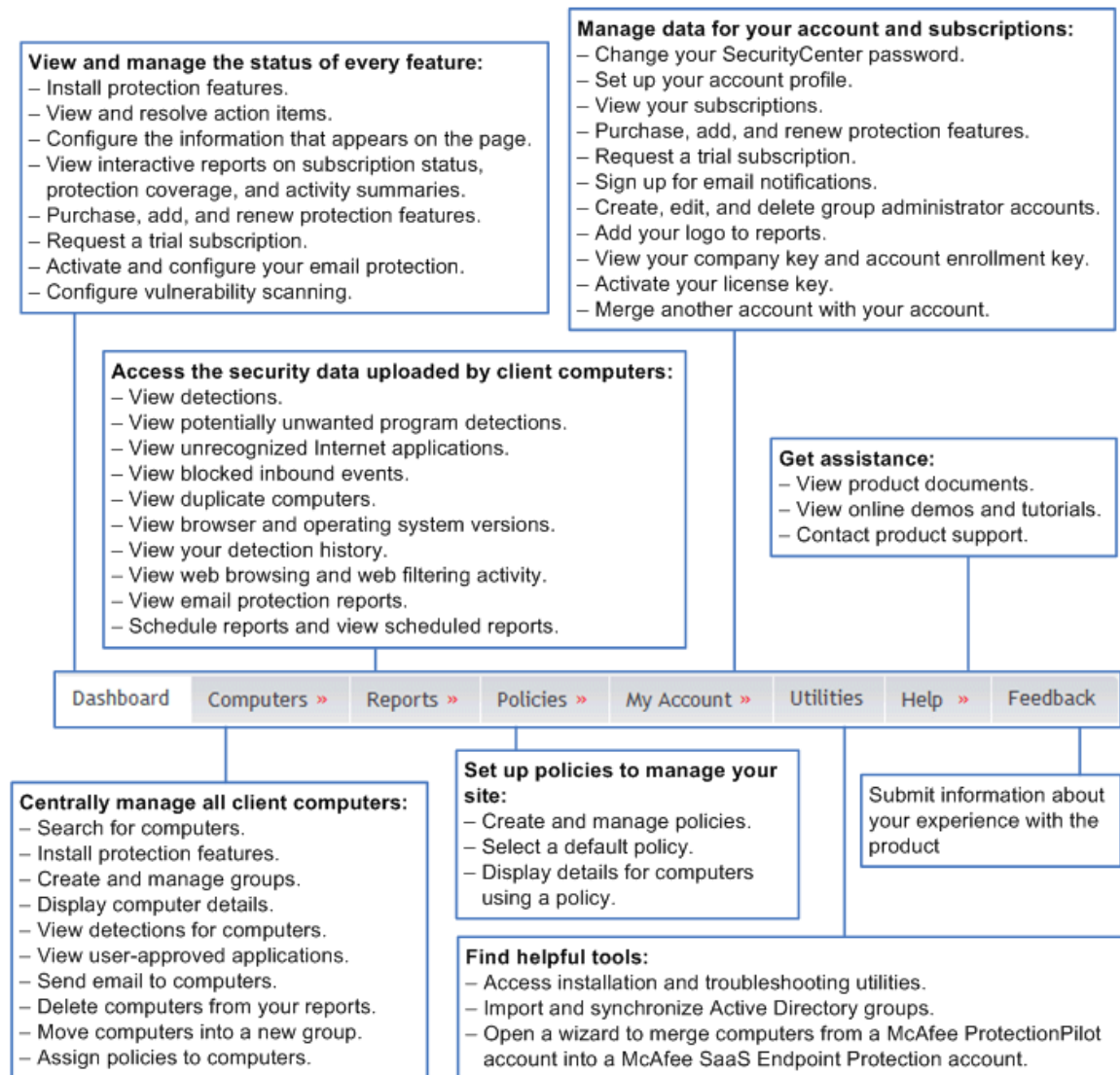
The SecurityCenter

The SecurityCenter offers a management console for monitoring the protection status of computers on your account and assessing their security needs.

Administrative features are divided among eight pages:

- Dashboard
- My Account
- Computers
- Utilities

- Reports
- Policies
- Help
- Feedback



Logging on to the SecurityCenter

Use this task to log on to the SecurityCenter and access administrative features.

Task

- 1 Paste or type the URL into your browser.
- 2 Type your login credentials.
 - **Email address** — The email address that you used to sign up for McAfee SaaS Endpoint Protection.
 - **Password** — In most cases, the password that you created when signing up. If you have forgotten your password, click the link and it will be emailed to you at the login email address.
- 3 Click **Log On**.


Accessing data on SecurityCenter pages

Each SecurityCenter page includes features for displaying the exact data you need and using it efficiently.

The screenshot shows the SecurityCenter interface with the following elements:

- Navigation:** Dashboard, Computers, Reports, Policies, My Account, Utilities, Help, Feedback, Log Off.
- Actions:** Install Protection, Manage Groups.
- Filters:** Report period: Last 7 days; View by: Computers; Group: All; Status: All; Policy: All.
- Search:** Find computers: [input field] Search.
- Table:** A table with columns: Computer, Group, Policy, Email, Last Connect, DAT Date, Detections, User-Approved Applications. It lists several computers like LabMachine-3, LabMachine-2, LabMachine-1, JohnDavies_Laptop, HumanResources-1, Computer-1, and AccountingMachine-1.
- Actions:** Email, Delete, Move to Group, Assign Policy.
- Page Info:** Show: 10 | 25 | 50 | 100 | 500 | 1000 | 7 record(s) [Page 1 / 1]

When you want to...	Do this...
Send the current page as an email attachment or scheduled report	Click the email icon (located along the upper-right margin of the page) to open the Scheduled Reports page, which contains a blank email message to fill out and delivery options. You can configure the message to be sent immediately or at regular intervals, then click Save . (You must have a local email application installed to use this feature.)
Print the current page	Click the print icon (located along the upper-right margin of the page) to open the page in a separate browser window, then select Send to Printer to open the Windows Print dialog box.
Save the current page as a file	Click the save icon (located along the upper-right margin of the page), then select the file format: <ul style="list-style-type: none"> • Microsoft Excel • Microsoft Word • Adobe PDF • Comma-separated text
Display context-sensitive help	Click the help (?) icon (located along the upper-right margin of the page) to display help for the current page, with links to related topics.
Navigate in multiple-page listings	Click the number of entries to display, or select a page number from the Go to page drop-down list.
Select computers to manage	Select the checkbox for individual computers, or select the checkbox in the heading to select all computers.
Check your action items and alerts	Problems that require your attention appear in red. The method for resolving them varies depending on the page. <ul style="list-style-type: none"> • In an action item, click the button at the end of the text to display instructions for resolving the problem. • In a computer listing, click the name of the computer to display details about it, then click the action item.
Display details about a computer	Click a computer name in a listing.

When you want to...	Do this...
Send email to a computer	Click an email address in the listing to open a blank, preaddressed message. (You must have a local email application installed to use this feature.)
Filter information on a page	At the top of a page, select the information to display (such as group name, period of time, or type of information).  For greater flexibility in managing large accounts, select whether to display groups or individual computers.
Sort information in listings	Click a column heading to sort by that column. Click it again to switch the order in which it is displayed (ascending order or descending order).

Protection status at a glance

The **Dashboard** page is your “home” page on the SecurityCenter website.

It provides a graphical overview of your coverage, with instant access to summary information about the computers and subscriptions in your account. Access the Dashboard page at any time by clicking the **Dashboard** tab.

- Install additional protection.
- View and resolve action items.
- View protection coverage and activity for all computers or specific groups with interactive reports (known as *widgets*) containing clickable charts and links.
- Check and update your subscriptions and licenses.

- Select, resize, and reposition the widgets that appear on the page.
- Access associated management portals or dashboards by clicking a link (available only when your account includes SaaS protection services or email server protection).

The screenshot displays the McAfee SecurityCenter dashboard with the following components:

- Navigation:** Dashboard, Computers, Reports, Policies, My Account, Utilities, Help, Feedback, Log Off.
- Actions:** Install Protection, Add Widget, Restore Default.
- Alerts:** Update Protection: 2 computer(s) are not protected against the latest threats. [Dismiss Alert] [Update Protection]
- Protection Coverage Widgets:**
 - Virus & Spyware Coverage:**

Computers	Status
1 (14%)	Up-to-Date
2 (28%)	Out-of-Date
4 (57%)	Not Installed
 - Browser Protection Coverage:**

Computers	Status
5 (71%)	Installed
2 (28%)	Not Installed
 - Firewall Coverage:**

Computers	Status
3 (42%)	Installed
4 (57%)	Not Installed
- Activity and Summary Widgets:**
 - Email Activity:** Status Messages: Virus (1000), Spam (1781), Clean (593). [Click here to configure]
 - Browser Protection 30-day Summary:** Line graph showing ratings (Red, Yellow) over the last 30 days.
 - Web Filtering 30-day Summary:** Line graph showing actions (Blocked, Warned-Continued, Warned-Cancelled) over the last 30 days.
- Vulnerability Scanning:** Bar chart titled "Vulnerability/Severity" showing counts for Low, Medium, High, Critical, and Urgent categories. Data as of 6/9/2009 7:50:45 PM.
- Subscription Summary Table:**

Protection Software	Type	Licenses in Use	Licenses purchased	Expiration	Add Protection
Virus and spyware protection	Subscription	3	15	6/9/2010	Buy More Renew
Firewall protection	Subscription	3	15	6/9/2010	Buy More Renew
Email protection	Subscription	10	15	6/9/2010	Buy More Renew
Vulnerability scanning	Subscription	8	1	6/9/2010	Buy More Renew
Web Filtering	Subscription	5	15	6/9/2010	Buy More Renew

Viewing protection at a glance

Use this task to view details about your account and protection coverage, resolve action items, and update protection.

Task

- 1 Click the **Dashboard** tab.
- 2 Select the group for which you want to display information. *(Optional)*
- 3 Do any of the following:

To...	Do this...
View instructions to resolve an action item	Click the button at the end of the text. Action items are security issues that need your immediate attention.
Install additional protection	Click Install Protection to open a wizard that guides you through the steps for installing protection on new or existing computers.
Add clickable charts and graphs (widgets) to the page	Click Add Widget , select a chart or graph, then click Add to Dashboard .
Redisplay the default page configuration	Click Restore Defaults .
View details about protection coverage	In a widget, click a color in the pie chart that shows the status of client computers in your account. <ul style="list-style-type: none"> • Red — Out-of-date or unprotected systems. • Green — Up-to-date or protected systems. • Gray — Computers where protection is not installed.
Update protection	In the Subscription Summary widget, click Buy , Buy More , or Renew , then follow the instructions on the Product Purchase page.
Create trial subscriptions	Click the Try link in the Subscription Summary widget, or in a widget for a type of protection not included in your account.
Customize the appearance of the page	<ul style="list-style-type: none"> • To remove a widget, click its close box (in the upper-right corner). • To reposition a widget, click its title bar and drag it to a new location. • To resize a widget, click its border and drag to a new size. • To email the information in the widget, click the email icon (in the upper-right corner). You can also schedule it to be sent as an email attachment at regular intervals.

Working with widgets

Use this task to view, manage, and access information in widgets.

Widgets are small, interactive reports that appear on the Dashboard page of the SecurityCenter. They provide summary and overview information about your account's protection status, activity, and subscriptions. Some widgets provide links to associated portals or subscription-related tasks.

You can add new widgets, remove widgets, and customize the way widgets appear.

Task

- 1 Click the **Dashboard** tab.
- 2 Do any of the following:

To...	Do this...
View details about protection coverage	In a widget, click a color in the pie chart that shows the status of client computers in your account. <ul style="list-style-type: none"> • Red — Out-of-date or unprotected systems. • Green — Up-to-date or protected systems. • Gray — Computers where protection is not installed.
View details about activity	In a widget, click links that display more information about reported activity, such as the computer names or the number of detections.
Buy or renew subscriptions and licenses	Click links in the Subscription Summary widget.
Create trial subscriptions	Click the Try link in the Subscription Summary widget, or click a link in a widget for a type of protection not included in your account.
Open a protection portal in a separate browser window	Click the Click here to configure link in a SaaS email protection or vulnerability scanning widget. (Available only when your subscription includes these types of protection.)
Remove a widget	Click its close box (in the upper-right corner).
Reposition a widget	Click its title bar and drag it to a new location.
Resize a widget	Click its border and drag to a new size. (Two sizes are available.)
Email the information in the widget	Click the email icon (in the upper-right corner), then select delivery options to send it now or schedule it to be sent at regular intervals. (You must have a local email application installed to use this feature.)
Add widgets to the page	Click Add Widget , locate the widget you want to display in the gallery, then click Add to Dashboard .

Management of client computers

The **Computers** page provides a centralized location for working with all the computers in your account.

You can instantly view each computer's group and email address, when it last connected to the network, whether its detection definition (DAT) file is current, the number of detections, and the number of Internet applications approved by its user. You can easily see which computers need your attention, display additional information, and perform necessary management tasks.

On the SecurityCenter, click the **Computers** tab to display the Computers page, which lists all the computers or groups in your account or only the computers in a selected group.



The Computers page lists up to 5000 computers. For larger accounts, we recommend organizing your computers into groups of no more than 100 computers to optimize SecurityCenter performance.

Computer	Group	Policy	Email	Last Connect	DAT Date	Detections	User-Approved Applications
LabMachine-3	Lab Group	Lab Policy	CB2@mcafee.com	8/5/2010 2:56:55 AM	7/13/2009	0	0
LabMachine-2	Lab Group	Lab Policy	NT_AUTHORITY\SYSTEM	8/5/2010 12:56:55 PM	7/13/2009	0	3
LabMachine-1	Lab Group	Lab Policy	computer1@mcafee.com	8/5/2010 12:56:55 PM	7/13/2009	16	0
JohnDavies_Laptop	Default	McAfee Default	John_Davies@demo.com	8/5/2010 1:56:55 PM	7/1/2009	0	0
HumanResources-1	Default	McAfee Default	NT_AUTHORITY\SYSTEM	8/5/2010 12:29:52 AM	5/19/2009	0	3
Computer-1	Default	McAfee Default	computer1@mcafee.com	8/4/2010 2:56:55 AM	7/1/2009	0	0
AccountingMachine-1	Default	McAfee Default	NT_AUTHORITY\SYSTEM	8/5/2010 12:27:52 PM	6/30/2009	14	0

From the Computers page you can click a computer name to display details of the individual computer on the **Computer Details** page.

See also

Management of security policies on page 56




Management of computer groups on page 48

Working with computers

Use this task to manage client computers from the **Computers** page.

Task

- On the Computers page, select information filters to determine what you want to appear at the bottom of the page:
 - Report period** — Specify the length of time for which to display information.
 - View by** — Display individual computers or groups.
 - Group** — Display only the computers in a group or display all computers. (Not available if you selected **View | Groups**.) If your account includes Active Directory groups, an icon appears to the right of the list; click the icon to display a tree view, then select a group.
 - Status** — Show all computers, out-of-date computers, computers with detections, or computers you have blocked from receiving updates.
 - Policy** — Show all computers or only those assigned a particular policy.
- Do any of the following:

To...	Do this...
Find one or more computers	Type the full or partial name of a computer in the Find Computers box and click Search .  The computer search feature does not recognize wildcard characters, so type letters or numbers only. Site administrators can search the entire account; group administrators can search only the groups their site administrator has assigned to them.
Add one or more computers	Click Install Protection to open the installation wizard, which guides you through the steps for installing protection on new or existing computers.
View or edit details for a computer	Click a computer name to display the Computer Details page for that computer.
Add user-approved applications to one or more policies	<ol style="list-style-type: none"> Click a quantity under User-Approved Applications. In the User-Approved Applications List, click Allow, select the policies to add the approved applications to, then click Save.  The User-Approved Applications List shows detected programs that users have approved to run on the computer. To prevent users from approving applications, configure policy options for Protect mode.
Send email to users about their computer's problems or tasks they need to perform	Click an email address for a computer. Alternatively, select the checkbox for multiple computers in the list, then click the Email button. A blank preaddressed email message appears. (You must have a local email application installed to use this feature.)
Delete obsolete or duplicate computers from the listing	Select the checkbox for one or more computers in the list, then click Delete .  Deleting a computer does not remove the client software. If you mistakenly delete a computer with enabled client software from the listing, it automatically reappears the next time its report data is uploaded; however, you can no longer view its historical detection data.
Move computers into a group	Select the checkbox for one or more computers in the list, then select an existing group from the Move to Group list.

To...	Do this...
Assign a policy to computers	Select the checkbox for one or more computers in the list, then select an existing policy from the Assign Policy list.
View detections for a computer	Click a quantity under Detections to open the Detections List, then click a detection name to view detailed information from the McAfee Labs Threat Library.



Working with an individual computer

Use this task to manage an individual computer on the **Computer Details** page.

This page displays information about the computer, its service components, and its detections. It lists the date and status for the last update and scan.

Task

- 1 From a computer listing, such as the Computers page, click a computer name.
- 2 On the Computer Details page, do any of the following:

To...	Do this...
Update the email address	In the System email address box, type a new email address, then click Save .
Move the computer to a new group	In the Group list, select a group, then click Save .
Assign a new policy	In the Assign Policy list, select a new policy, then click Save .
Install protection on an unprotected computer	Select the Click here to install link to open the installation wizard.
Display instructions for resolving an action item	Under Action Items, click the action item.
Display details about detections	In the Detections section, click a quantity under Detections or User-Approved Applications to display a detailed listing.
Add user-approved applications to one or more policies	<ol style="list-style-type: none"> 1 In the Detections section, click a quantity under User-Approved Applications. 2 In the User-Approved Applications List, click Allow, select the policies to add the approved applications to, then click Save. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  The User-Approved Applications List shows detected programs that users have approved to run on the computer. To prevent users from approving applications, configure policy options for Protect mode. </div>
View attempted visits to blocked websites	<p>In the Detections section, click a quantity under Blocked Sites to open a page that lists details about each attempted visit.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  This feature is available only when web browsing policy options are enabled in versions of McAfee SaaS Endpoint Protection that include the web filtering module. </div>

Identifying duplicate computers


Use this task to find computers listed more than once in your reports and delete them from your account.

Duplicate listings usually result when the client software has been installed more than once on a single computer or when users install it on their new computers without uninstalling it from their previous computers. This causes the number of installations for your account to be reported incorrectly.

Task

For option definitions, click ? in the interface.

- 1 Click the Reports tab, then click **Duplicate Computers**.
- 2 In the Duplicate Computers report, perform a task.

When you want to...	Do this...
Delete duplicate computers	<p>Select the checkbox for each duplicate computer listed, then click Delete.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> Deleting a computer does not remove the client software. If you mistakenly delete a computer with enabled client software from the listing, it automatically reappears the next time its report data is uploaded; however, you can no longer view its historical detection data.</p> </div>
View details about a computer	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.

Identifying Microsoft product versions on computers

Use this report to locate computers for maintenance, such as installing Microsoft software patches. You can also check shows whether computers are configured as relay servers, group information, and the version of software and DAT files.

Task

For option definitions, click ? in the interface.

- 1 On the Reports tab, click **Computer Profiles**.
- 2 In the Computer Profiles report, perform a task.

When you want to...	Do this...
Identify computers running an operating system that needs an update or patch installed	Filter the listing to display only computers running the specific operating system.
Identify computers running a browser that needs to be updated	Filter the listing to display only computers running the specific browser.
Send email notifying users about issues or maintenance specific to their operating system or browser	Select the checkbox for each applicable computer, then click Email to open a blank message to fill in and send. (You must have a local email application installed to use this feature.)
Locate group information for computers	Check the name and number of the group for each computer. (The group number is the group ID required when using the silent installation method (VSSETUP) to install client software.)

When you want to...	Do this...
See which computers are configured as relay servers	Check the Relay Server column.
Check details about the files running on computers	Check the version of the DAT file and the client computer software (agent build number).

Upgrading the client software

When a new version of the client software becomes available, you can schedule an upgrade for selected computers. This lets you test the new version before deploying it to all computers.

An action item on the **Dashboard** page of the SecurityCenter notifies you when a new version of the software is available.



You can't schedule upgrades for client computers that are configured as relay servers. Relay servers are updated during the first scheduled upgrade for client computers that are not configured as relay servers.

Task

For option definitions, click ? in the interface.

- On the **Software Upgrade** tab of the **Utilities** page, do any of the following:

To do this...	Do this...
Schedule an upgrade	<ol style="list-style-type: none"> 1 Select the computers you want to upgrade. 2 Click the calendar icon that appears above the computer listing, then select a month and a day. 3 Click Schedule My Upgrade.
Modify a scheduled upgrade	<ol style="list-style-type: none"> 1 Select the computers. 2 Click Clear Date. 3 Click the calendar icon that appears above the computer listing, then select a month and a day. 4 Click Schedule My Upgrade.
Cancel an upgrade.	<ol style="list-style-type: none"> 1 Select the computers. 2 Click Clear Date.

Management of computer groups

A group consists of one or more computers that share a particular feature.

You can create groups that are based on geographic location, department, computer type, the tasks performed by the users, or anything meaningful to your organization.

By default, every computer in your account is placed into a group called Default Group. You can create other groups in the SecurityCenter, then move computers into them. You can also import Active Directory groups from your network.

Why use groups?

Groups help you manage large numbers of computers or computers that use different security settings (defined in policies). They allow you to manage computers collectively rather than individually.

Groups are particularly helpful in larger organizations or companies that are widely distributed geographically. Placing similar computers into a single group enables you to view and manage security issues for the group separately from the other computers in your account.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. Then you can configure special security settings for those computers to provide greater protection against threats in unsecured networks such as airports and hotels. You can also track the number of detections on those computers through more frequent reports and adjust the security settings as needed.

Tips for large accounts

To more efficiently monitor large accounts and optimize SecurityCenter performance, we recommend that you organize your computers into groups of no more than 100 computers. This enables you to use the View filter to display reports and computer status by group, then drill down to see the individual computers within a group as needed.

How can I manage groups?

The **Manage Groups** page displays the groups in your organization. Access the page by clicking the **Manage Groups** button on the Computers page. If you have not created any groups or policies, only the Default Group is displayed.

Active Directory support

If you use Active Directory to define group hierarchies in your network, you can import the organizational unit (OU) structure into the SecurityCenter, then install the client software, assign policies, and view reports based on the imported groups of computers. Keep information in the SecurityCenter up-to-date by scheduling a synchronization utility to run at regular intervals.

The Default Group

Until you create additional groups, all computers are assigned to the Default Group when the McAfee SaaS Endpoint Protection client software is installed. If you delete a group that contains computers, they are moved into the Default Group. You cannot change the name of the Default Group.

After you create additional groups, you can assign computers to them during the installation process or move computers into them at a later time.

See also

Management of Active Directory groups on page 50

Management of group administrators on page 53

Management of security policies on page 56



Management of client computers on page 43

Working with groups

Use this task to create and configure groups in the SecurityCenter.

Task

- 1 Click the **Computers** tab, then click **Manage Groups**.
- 2 On the Manage Groups page, click an icon for flat view or tree view.
This changes the format in which groups are listed. (Available only if you have imported Active Directory groups.)
- 3 Do any of the following:

To...	Do this...
Create a group	<ol style="list-style-type: none"> 1 Click Add Group. 2 Type a name for the group. 3 Select the computers to add to the group. 4 Click Save.
View computers in a group	Under Computers , click a number to display the Computers page showing all the computers in the group.
Rename a group	<p>Under Action, select Rename, specify a new name for the existing group, then click Save.</p> <p> You cannot rename the Default Group or Active Directory groups.</p>
Delete a group	<p>Under Action, select Delete, then click OK. If you delete a group that contains computers, they will be moved into the Default Group.</p> <p> You cannot delete the Default Group or Active Directory groups.</p>

Management of Active Directory groups

If you use Active Directory to define group hierarchies in your network, you can import the organizational unit (OU) structure into the SecurityCenter.

- 1 Download the Active Directory Synchronization utility.
- 2 Run the utility to import Active Directory groups from your network.
- 3 Install the client software on computers in your Active Directory groups. You can select a policy to assign during the installation process.
 - Create and send an installation URL to users to install on their computers.
 - Run a utility to "push" the software to multiple computers directly from the service provider's website.
- 4 Schedule a time for the Active Directory Synchronization utility to run on a regular basis to import any modifications made to the network Active Directory structure. This ensures that the information in the SecurityCenter stays up-to-date.
- 5 Check the status of the last synchronization tasks.

Your account can contain both Active Directory groups and groups that you create in the SecurityCenter.

See also

[Management of computer groups on page 48](#)

Downloading the Active Directory synchronization utility

Use this task to download a utility that imports Active Directory groups from your network into the SecurityCenter.

Run this task on an administrative computer that has a connection to an Active Directory server.

Task

For option definitions, click ? in the interface.

- 1 On the Utilities page, click the **Active Directory Synchronization** tab.
- 2 Click **Download**.

Importing Active Directory groups

Use this task to import Active Directory groups from your network into the SecurityCenter.

Before you begin

You must download the Active Directory synchronization utility before you can perform this task.

Perform this task at an administrative computer has the client software installed and a connection to the Active Directory server.

Task

For option definitions, click ? in the interface.

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the Action menu, select **Product Details**.
- 3 In the client console, select **Synchronize Active Directory**.
- 4 Enter your Active Directory credentials, the name and port for the Active Directory server, and your credentials for logging in to the SecurityCenter, then click **Log On**.
The utility establishes a connection with the SecurityCenter and the Active Directory server.
- 5 Select the **Remember my credentials** option.
This allows the utility to access the information on the Active Directory server the next time it runs. This option must be enabled for the utility to run on a scheduled basis to keep the information on the SecurityCenter up-to-date.
- 6 Select the groups to import, then click **Import**.
You can select only the groups for which you entered credentials.
- 7 When the utility has finished importing your selection, click **Launch SecurityCenter** to proceed with installing client software.

Installing on Active Directory groups

Use this task to install the client software on computers in Active Directory groups.

Before you begin

You must import Active Directory groups before you can perform this task.

Note that all Active Directory organizational information is retained in the SecurityCenter. You cannot move Active Directory computers into groups that you have defined in the SecurityCenter, and no group selection options are displayed during the installation process.

Task

For option definitions, click ? in the interface.

- In the SecurityCenter, select a method for installing the client software on the imported computers.
 - On the Dashboard page, click **Install Protection**, and follow the steps in the installation wizard for creating a URL to send to users. This allows them to install the software on their computers.
 - On the Utilities page, click the **Active Directory Configuration** tab, then under **Push Install utility** click **Download** to get a utility that "pushes" the software to multiple computers. Version 2.0 of the Microsoft .NET Framework redistributable package must be installed on the administrative computer to run the Push Install utility.

When you run the Push Install utility, you select the Active Directory groups, the software to install, a policy to assign, and whether to scan the computer for threats when installation is complete. Click the help link (?) in the utility for online assistance.

Synchronizing Active Directory groups

Use this task to update the SecurityCenter with any modifications made to the Active Directory structure on the network by scheduling a synchronization utility.

The synchronization utility runs on a regular basis to keep the information synchronized automatically.



In the utility, the **Remember my credentials** option must be selected for the utility to run on a scheduled basis. This allows the utility to access information on the Active Directory server.

Task

For option definitions, click ? in the interface.

- 1 On the Utilities page, click the **Active Directory Synchronization** tab.
- 2 Under Synchronization Schedule, select **Enable scheduled synchronization**.
- 3 Select a day of the week or month to run.
- 4 If you want any groups that are part of the Active Directory structure on your network to be created in the SecurityCenter automatically, select **Allow group creation**.
If you select this option, computers will be placed in the same groups they are in on your network.
If you do not select this option, computers will be placed in the Default Group.
- 5 Click **Save**.

See also

[Logging on as a site administrator on page 34](#)

Viewing the synchronization status

Use this task to display details about the most recent activity to synchronize Active Directory groups in the SecurityCenter with your network.

Task

For option definitions, click ? in the interface.

- 1 On the Utilities page, click the **Active Directory Synchronization** tab.
- 2 Under Synchronization Status, check the last time the synchronization utility ran.
- 3 Click **View synchronization history**.

A page lists up to 25 computers that ran the synchronization task and the results.

Viewing the Active Directory tree in the SecurityCenter

Use this task to view Active Directory computers and groups you have imported into the SecurityCenter.

Task

For option definitions, click ? in the interface.

- Perform one of these tasks.
 - On the Utilities page, click the **Active Directory Synchronization** tab, then click **Active Directory Structure** to open a page showing the Active Directory tree for your account.
 - On any page with a **Groups** filter, click the icon that appears to the right of the drop-down list to open a page where you can select computers or groups.
 - On pages that display a group listing, click the viewing icon for the tree view. The viewing icons, which appear just above the left top corner of the group listing, select a flat listing of group paths and names or a tree view.

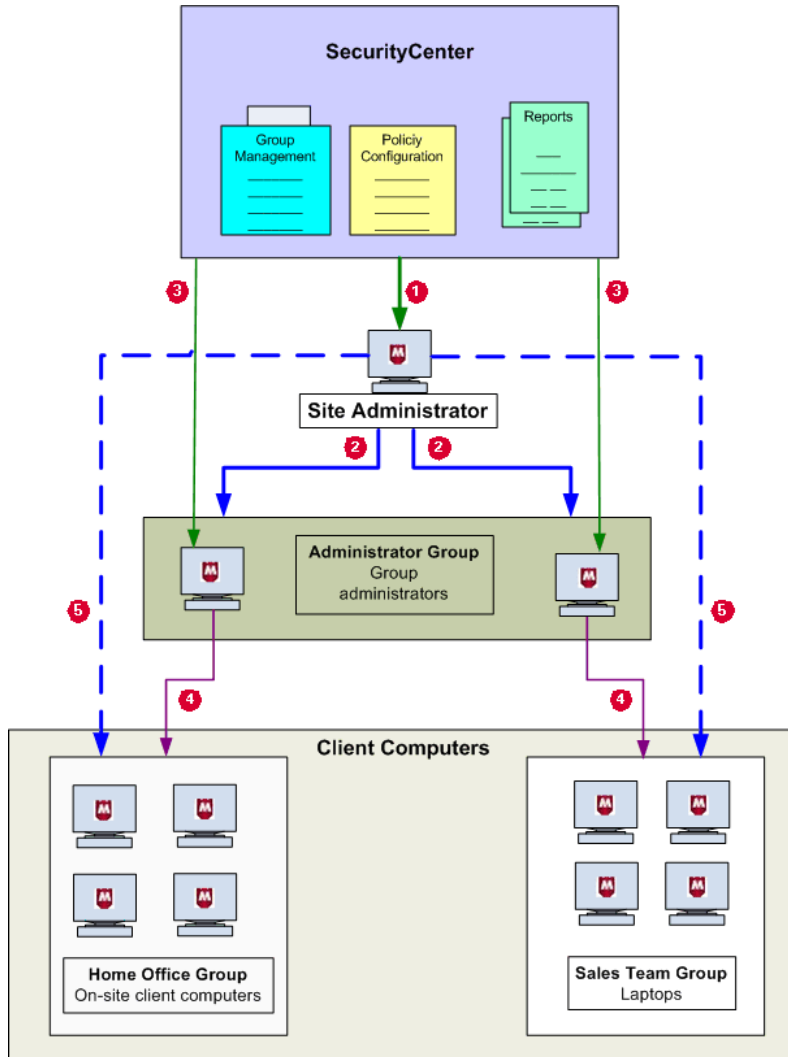
Management of group administrators

Group administrators oversee and manage the groups that you, the site administrator, assign to them. When creating group administrators, you specify which groups they manage, a password they use to access the SecurityCenter, and their access level.

Why use group administrators?

Create group administrators to distribute security management in large organizations.

Group administrators have fewer access rights than the site administrator. While the site administrator can access all security information for all client computers in the account, group administrators can access information only for client computers in the groups they are assigned to.




- 1 The site administrator communicates directly with the SecurityCenter to create policies, check reports, and maintain the SecurityCenter account.
- 2 The site administrator creates and manages group administrators.
- 3 Group administrators communicate directly with the SecurityCenter to access security data for the groups they are assigned to.
- 4 Group administrators manage the client computers in their assigned groups. The management tasks they can perform and the information they can access on the SecurityCenter depend on the access level assigned to them.
- 5 The site administrator can manage all client computers in all groups.

What can group administrators do?

The access level you assign to group administrators determines which tasks they can perform for their groups. Select from two access levels:

- Read Only
- Read and Modify Reports

Basic tasks for Read Only	Additional tasks for Read and Modify Reports
<ul style="list-style-type: none"> • Access the SecurityCenter website. <div style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin: 5px 0;">  No subscription information is visible. Only the assigned groups are visible. </div> <ul style="list-style-type: none"> • Manage from client computers: <ul style="list-style-type: none"> • Manage quarantined files. • Disable on-access scanning. • View the status of a scheduled scan in progress. • View computers from the SecurityCenter. • Check data in reports. 	<ul style="list-style-type: none"> • Install protection. • View and manage computers from the SecurityCenter. • View policies. • Rename groups. • Modify the information in listings and reports: <ul style="list-style-type: none"> • Send email to computers. • Delete computers from your reports. • Move computers in and out of groups. • Send email to users. • Schedule and send reports to users in email.

See also

Management of computer groups on page 48

Working with group administrators

Use this task to manage group administrators on the **My Account** page. Here you can view, edit, create, or delete group administrators.


Up to six group administrators can be listed. If you have created more than six group administrator accounts, click **View all group administrators** to display a complete listing.

Task

- 1 Click the **My Account** tab.
- 2 Click the **Group Administrators** tab, then do any of the following:

To...	Do this...
Add a group administrator	<ol style="list-style-type: none"> 1 In the Group Administrators section, select Add. 2 On the Manage Group Administrators page, select Create New. 3 Type the group administrator’s name, email address, and password. 4 Select an access level. 5 For each group you want the administrator to manage, select the group in the listing on the left, then click Add Group. 6 Click Save.
Modify information for a group administrator	<ol style="list-style-type: none"> 1 Under Actions, select Edit for the group administrator you want to update. 2 On the Add Group Administrators page, modify information, then click Save.

To...	Do this...
Delete a group administrator	Under Actions, select Delete for the group administrator you want to delete, then click OK .
Email a new password to a group administrator	Under Actions, select Email Password . After your local email application opens a preaddressed message explaining how to log on to the SecurityCenter, assign groups, and access information about their responsibilities, send the email.

 You must have a local email application installed to use this feature.

Management of security policies

A policy is a collection of security settings that define how the product features operate. A policy is assigned to each computer when it is added to your account.

Why use policies?

Policies enable you to customize security settings for your entire organization or for different computers in your organization. You can assign a unique policy to each computer, assign a single policy to every computer in a group, or allow all computers to share a single policy.

For example, you might place all laptops used by traveling sales representatives into a single group called Sales Team. For each computer in the group, you can assign a policy with high security settings that will provide greater protection against threats in unsecured networks such as airports and hotels. Whenever you want to adjust those setting, simply change the policy. Your changes will be applied to all the computers in the Sales Team group automatically. There is no need to update each computer's setting individually.

How can I manage policies?

The **Policies** page displays all your policies. Use this page to create, copy, modify, and delete policies for your account. If you have not created any policies, only the McAfee Default policy is displayed.

See also

[Management of computer groups on page 48](#)

[Management of client computers on page 43](#)

McAfee Default policy

Until you create additional policies, all computers are assigned the McAfee Default policy.

The McAfee Default policy is configured with settings recommended by McAfee to protect many environments and ensure that all computers can access important websites and applications until you have a chance to create a customized policy.

You cannot rename or modify the McAfee Default policy. When you add computers to your account, the McAfee Default policy is assigned to them. When you delete a policy that is assigned to one or more groups, the McAfee Default policy is assigned to those groups automatically.

The first time you create a new policy, the McAfee Default policy settings appear as a guideline. This enables you to configure only the settings you want to change without having to configure them all.

After you create one or more new policies, you can select a different default policy for your account. In the future, new policies will be prepopulated with these default settings, and the new default policy is assigned to new computers (if no other policy is selected) and groups whose policy is deleted.



This section explains only the settings for the McAfee Default policy. See the chapters for the protection services for a complete explanation of all related policy options.

Client Settings

Client Settings Tab

Option	Definition
Update Settings	
Check for updates every	12 hours: Client computers check for updated detection definition (DAT) files and product components every 12 hours.
Update client computers where users are not logged in	Disabled: Automatic updates do not occur on computers where no user is logged on (for example, terminal servers and computers where the fast user switching feature is used). This prevents failed automatic updates that would be reported as errors.
Display Settings	
Console display on client computers	Show full console: Allow users to view the McAfee SaaS Endpoint Protection console and access all the client software features.
Hide the splash screen	Disabled: The McAfee SaaS Endpoint Protection splash screen is displayed when a computer is powered on and the client software starts running.
Display support notifications on client computers	Enabled: Notification dialog boxes warn client computer users when software upgrades and DAT file updates are being discontinued for their operating system.


Virus and Spyware Protection

No excluded files and folders or approved programs are configured.



With the default advanced settings for the virus and spyware protection service, it is possible for an on-demand scan to detect threats in archived files that are not detected during an on-access scan. This is because on-access scans do not look at compressed archives by default. If this is a concern for your organization, you should create a new policy where this option is enabled.

General Settings Tab

Option	Definition
Scheduled Scan Settings	Off: No on-demand scan is scheduled. On-access scans still occur every time users run, open, or download files.
Spyware Protection Mode	Prompt: Spyware scanning is enabled. When potentially unwanted programs are detected, the virus and spyware protection service asks users how to respond.
	 To prevent prompts from displaying, create a new policy with a different setting. For maximum protection, we recommend selecting Protect mode to automatically delete potentially unwanted programs.


Advanced Settings Tab

Option	Definition
Virus Protection Settings	
Enable outbreak response	Enabled: Client computers check for an outbreak detection definition (DAT) file every hour.
Enable buffer overflow protection	Enabled: Detect code starting to run from data in reserved memory and prevent that code from running.
Enable script scanning	Enabled: Detect harmful code embedded in web pages that would cause unauthorized programs to run on client computers.
Scan email (before delivering to the Outlook Inbox)	Enabled: Look for threats in email before it is placed into the user's Inbox.
Scan all file types during on-access scans	Enabled: Look for threats in all types of files, instead of only default types, when they are downloaded, opened, or run. (Default file types are defined in the DAT files.)
Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz)	Disabled: Do not look for threats in compressed archive files when the files are accessed.
Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz)	Enabled: Look for threats in compressed archive files when files are scanned manually and during scheduled scans.
Enable Artemis heuristic network check for suspicious files	Enabled: Send information about unrecognized threat detections to McAfee Labs for analysis.
Scan mapped network drives during on-access scans	Disabled: Do not look for threats in files on mapped network drives when they are accessed.
Enable on-access scanning (if disabled) the next time client computers check for an update	Enabled: If on-access scanning is disabled on a client computer, it is re-enabled when the computer checks for updates.
Maximum percentage of CPU time allocated for on-demand and scheduled scans	High: These scans are allowed to use a high percentage of CPU time. (Scans should be requested during non-peak hours, when users are not performing tasks on their computers.)
Spyware Protection Settings	
Detect ...	Enabled: Detect all types of spyware threats during scans.

Firewall Protection

No allowed applications are configured.

General Settings Tab

Option	Definition
Firewall Configuration	<p>User configures firewall: Users must configure the firewall protection service for their computers. When this option is selected, other firewall protection options do not appear on this page.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> It is important to educate users about threats and strategies for avoiding intrusions. To ensure the highest level of security, we recommend that administrators create a new policy and configure the firewall protection service.</p> </div>

Browser Protection

General Settings


Option	Definition
Automatically install browser protection on all computers using this policy	Disabled: Do not check whether the browser protection service is installed on computers checking for updates. (This option is available for all versions of McAfee SaaS Endpoint Protection.)

Browser Protection & Web Filtering

No exceptions or content rules are configured.

Web Filtering options appear only in versions of McAfee SaaS Endpoint Protection that include the web filtering module.

General Settings

Option	Definition
Automatically install browser protection on all computers using this policy	Disabled: Do not check whether the browser protection service is installed on computers checking for updates. (This option is available for all versions of McAfee SaaS Endpoint Protection.)
Access to Sites	Regulate access to websites according to their safety ratings: <ul style="list-style-type: none"> • Yellow: Warn • Red: Block • Unrated: Allow
Access to Downloads	Regulate access to file downloads according to their safety ratings: <ul style="list-style-type: none"> • Yellow: Warn • Red: Block • Unrated: Allow <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  This feature is not supported on Firefox browsers. </div>
Block phishing pages	Enabled: Do not allow access to pages with phishing content, even if they are located on a website with a green overall safety rating.
Enforcement Messaging	Display this message when users attempt to access blocked content: <ul style="list-style-type: none"> • Language: The default language for your account. • Message: The text of the message, An unacceptable security risk is posed by this site.
Browser Protection Status	
Disable browser protection on all computers using this policy	Disabled: Do not disable browser protection on computers using this policy.
Allow users to enable or disable browser protection	Disabled: Do not allow browser protection to be disabled at the client computer.

Working with policies



Use this task to create and modify policies from the **Policies** page. You can also select a new default policy for your account.



Configure policies for SaaS protection services and the email server protection service on portals. To open a portal, click the **Policies** tab, then select the service you want to configure from the drop-down menu.

Task

- 1 Click the **Policies** tab.
- 2 On the Policies page, do any of the following:

To...	Do this...
Specify a default policy	Select an existing policy from the Default Policy list.
Create a policy	<ol style="list-style-type: none"> 1 Click Add Policy. <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin: 5px 0;">  The new policy is prepopulated with settings from the McAfee Default policy or another policy that you have selected as the default for your account. To prepopulate a new policy with settings from a different policy, locate the policy and select Copy. </div> <ol style="list-style-type: none"> 2 Type a name for the policy. 3 Configure the settings on each tab. 4 Click Next. 5 Assign the policy to one or more computers or groups. <i>(Optional)</i> 6 Click Save.
Edit a policy	<ol style="list-style-type: none"> 1 Under Actions, select Edit for the policy. 2 Make changes to the policy, then click Save.
Delete a policy	<p>Under Actions, select Delete for the policy, then click Save.</p> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin: 5px 0;">  If you delete a policy that is assigned to one or more groups, the default policy you have selected for your account (or the McAfee Default policy) is assigned to the groups in its place. You cannot delete the McAfee Default policy. </div>

Generation of security reports

Whenever a client computer checks for updates, it also sends information about itself to the SecurityCenter.

It sends its scanning history, update status, and detections in encrypted XML files. It uploads the data directly through an Internet connection or via a relay server. Report data is saved for one year.

To view this data, click the **Reports** tab to display the Reports page. You can display reports that include all the computers on your account (using the same company key) or only computers in a particular group.

Why use reports?

Reports provide valuable tools for monitoring detections and fine-tuning your protection strategy. Only the reports available for the types of protection installed appear on this page.

Emailing and scheduling reports

You can run reports on demand or schedule them to at run regular intervals and then send them as email attachments to one or more recipients.



For more information about reports for a specific protection service, see the chapters for that service. For versions of McAfee SaaS Endpoint Protection that include SaaS protection services, reports are available on the associated portal.

Use this report...	To view...
Detections	<p>The types of potentially malicious code or unwanted programs that have been found on your network.</p> <p>Use this report to manage detections of viruses and potentially unwanted programs.</p>
Computer Profiles	<p>For each client computer, the version of the Microsoft Windows operating system and Microsoft Internet Explorer web browser running, which group it belongs to, whether it is configured as a relay server, and other details.</p> <p>Use this report to locate computers where you need to install software patches for a specific browser or operating system, check the version of the client software, identify relay servers, and identify the group number for use in silent installation.</p>
Duplicate Computers	<p>Computers that appear more than once in administrative reports.</p> <p>Use this report to track down obsolete computers and those where McAfee SaaS Endpoint Protection has been incorrectly reinstalled and tracked as multiple installations.</p>
Unrecognized Programs	<p>Programs that spyware protection or firewall protection detected on your network.</p> <p>Use this report to manage your potentially unwanted program detections and Internet applications blocked by firewall protection. You can add approved programs and allowed Internet applications to policies directly from the report.</p>
Inbound Events Blocked by Firewall	<p>Computers where inbound or outbound communications were blocked by firewall protection.</p> <p>Use this report to manage blocked communications.</p> <div data-bbox="925 1795 974 1841" data-label="Image"> </div> <p>For blocked events to be reported, the Report blocked events option must be enabled in the Firewall Protection policy. Blocked events are logged for all computers that are assigned a policy where this option is enabled.</p>

Use this report...	To view...
Detection History	<p>A graphical summary of the number of detections and the number of computers where detections occurred on your network over the past year.</p> <p>Use this report to evaluate the effectiveness of your security strategy.</p>
Web Filtering	<p>A summary of browsing activity monitored by the browser protection service. Shows the types of sites that client computers attempted to access by content rating and category. Includes successful, warned, and blocked access attempts. (Available only when web filtering policy options are enabled for versions of McAfee SaaS Endpoint Protection that include the web filtering module.)</p> <p>Use this report to evaluate the types of sites being accessed by which computers and the effectiveness of the content rules defined in policies.</p>
Email Server Protection	<p>Summary information for each email server running email server protection. Shows the version of Exchange Server, the DAT files, and the spam rule, the Exchange server role, detections on the Exchange server, and other details.</p> <p>Use this report to monitor status and detections. Click the IP address of an Exchange server to open the email server protection dashboard on the server, which enables you to view details about detections and manage email server protection.</p>
SaaS Email Protection	<p>Data about email activity and detections for your account, accessed on the SaaS email and web protection portal. (Available only for versions of McAfee SaaS Endpoint Protection that include the SaaS email protection service.)</p> <p>Use these reports to monitor email activity and detections.</p>
SaaS Web Protection	<p>Data about web traffic and content for your account, accessed on the SaaS email and web protection portal. (Available only for versions of McAfee SaaS Endpoint Protection that include the SaaS web protection service.)</p> <p>Use this report to evaluate the types of sites being accessed by which computers and the effectiveness of the content rules defined in policies.</p>

Use this report...	To view...
SaaS Vulnerability Scanning/PCI Certification	Information about potential security risks detected during network security audits and recommendations for eliminating them, accessed on the SaaS vulnerability scanning portal. (Available only for versions of McAfee SaaS Endpoint Protection that include the SaaS vulnerability service and the PCI certification service.) Use this report to check for risks and to ensure that your site adheres to security standards.
Trustmark module	Trustmark code and instructions for posting it on your website. After it is posted, this code displays your certification status to your customers. (Available only with versions of McAfee SaaS Endpoint Protection that include the trustmark module.)

Scheduling reports

Use this task to send information from the SecurityCenter as an email attachment at regular intervals.

This type of information can be scheduled:

- Reports
- Dashboard page
- Computers or Computer Details page
- Widgets on the Dashboard page

The screenshot shows the McAfee SecurityCenter interface. At the top, there is a navigation bar with links: Dashboard, Computers, Reports, Policies, My Account, Utilities, Help, Feedback, and Log Off. Below this is a search bar for 'Reports'. The main content area has two tabs: 'Reports' and 'Scheduled Reports'. Under 'Scheduled Reports', there is a table with the following data:

Subject	Recipients	Sender	Type	Schedule	Action
Duplicate computers on your account	customer789@mcafee.com	democustomer@mcafee.com	Duplicate Computers	Monthly on 1	Edit View Run Report Delete
Unrecognized Programs on your Account	customer456@company.com	democustomer@mcafee.com	Unrecognized Programs	Monday, Friday	Edit View Run Report Delete
Weekly Detections Report	account123@company.com	democustomer@mcafee.com	Detections	Monday	Edit View Run Report Delete

Below the table, there is a note: "To schedule a report, navigate to the report and click the email icon in the top right corner of the screen. Select the information that appears in the scheduled report by using the available filters (such as View, Groups, and Reporting period)."

Task

For option definitions, click ? in the interface.

- 1 Display the page or widget that shows the information you want to send.
- 2 Click the email icon in the upper-right corner.
A blank email message appears.

- 3 Select delivery options.
 - **Immediately** — Send the information once, as soon as you click **Save**.
 - **Weekly on** — Send the information each week, on the selected day.
 - **Monthly on** — Send the information each month, on the selected day.
- 4 Type one or more email addresses to receive the report.
Separate multiple addressees with commas.
- 5 Type a subject and a message for the email.
- 6 Click **Save**.

Adding your logo to reports

Use this task to customize reports by adding or revising a logo.

You can upload a logo that appears in the upper-right corner of the SecurityCenter website and reports.

Logo files can be .gif, .jpeg, .jpg, or .png format. Logo dimensions must be 175 x 65 pixels with a file size under 500 KB. Other dimensions will result in a stretched or shrunken logo.

Task

For option definitions, click ? in the interface.

- 1 On the My Account page, click the **My Profile & Logo** tab.
The My Logo section displays the current logo, or a placeholder if you have not uploaded a logo.
- 2 Click **Edit**.
- 3 On the Manage Logo page, perform a task.

To...	Do this...
Add or replace a logo	<ol style="list-style-type: none"> 1 Click Upload New Logo. 2 On the Upload Your Logo page, type the name of the file you want to upload or browse to locate the file. 3 In the Verification Code box, type the characters displayed in the black box. Alphabetic characters are not case-sensitive. 4 Click Upload Logo. If your logo file is not the correct size, the SecurityCenter resizes it to fit the allotted area and displays a preview of how it will appear on reports. <ul style="list-style-type: none"> • Click Approve to accept the resized logo. • Click Delete and Resubmit to select a different file. 5 Click Close Window.
Delete a logo	Click Delete Logo .

- 4 Click **Done**.

Management of your account

Access tasks for managing your McAfee SaaS Endpoint Protection account on the **My Account** page of the SecurityCenter.

- **My Profile & Logo** tab — Update the contact information for your account and add a customized logo to appear in reports.
- **Subscription & Notification** tab — View details about your current and past subscriptions, buy or renew a subscription, buy more licenses, request a trial subscription, and select the automatic emails you want to receive.
- **Group Administrators** tab — Create and manage administrators for groups in your account.
- **Accounts & Keys** tab — View the company key, enrollment key, and license key for your account or merge another account into your account.

Configuring your account profile

Use this task to update information in your customer profile when it changes.

Your profile contains the information your service provider needs to contact you about your account. Initially, information supplied during your product purchase is placed into your profile. It is important to keep this information up-to-date to prevent a disruption in your protection.

Task

For option definitions, click ? in the interface.

- 1 On the My Account page, click the **My Profile & Logo** tab.
- 2 In the My Profile section, click **Edit**.
- 3 Type or select information as needed.
 - Your password for logging on to the SecurityCenter.
 - Your administrator email address.
 - Contact information.
 - Language for account correspondence and notifications.
- 4 Click **Save**.

Signing up for email notifications

Use this task to select the email notifications you want to receive from your service provider.

Task

For option definitions, click ? in the interface.

- 1 On the My Account page, click the **Subscription & Notification** tab.
- 2 In the Notification Preferences section, click **Edit**.

- 3 Sign up for email notifications for account status and subscription expiration. The type of notifications available depends on your service provider.



Status emails keep you informed about detections and coverage for your account. It is important to receive status emails at regular intervals that are appropriate for your account, based on the frequency with which you need to review detection information. By default, you receive status emails weekly.

- 4 Click **Save**.

Viewing and updating subscription information

Use this task to view current and cancelled subscriptions and to update subscription information.

It is important to check the status of your subscriptions to ensure that protection remains active and you have the right number of licenses to protect new computers as your organization grows.

Task

- 1 On the My Account page, click the **Subscription & Notification** tab.

The Subscription Summary section lists details about each subscription, including the number of licenses and their expiration date.

- 2 Do any of the following.

To...	Do this...
Purchase or extend coverage	In the Subscription Summary section, check the number of licenses available and their expiration dates. If needed, click Buy , Buy More , or Renew .
View details of each subscription	Click View subscription history .
Update information for a subscription	<ol style="list-style-type: none"> 1 Click Edit. 2 On the Edit Subscription Information page, type new information for any of the following: <ul style="list-style-type: none"> • Email address • Company name • First name or Last name 3 Click Submit.
Display a list of subscriptions that are no longer current	Select View cancelled subscriptions .

Buying and renewing subscriptions and licenses

Use this task to buy, add, or renew subscriptions and licenses.

Subscriptions entitle you to one or more protection services, and the number of licenses determine how many computers are protected.



You can configure your notification preferences to receive an email whenever the expiration date for a subscription approaches.

To ensure that additional or renewed services remain on the same account with your existing services, follow these guidelines:

- Submit your order through the same SecurityCenter account you use to maintain your original subscriptions.
- Submit your order with the same email address you use to log on to the SecurityCenter.

By keeping all your subscriptions on the same account, all your client computers report to the same SecurityCenter website, and your service provider sends all correspondence and notifications to one email address.

If you do purchase subscriptions on multiple accounts, you can merge them into a single account.

Task

- 1 On the My Account page, click the **Subscription & Notification** tab.

The Subscription Summary section lists details about each subscription, including the number of licences and their expiration date.

- 2 In the Add Protection column, click **Buy**, **Buy More**, or **Renew**, as needed.



To try a new protection service free-of-charge for 30 days, request a trial subscription by clicking **Try**. Before it expires, you will have an opportunity to purchase the full subscription and continue using it with no interruption.

- 3 Follow the instructions on the Product Purchase page.

Locating or creating keys for your account

Use this task to reference important keys for your account.

- Company key — Required for URL-based or silent installation of client software.
- Account enrollment key — Required to activate pre-installed versions of client software and place them under your account. If no valid enrollment key exists, create a new one.



A license key is required to activate CD-based versions of the client software. Locate the license key on the CD label. See the installation guide or user help for activation instructions.

Task

For option definitions, click ? in the interface.

- 1 On the My Account page, click the **Accounts & Keys** tab.
- 2 Do any of the following.

To...	Do this...
Access your company key	Locate the company key for your account in the Company Key section.
Install protection on new computers	<ol style="list-style-type: none"> 1 Click standard URL installation to open the installation wizard. 2 Click VSETUP to download the silent installation utility. <p>See the installation guide for more information.</p>

To...	Do this...
Access your account enrollment key	Locate the enrollment key for your account in the Account Enrollment Key section
Create a new account enrollment key	Click Create a new key . Account enrollment keys are valid for seven days.

Merging accounts

Use this feature to merge other installations of McAfee SaaS Endpoint Protection into your account.

Merging other installations of McAfee SaaS Endpoint Protection into your account is useful when the client software was installed using another license key or when licenses were purchased using another administrator's email address.

For example, if you set up Account 1, then order additional licenses and activate them with a different email address than the one you originally used, the new licenses appear in Account 2. To view all the computers and licenses under Account 1, you must merge Account 2 into Account 1.

Once they are merged, Account 2 no longer exists. All the computers and licenses formerly listed under Account 2 are listed in the SecurityCenter for Account 1.

Task

For option definitions, click ? in the interface.

- 1 On the My Account page, click the **Accounts & Keys** tab.
- 2 In the Manage Accounts section, select **Merge another account**.
- 3 On the Step 1 page, enter the email address and password activated for the account you want to merge into your main account, then click **Next**.
- 4 On the Step 2 page, view details for the account you have selected. Verify that the licenses and computers listed for the account are the ones you want to merge, then click **Next**.
- 5 On the Step 3 page, click **Merge Account**.

Utilities

Access tools for managing your account on the **Utilities** page of the SecurityCenter.

Utilities are organized by purpose on different tabs.

Installation Tab	
Basic URL installation	Click Run to open the wizard, which guides you through the steps for selecting which software to install on which computers. Select this option from a client computer.
Silent installation	Click Download to get the silent installation package, which enables you to deploy McAfee SaaS Endpoint Protection on a client computer with no user interaction. Select this option from either an administrative or client computer.

Installation Tab	
Push installation	Click Download to run an ActiveX control that enables you to deploy the client software directly from the service provider's server onto multiple client computers. Select this option from an administrative computer.
Installation agent	Click Download to get software that you can install on client computers to allow users without administrative rights to install the client software.
Welcome kit	Select a link to open instructions for activating an account for SaaS protection services and setting up the features you have purchased. (Available only for the SaaS protection services for which you have purchased a subscription.)
Migration & Optimization Tab	
Cleanup utility	Click Run to get a program that removes components left from a previous installation of McAfee SaaS Endpoint Protection or another vendor's protection software. Select this option from a client computer, then double-click to begin installation.
ProtectionPilot Migration Tool	Click Download to get a wizard that guides you through the steps for migrating computers in a McAfee® ProtectionPilot™ account to a McAfee SaaS Endpoint Protection account. A link to documentation is also provided.
Active Directory Configuration Tab	
View synchronization history	Click this link to open a page listing details for up to 25 computers whose information was synchronized most recently with the SecurityCenter.
Active Directory Structure	Click this link to open a page showing the Active Directory tree for your account.
Active Directory Synchronization utility	Click Download to get a tool that imports Active Directory groups into your account, then later imports modifications so the SecurityCenter stays up-to-date.
Push Install utility	Click Download to run a utility that deploys the client software directly from the service provider's server onto multiple client computers in your Active Directory tree. Select this option from an administrative computer that has a network connection to an Active Directory server.
Synchronization Schedule	Select options to configure the Active Directory Synchronization utility to run at regular intervals.

Getting assistance

Use this task to get assistance in using McAfee SaaS Endpoint Protection and the SecurityCenter.

Context-sensitive online help is available on any page of the SecurityCenter by clicking the help link (?) in the upper-right corner.



Guides or online help for these services are available separately. See their chapters for instructions on accessing them.

- SaaS vulnerability scanning
- Email server protection

Task

- Click the **Help** tab, then do any of the following:

To...	Do this...
View online documents	Click a link for the <i>Product Guide</i> , <i>Installation Guide</i> , or <i>Release Notes</i> .
View demos and tutorials	<p>Click the icon for a multimedia presentation.</p> <ul style="list-style-type: none"> • View the McAfee SaaS Endpoint Protection Demo — Describes how the product protects computers on your account. • View the Installation Tutorial — Describes how to install the product. • View the SecurityCenter Demo — Describes how to use the features of the administrative website to manage your account. <p> Your service provider determines which demos are available.</p>
Contact product support	<p>Click an option.</p> <ul style="list-style-type: none"> • Online support — Opens a form where you can submit a description of your problem to a product support representative. • Phone support — Opens a page with a phone number for you to call.
View guides for the SaaS email or web protection service	Click the link to open a page with links to detailed guides. (Available only for SaaS protection services for which you have purchased subscriptions.)

4

Using the Virus and Spyware Protection Service

The virus and spyware protection service checks for viruses, spyware, unwanted programs, and other potential threats by scanning files and programs each time they are accessed on client computers.

It checks removable media, email messages and attachments, and network files. Users can manually request scans for any or all files, folders, and programs on their computers, and administrators can schedule scans to occur at regular intervals.


The virus and spyware protection service functions as a single component within McAfee SaaS Endpoint Protection, but includes policy options that let you configure some of the virus protection and spyware protection features separately. The virus and spyware protection service includes optional features that let you or client computer users select the types of files and programs to scan and the types of threats to detect. You or the users can also specify files to exclude from virus scans and programs that should not be detected as spyware.

Contents

- ▶ *How detections are handled*
- ▶ *Spyware protection mode and detections*
- ▶ *Types of scans*
- ▶ *Scanning on client computers*
- ▶ *Configuring scanning policy options*
- ▶ *Managing detections*
- ▶ *Reports for virus and spyware protection*
- ▶ *Best practices (virus and spyware protection)*

How detections are handled

The type of threat and the policy settings determine how the virus and spyware protection service handles a detection.

Items with detections	How the virus and spyware protection service handles the detections
Files and programs	<p>Virus detections: The virus and spyware protection service attempts to clean the file. If it can be cleaned, the user is not interrupted with an alert. If it cannot be cleaned, an alert appears, and the detected file is deleted. A copy is placed in the quarantine folder. Potentially unwanted program detections: In Protect mode, detections are cleaned or deleted. In Prompt mode, users must select the response.</p> <p>In all cases, a backup copy of the original item is saved in a quarantine folder, in a proprietary binary format. Data for all activity is uploaded to the SecurityCenter for use in reports.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Files are placed into the quarantine folder in a format that is no longer a threat to the client computer. It is not necessary to view or delete them, but you might occasionally want to do so. In these situations, you must view files on the client computer by using the Quarantine Viewer. Only users logged on as an administrator can access the Quarantine Viewer. After 30 days, these files are deleted.</p> </div>
Registry keys and cookies	Detections initially appear as Detected . Cleaning detected files also cleans their associated registry keys and cookies. Their status is then reported as Cleaned .

See also

[Managing detections on page 83](#)

[Managing quarantined files on page 85](#)

Spyware protection mode and detections

Spyware protection monitors programs that attempt to install or run on client computers. When it detects an unrecognized program, it either allows or blocks it. The response is based on the spyware protection mode selected in the policy assigned to the client computer.

In this mode...	Spyware protection does this...
Protect	Checks the list of allowed and blocked programs created by the administrator for computers using the policy. If the program is not on the list, spyware protection blocks the potentially unwanted program.
Prompt	Checks the list of approved and blocked programs created by the administrator for computers using the policy. Checks the list of programs the user has approved. If the program is not on either list, spyware protection displays a prompt with information about the detection and allows the user to select a response. This setting is the default.
Report	Checks the list of approved and blocked programs created by the administrator for computers using the policy. If the program is not on the list, it sends information about the potentially unwanted program to the SecurityCenter and takes no additional action.

For all modes, detections are reported to the SecurityCenter, where you can view information about them in reports.



To prevent popup prompts from appearing on client computers when potentially unwanted programs are detected, and for highest security, we recommend using Protect mode.

How policy options are implemented in the three protection modes

Mode	Behavior of the virus and spyware protection service
Report	<ul style="list-style-type: none"> • Users are not prompted about detections. • Detections are reported to the SecurityCenter. • Administrator can select approved programs, which are not reported as detections. • Can be used as a "learn" mode to discover which programs to approve and block.
Prompt	<ul style="list-style-type: none"> • Users are prompted about detections. • Detections are reported to the SecurityCenter. • Administrator can select approved programs. These programs are not reported as detections, and users are not prompted for a response to them. • Users can approve additional programs in response to prompts. These are reported to the SecurityCenter.
Protect	<ul style="list-style-type: none"> • Users are not prompted about detections. • Users are notified about deleted or quarantined programs. • Detections are reported to the SecurityCenter. • Administrator can select approved programs, which are not reported as detections.

See also

[Selecting spyware scanning options on page 82](#)

Use learn mode to discover programs

Report mode can be used as a "learn mode" to help you determine which programs to approve.

In Report mode, spyware protection tracks but does not block potentially unwanted programs. You can review detected programs in the Unrecognized Programs report and approve those that are appropriate for your policy. When you no longer see unapproved programs you want to approve in the report, change the policy setting for spyware protection mode to Prompt or Protect.

Types of scans

The virus and spyware protection service scans files automatically for viruses and spyware.

At any time, users can perform manual scans of files, folders, or email, and administrators can set up scheduled scans. Policy options let you configure whether optional email and spyware scans occur.

The basic types of scans are:

- Automatic (on-access) scans
- Manual on-demand scans
- Scheduled on-demand scans
- Email scans
- Spyware scans

The behavior of the scanning features on client computers is defined in the policies configured in the SecurityCenter. Policy settings determine the types of files, programs, and other items detected; whether users can manage their detections; how frequently computers check for updates; and when scheduled scans occur.

On-access (automatic) scans

On-access scans are those that occur on client computers whenever users access files (for example, open a file or run a program).

The virus and spyware protection service policy options let you configure these on-access scanning features:

- The types of files scanned and whether files on network drives are scanned.
- Whether email and attachments are scanned.
- Whether files in archives (compressed files, such as .zip files) are scanned.
- Whether files are scanned for spyware.
- The types of virus and spyware threats to detect.
- Whether unrecognized detections are sent to McAfee Labs for investigation.
- Whether to enable on-access scanning (if it is disabled) whenever computers check for updates.
- Files and folders excluded from scans.
- Approved programs that should not be detected as threats.

The default settings for on-access scanning are:

- Scan all types of local files when opened, and again when closed (if they were modified). Do not scan files on network drives.
- Scan all email attachments when accessed and when saved to the hard drive, protecting the computer from email infections.
- Do not scan files in archives.
- Scan programs for spyware identifiers, to detect if a spyware program attempts to run or a program attempts to install spyware.
- Scan for all types of virus and spyware threats.
- Send unrecognized detections to McAfee Labs.
- Enable on-access scanning when computers check for updates.

See also

[Configuring scanning policy options on page 80](#)

[Enabling and disabling on-access scanning on page 79](#)

On-demand scans

On-demand scans are those that occur whenever administrators or users request them. Users can request on-demand scans to occur immediately, and administrators can schedule them to occur at regular intervals.

On-demand scans use many of the same policy options as on-access scans. In addition, the virus and spyware protection policy options let you configure these on-demand scanning features:

- Whether files in archives (compressed files, such as .zip files) are scanned.
- A schedule for performing an on-demand scan at regular intervals.

The default settings for on-demand scans are:

- Scan all local files, including those in archives.
- Scan all critical registry keys.
- Scan all processes running in memory.
- Do not perform a scheduled scan.

In addition, during an on-demand scan of the My Computer folder, the drive where Windows is installed, or the Windows folder:

- Scan all cookies.
- Scan all registry keys.



At the start of an on-demand scan, all previous detections of potentially unwanted programs are cleared from the Potentially Unwanted Program Viewer.

Scheduled scans

Schedule an on-demand scan to occur at a specific date and time, either once or on a recurring basis. For example, you might want to scan client computers at 11:00 P.M. each Saturday, when it is unlikely to interfere with other processes running on client computers.

Configure scheduled scans by selecting policy options for the virus and spyware protection service. Scheduled scans run on all computers using the policy.

See also

[Scanning on demand from the console on page 77](#)

[Scanning on demand from Windows Explorer on page 78](#)

[Scheduling a scan on page 80](#)

[Viewing scheduled scans on page 78](#)

Email scans

Email scans occur during on-access and on-demand scans.

Policy options let you configure whether email is scanned before it reaches a users' Inbox. The default settings for email scanning are:

- Scan all email attachments when accessed and when saved to the hard drive, protecting the computer from email infections.
- Scan email before placing it in a user's Inbox.

Users can also scan email on demand at the client computer.

See also

[Scanning email on client computers on page 78](#)

[Configuring scanning policy options on page 80](#)

Spyware scans

Spyware scanning is a feature within the virus and spyware protection service that looks for and identifies spyware indicators.

Spyware scanning occurs:

- Whenever programs are installed or run, as part of on-access scans.
- During on-demand scans.

Policy options let you configure these spyware scanning features:

- Whether files are scanned for spyware.
- The types of spyware threats to detect.
- Approved programs that should not be detected as threats.

The default spyware-related settings are:

- Look for spyware identifiers during on-access and on-demand scans, to detect if a spyware program attempts to run or a program attempts to install spyware.
- Scan for all types of spyware threats.

The response to detections depends on the spyware protection mode configured in the client computer's policy. Three responses are possible:

- Attempt to clean the program (Protect mode).
- Prompt the user for a response (Prompt mode). This is the default setting.
- Report the detection and take no further action (Report mode).

Cookies and registry keys that indicate spyware are also detected. Deleting a potentially unwanted program deletes any associated cookies and registry keys.

All detections are listed in administrative reports available from the SecurityCenter. On client computers, users can view and manage detections by using the Potentially Unwanted Programs Viewer.



At the start of an on-demand scan, all previous detections of potentially unwanted programs are cleared from the Potentially Unwanted Programs Viewer. For on-access scans, previous detections remain in the Potentially Unwanted Programs Viewer.

See also

[Configuring scanning policy options on page 80](#)

[Managing potentially unwanted program detections on page 84](#)

Scanning on client computers

Use these tasks from a client computer to scan for threats on the computer and to temporarily disable the scanning feature for testing.

Tasks

- [Scanning on demand from the console on page 77](#)
Use this task to perform a manual scan from the console on a client computer.
- [Scanning on demand from Windows Explorer on page 78](#)
Use this task to perform a manual scan from Microsoft Windows Explorer on a client computer.
- [Scanning email on client computers on page 78](#)
Use this task to scan an email message manually on a client computer.
- [Viewing scheduled scans on page 78](#)
Use this task to view a scheduled scan that is in progress on a client computer. You must be logged on as a site administrator to access this task.
- [Enabling and disabling on-access scanning on page 79](#)
Use this task at the client computer to disable the on-access scanner temporarily, which is useful when working with product support to troubleshoot issues with scanning and cleaning files. Use the same task to re-enable on-access scanning.

Scanning on demand from the console

Use this task to perform a manual scan from the console on a client computer.

Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the Action Menu, select **Scan Computer**.
- 3 Select the scan target.
 - **Scan my entire computer** — Scan all drives, folders, and files.
 - **Scan a specific drive or folder** — Type the full path and name of the scan target or browse to locate it.
- 4 Click **Start Scan**.

The virus and spyware protection service displays the progress of the scan.
- 5 If needed, click **Pause Scan** to temporarily interrupt the scan or **Cancel Scan** to end the scan. (*Optional*)
- 6 Click **View detailed report** to open a browser window and display the results of the scan.

See also

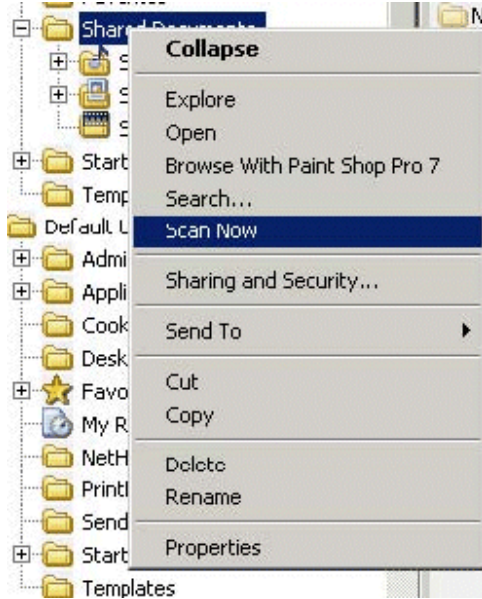
- [Scanning on demand from Windows Explorer on page 78](#)
- [On-demand scans on page 74](#)

Scanning on demand from Windows Explorer

Use this task to perform a manual scan from Microsoft Windows Explorer on a client computer.

Task

- 1 In Windows Explorer, right-click any drive or folder, then select **Scan Now**.



- 2 Close the Scan Completed panel or click **View detailed report** to display the Scan Statistics report.

See also

[Scanning on demand from the console on page 77](#)

[On-demand scans on page 74](#)

Scanning email on client computers

Use this task to scan an email message manually on a client computer.

Task

- 1 In the Microsoft Outlook Inbox, highlight one or more messages in the right pane.
- 2 Under Tools, select **Scan for Threats**.

The On-Demand Email Scan window displays any detections. If the window is empty, no threats were detected.

See also

[Email scans on page 75](#)

Viewing scheduled scans

Use this task to view a scheduled scan that is in progress on a client computer. You must be logged on as a site administrator to access this task.

Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the Action Menu, select **Product Details**.

- 3 In the Virus and Spyware Protection section, select **View Scheduled Scan** to display the progress of the scan.



This option is available only when a scheduled scan is in progress.

- 4 If needed, click **Pause Scan** to temporarily interrupt the scan or **Cancel Scan** to end the scan. (*Optional*)
- 5 Click **View detailed report** to open a browser window and display the results of the scan.

See also

[Logging on as a site administrator on page 34](#)

[Scheduling a scan on page 80](#)

[On-demand scans on page 74](#)

Enabling and disabling on-access scanning

Use this task at the client computer to disable the on-access scanner temporarily, which is useful when working with product support to troubleshoot issues with scanning and cleaning files. Use the same task to re-enable on-access scanning.

The next time the computer checks for updates, on-access scanning is re-enabled (unless the site administrator has changed the policy settings).



This task disables only on-access scanning. Buffer overflow protection continues to function. To disable buffer overflow protection, you must update the policy.

Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the Action Menu, select **Product Details**.
- 3 Under Virus and Spyware Protection, for On-access scanning, select the **Disable** option.



If you disable on-access scanning, files are no longer checked for threats when they are accessed. We recommend that you re-enable this feature as soon as possible.

- 4 Under Virus and Spyware Protection, for On-access scanning, select the **Enable** option to re-enable the feature.

See also

[Logging on as a site administrator on page 34](#)

[On-access \(automatic\) scans on page 74](#)

Configuring scanning policy options

Use these SecurityCenter tasks to configure policy options for virus and spyware scans performed on client computers.

Tasks

- [Scheduling a scan on page 80](#)
Use this SecurityCenter task to schedule an on-demand scan.
- [Enabling optional types of virus scans on page 80](#)
Use this SecurityCenter task to specify optional scans and features for virus protection. If none of these features is selected, virus protection still detects viruses.
- [Excluding files and folders from virus scans on page 82](#)
Use this SecurityCenter task to define and manage items that are not scanned for viruses. You can add files, folders, or file extensions to the list of exclusions or remove them from the list.
- [Selecting spyware scanning options on page 82](#)
Use this task to configure policy options for spyware scanning features.
- [Approving and unapproving programs in a policy on page 82](#)
Use this SecurityCenter task to add approved programs to a policy or remove approved programs from a policy. Approved programs are not detected as potentially unwanted programs.

See also

[On-access \(automatic\) scans on page 74](#)

[Email scans on page 75](#)

[Spyware scans on page 76](#)

[On-demand scans on page 74](#)

Scheduling a scan

Use this SecurityCenter task to schedule an on-demand scan.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Virus & Spyware Protection**, then click the **General Settings** tab.
- 3 Under Scheduled Scan Settings, select **On**.
- 4 Select a frequency, day, and time for the scan to run, then click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

[Viewing scheduled scans on page 78](#)

[On-demand scans on page 74](#)



Enabling optional types of virus scans

Use this SecurityCenter task to specify optional scans and features for virus protection. If none of these features is selected, virus protection still detects viruses.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Virus & Spyware Protection**, then click the **Advanced Settings** tab.
- 3 Under Virus Protection Settings, select each scan you want to enable.

Select this option...	To do this...
Enable outbreak response	Check for an outbreak detection definition (DAT) file every hour.
Enable buffer overflow protection	<p>Detect code starting to run from data in reserved memory and prevent that code from running. The virus and spyware protection service protects against buffer overflow in more than 30 most commonly used Windows-based programs. McAfee updates this list as it adds buffer overflow protection for additional programs.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Buffer overflow protection does not stop data from being written. Do not rely on the exploited application remaining stable after being compromised, even if buffer overflow protection stops the corrupted code from running. </div>
Enable script scanning	<p>Detect harmful code embedded in web pages that would cause unauthorized programs to run on client computers.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Script scanning is always enabled for on-access and on-demand scans. </div>
Scan email (before delivering to the Outlook Inbox)	Look for threats in email before it is placed into the user's Inbox. (Email is always scanned when it is accessed.)
Scan all file types during on-access scans	Inspect all types of files, instead of only default types, when they are downloaded, opened, or run. (Default file types are defined in the DAT files.)
Scan within archives during on-access scans (e.g., .zip, .rar, .tat, .tgz)	Look for threats in compressed archive files when the files are accessed.
Scan within archives during on-demand scans (e.g., .zip, .rar, .tat, .tgz)	Look for threats in compressed archive files during manual or scheduled scans.
Enable Artemis heuristic network check for suspicious files	Send unrecognized threats to McAfee Labs for investigation. (This occurs in the background with no user notification.)
Scan mapped network drives during on-access scans	Look for threats in files located on mapped network drives when the files are accessed.
Enable on-access scanning (if disabled) the next time client computers check for an update	If on-access scanning has been disabled on a client computer, re-enable it the next time that computer checks for updates.
Maximum percentage of CPU time allocated for on-demand and scheduled scans	Use up to the selected percentage of CPU resources when performing on-demand scans. When set to High, we recommend scheduling scans to occur during off-peak hours.

- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

[On-access \(automatic\) scans on page 74](#)

Excluding files and folders from virus scans

Use this SecurityCenter task to define and manage items that are not scanned for viruses. You can add files, folders, or file extensions to the list of exclusions or remove them from the list.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Virus & Spyware Protection**, then click the **Excluded Files and Folders** tab.
- 3 Select the type of exclusion you want to create.
- 4 Specify the value (browse for a file or folder, or type a file extension).
- 5 Click **Add Exclusion**. The new exclusion appears in a list.
- 6 To remove an entry from the list of exclusions, click **Block**.
- 7 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Selecting spyware scanning options

Use this task to configure policy options for spyware scanning features.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Virus & Spyware Protection**, then click the **General Settings** tab.
- 3 For Spyware Protection Status, select a protection mode to enable spyware protection, or select **Off** to disable spyware protection.
- 4 Click the **Advanced Settings** tab.
- 5 Under Spyware Protection Settings, select each type of program you want to detect.
- 6 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

[Spyware protection mode and detections on page 72](#)

Approving and unapproving programs in a policy

Use this SecurityCenter task to add approved programs to a policy or remove approved programs from a policy. Approved programs are not detected as potentially unwanted programs.



You can also use the Unrecognized Programs report to view a complete listing of all programs detected on client computers and add them to policies.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Click **Virus & Spyware Protection**, then click the **Approved Programs** tab.
- 3 Locate the program you want to approve in the listing of all programs detected on client computers, then select an option.

Select this...	To do this...
Approve	Approve the selected program.
Approve All	Approve all the programs listed.
Block	Block the selected program.
Block All	Block all the programs listed.

- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

[Viewing user-approved programs and applications on page 86](#)

[Viewing unrecognized programs detected on the account on page 87](#)

Managing detections

Use these tasks to view and manage threats detected during virus and spyware scans.

- For an individual client computer, perform tasks at the computer (users and administrators).
- For multiple computers, groups, or an entire account, access administrative reports from the SecurityCenter.

Tasks

- [Viewing scan results on client computers on page 84](#)
Users and administrators can use this task from a client computer to view the Scan Statistics report on a client computer after completing an on-demand scan.
- [Managing potentially unwanted program detections on page 84](#)
The Potentially Unwanted Programs Viewer lists all items detected by spyware protection, which might include program files, registry keys, and cookies.
- [Managing quarantined files on page 85](#)
When the virus and spyware protection service detects a threat, it places a copy of the item containing the threat in a quarantine folder before cleaning or deleting the original item.
- [Viewing user-approved programs and applications on page 86](#)
Use this SecurityCenter task to see which applications users have approved to run on their computers.
- [Viewing threats detected on the account on page 87](#)
Use this SecurityCenter task to view the Detections report.
- [Viewing unrecognized programs detected on the account on page 87](#)
Use this SecurityCenter task to view the Unrecognized Programs report, which lists potentially unwanted programs detected on all the client computers on your account.
- [Viewing historical information about detections on page 88](#)
Use this SecurityCenter task to view the Detection History report.

See also

[How detections are handled on page 72](#)

Viewing scan results on client computers

Users and administrators can use this task from a client computer to view the Scan Statistics report on a client computer after completing an on-demand scan.



Client computers also send information about threats detected during scans to the SecurityCenter in encrypted XML files. Administrators can access three reports containing information about detected virus and spyware threats and potentially unwanted programs from the Reports page on the SecurityCenter.

Task

- Select **View detailed report** in the Scan Completed panel. A browser window opens and displays the Scan Statistics report, which includes this information:
 - Date and time the scan was started.
 - Elapsed time for the scan.
 - Version of the scanning engine software and DAT file.
 - Date of the last update.
 - Completion status of the scan.
 - Location of the scanned items.
 - Status for scanned files, registry keys, and cookies.

Status	What it means...
Scanned	Number of items scanned.
Detected	The item is still a threat and still resides on the system. For files, they are most likely contained within a compressed archive (for example, a .ZIP archive) or on write-protected media. For registry keys and cookies, the file they are associated with has a status of Detected.
Cleaned	The item was cleaned of the threat. A backup copy of the original item was saved in a quarantine folder, in a proprietary binary format, where it can be accessed only with the Quarantine Viewer.
Deleted	The item could not be cleaned; it was deleted instead. A copy was saved in a quarantine folder, in a proprietary binary format, where it can be accessed only with the Quarantine Viewer.

See also

[How detections are handled on page 72](#)

Managing potentially unwanted program detections

The Potentially Unwanted Programs Viewer lists all items detected by spyware protection, which might include program files, registry keys, and cookies.

Users and administrators can use this task from a client computer to view and manage detections of potentially unwanted programs in the Potentially Unwanted Programs Viewer.

Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 In the Virus and Spyware Protection section, select **View Potentially Unwanted Programs**.
- 3 From the list of detections, select one or more items, then click an action.
 - **Clean** — Place an original copy of each selected item in a quarantine folder, in a proprietary binary format, then attempt to clean it. If it cannot be cleaned, delete the item.
 - **Approve** — Add selected items to the list of approved programs so they will not be detected as spyware.



Clicking **Approved** displays a list of all currently approved programs on the computer.

- 4 Check the status of each item.
 - **Action Required** — You have not performed any action on this item since it was detected.
 - **Approved** — The item was added to the list of user-approved programs and will no longer be detected as spyware.
 - **Cleaned** — The item was cleaned successfully and can be used safely. A backup copy of the original item was placed in a quarantine folder, in a proprietary binary format.
 - **Quarantined** — The item could not be cleaned. The original item was deleted and a copy was placed in a quarantine folder, in a proprietary binary format. If the item was a program, all associated cookies and registry keys were also deleted.



Items are placed into the quarantine folder in a format that is no longer a threat to the computer. These items are deleted after 30 days. Users with administrator rights can manage these items using the Quarantine Viewer.

- 5 Click **Back** to return to the console.

See also

[Spyware scans on page 76](#)

Managing quarantined files

When the virus and spyware protection service detects a threat, it places a copy of the item containing the threat in a quarantine folder before cleaning or deleting the original item.

The copy is stored in a proprietary binary format and cannot harm the computer. By default, items in the quarantine folder are deleted after 30 days.


Use this task from a client computer to view and manage quarantined items in the Quarantine Viewer. You must be logged on as a site administrator to access this task.


Task

- 1 Click the product icon in the system tray, then select **Open Console**.
- 2 From the Action Menu, select **Product Details**.
- 3 In the Virus and Spyware Protection section, select **View Quarantined Files**.

The Quarantine Viewer lists all the items in the quarantine folder and their status.

- 4 Select one or more items, then click an action.
 - **Rescan** — Scan each selected item again. This option is useful when new detection definition (DAT) files include a method of cleaning a detection that could not be cleaned previously. In this case, rescanning the file cleans it and allows you to restore it for normal use.
 - **Restore** — Place each selected item back in its original location on the computer. The restored item will overwrite any other items with the same name in that location.

 Virus and spyware protection detected this item because it considers the item to be a threat. Do not restore the item unless you are sure it is safe.
 - **Delete** — Remove each selected item from the quarantine folder, along with all associated registry keys and cookies. No copy will remain on the computer.
- 5 Check the status of each item:
 - **Cleaned** — The item was cleaned successfully and can be used safely. A backup copy of the original item was placed in a quarantine folder, in a proprietary binary format.
 - **Clean failed** — The item cannot be cleaned.
 - **Delete failed** — The item cannot be cleaned or deleted. If it is in use, close it and attempt the clean again. If it resides on read-only media, such as CD, no further action is required. The virus and spyware protection service has prevented the original item from accessing the computer, but it cannot delete the item. Any items copied to the computer have been cleaned.

 If you are not sure why the item could not be cleaned, a risk might still exist.
 - **Quarantined** — You have not performed any action on this item since it was placed in the quarantine folder.
- 6 Select **Get more information on the threats detected** to open a browser window and visit the McAfee Labs Threat Library.
- 7 Click **Back** to close the Quarantine Viewer and return to the console.

Viewing user-approved programs and applications

Use this SecurityCenter task to see which applications users have approved to run on their computers.

You can also add the applications to one or more policies so they will not be detected as unrecognized programs on computers using the policies.

Task

For option definitions, click ? in the interface.

- 1 From the SecurityCenter, do any of the following:
 - Click the **Computers** tab, then click a number in the User-Approved Applications column to view applications for the associated computer.
 - Click the **Computers** tab, then click the name of a computer. In the Computer Details page, under Detections, click a number in the User-Approved Applications column to view applications.
- 2 To add the application to one or more policies, in the User-Approved Applications list, under Actions click **Allow**.
- 3 In the Add Approved Application page, select each policy where you want to add the application, then click **Save**.

See also

[Approving and unapproving programs in a policy](#) on page 82

[Configuring options for Internet applications](#) on page 100

Viewing threats detected on the account

Use this SecurityCenter task to view the Detections report.

The Detections report lists these types of threats detected on all the client computers on your account:

- virus and malware threats
- potentially unwanted programs
- buffer overflow processes
- cookies

Task

For option definitions, click ? in the interface.

- 1 Click the **Reports** tab, then click **Detections**.
- 2 In the Detections report, view detailed information about detections and the computers where detections occurred by using one of these methods.

When you want to...	Do this...
Display computers or detections	<p>Click the triangle icon next to a name.</p> <ul style="list-style-type: none"> • Under a computer name, show which detections were found. • Under a detection name, show the computers where it was found. <p>Click a group name to display computers in that group.</p>
View details about detections	<p>If detections are listed for a computer, click a quantity to display details.</p> <ul style="list-style-type: none"> • Click a quantity for Detected Objects to display a list of detected threats and their status. • From the Detections List, click the name of a detection to display detailed information from the McAfee Labs Threat Library.
View details about a computer where a detection occurred	<p>Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.</p>

See also

[Viewing historical information about detections](#) on page 88

Viewing unrecognized programs detected on the account

Use this SecurityCenter task to view the Unrecognized Programs report, which lists potentially unwanted programs detected on all the client computers on your account.

Task

For option definitions, click ? in the interface.

- 1 Click the **Reports** tab, then click **Unrecognized Programs**.
- 2 In the Unrecognized Programs report, view detailed information about unrecognized programs and the computers where they were detected by using one of these methods.

When you want to...	Do this...
Display computers or detections	<p>Click the triangle icon next to a name.</p> <ul style="list-style-type: none"> • Under a computer name, show which programs were detected. • Under a program name, show the computers where it was detected. <p>Click a group name to display computers in that group.</p>
View details about detections	Click the name of a potentially unwanted program to display detailed information from the McAfee Labs Threat Library.
View details about a computer where a detection occurred	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.
Approve a program	Click Allow , select one or more programs, select one or more policies where the programs will be approved, then click Save . The selected programs will no longer be detected as threats on computers using the selected policies.

See also

[Approving and unapproving programs in a policy on page 82](#)

[Configuring options for Internet applications on page 100](#)

Viewing historical information about detections

Use this SecurityCenter task to view the Detection History report.

The Detection History report shows summary information for the detections on your account over the past year. Data can be displayed by month or by quarter.

This information can help you determine how successfully your protection features have performed, and whether strategies you have implemented, such as user education or policy adjustments, have been effective.

Task

For option definitions, click ? in the interface.

- 1 Click the **Reports** tab, then click **Detections**.
- 2 In the Detection History report, view a chart of summary information about threats detected over the past year by selecting the appropriate options.

When you want to...	Do this...
Display information for the last year in monthly increments.	In the Display by list, select Monthly .
Display information for the last year in quarterly increments.	In the Display by list, select Quarterly .

When you want to...	Do this...
Display detections for all the computers on your account.	In the Groups list, select All .
Display detections for a single group.	In the Groups list, select the group for which you want to display data.

See also

[Viewing threats detected on the account on page 87](#)

Reports for virus and spyware protection

View information about virus and spyware detections in administrative reports available from the Reports page of the SecurityCenter. Reports provide details about the specific threats detected and the history of detections over the past year.

- Detections report — Lists the malware threats, potentially unwanted programs, buffer overflow processes, and cookies that the virus and spyware protection service detected on client computers.
- Unrecognized Programs report — Lists programs detected on client computers that are not recognized by spyware protection and firewall protection. Allows you to approve programs from within the report.
- Detection History report — Graphs detections on client computers over the past year.

See also

[Viewing threats detected on the account on page 87](#)

[Viewing user-approved programs and applications on page 86](#)


[Viewing unrecognized programs detected on the account on page 87](#)

[Viewing historical information about detections on page 88](#)

Best practices (virus and spyware protection)

To develop an effective strategy for guarding against virus and spyware threats, we recommend that you proactively track the types of threats being detected on your network and where they are occurring.

- 1 Check your status emails or the SecurityCenter website for an overview of your account's status.
 - Ensure that computers in your account are up-to-date.
 - Ensure that protection is installed on all computers.
- 2 Check the Detections report regularly to see what is being detected.
- 3 Check the Unrecognized Programs report frequently to monitor the programs that users are approving on client computers. If you know some of the programs are safe and do not want them to be detected as potentially unwanted, add them to policies as approved programs.
- 4 To centralize management and more easily monitor the types of programs allowed on client computers, define client security settings in a policy.

- 5 If particular types of detections are occurring frequently or certain computers appear vulnerable, update the policy to resolve these issues.
 - Schedule scans or add exclusions.
 - Enable advanced scanning options.
 - Ensure that spyware protection is enabled.
 - For maximum protection, set your spyware protection mode to Protect to automatically clean potentially unwanted programs.
-  Protect mode is not the default setting. For maximum protection, create a policy that includes Protect mode.
- Enable all advanced spyware options.
 - 6 Use “learn” mode to identify which programs to add to the Approved Programs list. This ensures that no required programs are deleted before you have the opportunity to authorize their use. Then change your spyware protection mode to Protect.
 - 7 View the Detection History report periodically to discover trends specific to your network, and verify your strategy’s success in reducing detections.

5

Using the Firewall Protection Service

The firewall protection service checks for suspicious activity in communications sent between client computers and network resources or the Internet.

As the administrator, you can define what constitutes suspicious activity and how the firewall protection service responds to:

- IP addresses and communication ports that attempt to communicate with your computer. You can specify whether to allow or block communications from other IP addresses on your network or outside your network, or you can identify specific IP addresses and ports to allow or block.
- Applications that attempt to access the Internet. You can use McAfee's recommendations for safe Internet applications, or you can identify specific applications to allow or block. You can also select the firewall protection service's response to detections of unrecognized applications.

The firewall protection service has two primary modes: users configure firewall settings and an administrator configures firewall settings. The McAfee default policy is configured to let client computer users decide which communications and applications the firewall protection service allows. The administrator setting puts all or partial control with the administrator.



To ensure the highest level of protection for your network, we recommend that an administrator configure settings for the firewall protection service in one or more policies, which are then assigned to client computers. When an administrator configures the settings, it is important that the applications and communications that are important to your users are allowed before deploying the policy. This ensures that no important communications are blocked.

Contents

- ▶ *Connection type and detections of incoming communications*
- ▶ *Firewall protection mode and detections of unknown applications*
- ▶ *The role of IP addresses*
- ▶ *The role of system service ports*
- ▶ *Configuration of the firewall protection service*
- ▶ *Configuring policy options*
- ▶ *Configuring custom connections*
- ▶ *Installing and enabling firewall protection at the policy level*
- ▶ *Managing detections*
- ▶ *Reports for the firewall protection service*
- ▶ *Best practices (firewall protection)*

Connection type and detections of incoming communications



The firewall protection service monitors communications coming into the network (known as *inbound events*) to determine whether they meet criteria specified for safe communications. If an event does not meet the criteria, it is blocked from reaching computers on the network.

Specify criteria by selecting the type of connection client computers are using. A policy option setting determines whether the administrator or the user selects the connection type.

Types of connections

The connection type defines the environment where client computers are used. It determines what the firewall protection service considers to be suspicious activity and, therefore, which IP addresses and ports are allowed to communicate with the network computers.

Select from three connection environments.

Select this...	When the computer...	Then the firewall protection service...
Untrusted network	Is connected directly to the Internet. For example: through a dial-up connection, a DSL line, or a cable modem; through any type of connection in a coffee shop, hotel, or airport.	Blocks communications with all other computers, including those on the same subnet.  This is the default setting for client operating systems.
Trusted network	Is connected indirectly to a network that is separated from the Internet by a hardware router or firewall. For example: in a home or office network.	Allows communications with other computers on the same subnet, but blocks all other network communications.  This is the default setting for server operating systems.
Custom	Should communicate only through specific ports or with a specific range of IP addresses, or the computer is a server providing system services.	Allows communications with the ports and IP addresses you specify, blocks all other communications. When you select this option, an Edit button becomes available that enables you to configure options.

Additional information about connection types

It is important to update the connection type whenever the working environment changes. For example, mobile users who connect to both secured (trusted) and unsecured (untrusted) networks must be able to change their setting accordingly.

A policy option specifies whether the firewall protection service tracks blocked events for reporting purposes. When the option is enabled, you can see a listing of all blocked events in the report entitled *Inbound Events Blocked by Firewall*.

The connection type does not affect the way that the firewall protection service handles detections of Internet applications running on client computers.

See also

[Selecting general firewall settings on page 99](#)

[Configuring custom connections on page 101](#)

Custom connections

Trusted and untrusted connection types let you specify whether to allow or block communications originating within a network.

Configure a custom connection type when you want to be more specific about where communications originate. When you set up a custom connection, you can designate:

- Open and blocked ports, through which a computer can and cannot receive communications. This is required to set up a computer as a server that provides system services. The server will accept communications through any open port from any computer. Conversely, it will not accept communications through any blocked port.
- IP addresses from which a computer can receive communications. This allows you to limit communications to specific IP addresses.

Configure settings for custom connections on the **General** tab of the Firewall Protection policy page.

Connection Type

Untrusted network (directly connected to the Internet through a dial-up, DSL, or cable modem; or connected at a public coffee shop, hotel, or airport)

Trusted network (indirectly connected to the Internet through a router or hardware firewall in a home or office network)

Custom settings [[edit](#)]

OK Cancel

Firewall Custom Settings

Allowed Incoming Connections

In Custom mode, the firewall allows connections from the system services checked below.

Allow	Connection Name	Action
✓	File and Print Sharing	
✓	Remote Assistance	
✓	Remote Desktop	

[Add Connection](#)

Allowed Incoming Addresses

In addition to the above services, the computers selected below can connect with client computers.

Any computer
 My network (the subnet only)
 Specific address range:

to [Allow](#)

OK Cancel

Once configured, custom connection settings are saved until you reconfigure them. If you temporarily select a Trusted network or Untrusted network connection type, the custom settings will still be there the next time you want to configure a custom connection.



Custom settings configured on the SecurityCenter are ignored on client computers if firewall protection mode is set to Prompt. In Prompt mode, settings configured by users override administrator settings.

See also

[Configuring custom connections on page 101](#)

Firewall protection mode and detections of unknown applications

The firewall protection mode determines whether the firewall protection service allows unrecognized applications to access the Internet.

The firewall protection service monitors communications with Internet applications, which connect to the Internet and communicate with client computers. When it detects an Internet application running on a computer, it either allows the application to connect to the Internet or blocks the connection, depending on the firewall protection mode selected in the policy assigned to the client computer.

In this mode...	The firewall protection service does this...
Protect	Blocks the suspicious activity.
Prompt	Displays a dialog box with information about the detection, and allows the user to select a response. This setting is the default.
Report	Sends information about suspicious activity to the SecurityCenter and takes no additional action.

For all modes, detections are reported to the SecurityCenter, where you can view information about them in reports.



To prevent popup prompts from appearing on client computers when applications are detected, and for highest security, we recommend using Protect mode.

How policy options are implemented in the three protection modes

Use the following table to determine how policy options are implemented in the different protection modes.

Mode	Behavior of the firewall protection service
Report	<ul style="list-style-type: none"> • Users are not prompted about detections. • Detections are reported to the SecurityCenter. • Administrator can select allowed applications, which are not reported as detections. • Can be used as a "learn" mode to discover which applications to allow and block.
Prompt	<ul style="list-style-type: none"> • Users are prompted about detections. • Detections are reported to the SecurityCenter. • Administrator can select allowed applications. These applications are not reported as detections, and users are not prompted for a response to them. • Users can approve additional applications in response to prompts. These are reported to the SecurityCenter.
Protect	<ul style="list-style-type: none"> • Users are not prompted about detections. • Users are notified about blocked applications. • Detections are reported to the SecurityCenter. • Administrator can select allowed applications, which are not reported as detections.



If the policy is changed from Prompt mode to Protect mode or Report mode, the firewall protection service saves user settings for allowed applications. If the policy is then changed back to Prompt mode, these settings are reinstated.

See also

[Configuring options for Internet applications on page 100](#)

Use learn mode to discover Internet applications

Report mode can be used as a "learn mode" to help you determine which applications to allow.

In Report mode, the firewall protection service tracks but does not block unrecognized Internet applications. You can review detected applications in the Unrecognized Programs report and approve those that are appropriate for your policy. When you no longer see applications you want to allow in the report, change the policy setting to Prompt or Protect mode.

The role of IP addresses

An IP address is used to identify any device that originates or receives a request or a message over networks and the Internet (which comprises a very large group of networks).

Each IP address uses a unique set of hexadecimal characters to identify a network, a subnetwork (if applicable), and a device within the network.

An IP address enables:

- The request or message to be delivered to the correct destination.
- The receiving device to know where the request or message originated and where to send a response if one is required.

McAfee SaaS Endpoint Protection allows you to configure a custom connection to accept only communications that originate from designated IP addresses. You can specify IP addresses that conform to either of these standards:

- IPv4 (Internet Protocol Version 4) — The most common Internet addressing scheme. Supports 32-bit IP addresses consisting of four groups of four numbers between 0 and 255.
- IPv6 (Internet Protocol Version 6) — Supports 128-bit IP addresses consisting of eight groups of four hexadecimal characters.

See also

[Configuring IP addresses on page 103](#)

The role of system service ports

System services communicate through ports, which are logical network connections.

Common Windows system services are typically associated with particular service ports, and your computer's operating system or other system applications might attempt to open them. Because these ports represent a potential source of intrusions into a client computer, you must open them before the computer can communicate through them.

Certain applications, including web servers and file-sharing server programs, must accept unsolicited connections from other computers through designated system service ports. When configuring a custom connection, you can:

- Allow applications to act as servers on the local network or the Internet.
- Add or edit a port for a system service.
- Disable or remove a port for a system service.



Select a port for system services only if you are certain it must be open. You will rarely need to open a port. We recommend that you disable unused system services.

Examples of system services that typically require ports to be opened are:

- **Email server** — You do not need to open a mail server port to receive email. You need to open a port only if the computer running the firewall protection service acts as an email server.
- **Web server** — You do not need to open a web server port to run a web browser. You need to open a port only if the computer running the firewall protection service acts as a web server.



An opened service port that does not have an application running on it poses no security threat. However, we recommend that you close unused ports.

See also

[Configuring system services and port assignments on page 102](#)

Standard assignments for system service ports

These commonly used standard service ports are listed by default, where you can open or close them:

- File and Print Sharing
- Remote Desktop
- Remote Assistance

You can add other service ports as needed. Standard service ports for typical system services are:

System Service	Port(s)
File Transfer Protocol (FTP)	20-21
Mail Server (IMAP)	143
Mail Server (POP3)	110
Mail Server (SMTP)	25
Microsoft Directory Server (MSFT DS)	445
Microsoft SQL Server (MSFT SQL)	1433
Network Time Protocol Port	123
Remote Assistance / Terminal Server (RDP)	3389 (same as Remote Assistance and Remote Desktop)
Remote Procedure Calls (RPC)	135
Secure Web Server (HTTPS)	443
Universal Plug and Play (UPNP)	5000
Web Server (HTTP)	80
Windows File Sharing (NETBIOS)	137-139 (same as File and Print Sharing)

See also

[Configuring system services and port assignments on page 102](#)

Configuration of the firewall protection service

Protecting computers from suspicious activity with a firewall involves monitoring network activity to identify applications, IP addresses, and ports, and blocking those that could cause harm.

There are two methods of configuring the firewall protection service:

- The administrator configures settings in a policy.
- Client computer users configure settings for their computers.

The screenshot shows the configuration interface for the Firewall Protection Service. The top navigation bar includes: Dashboard, Computers, Reports, Policies, My Account, Utilities, Help, Feedback, and Log Off. Below the navigation bar are 'Save' and 'Cancel' buttons. The main content area is titled 'Lab Policy' and has two tabs: 'General Settings' and 'Allowed Internet Applications'. The 'General Settings' tab is active and contains the following sections:

- Client Settings**
- Virus & Spyware Protection**
- Firewall Protection**
- Browser Protection & Web Filtering**

The 'Firewall Protection' section is expanded and shows the following configuration options:

- Firewall Configuration**
 - User configures firewall
 - Administrator configures firewall
- Firewall Configuration**
 - Automatically install firewall protection on all computers using this policy
 - Use Smart Recommendations to automatically approve common Internet applications

When this option is selected, firewall protection allows common Internet applications to access the Internet, as well as the Allowed Internet Applications you specify for this policy. When this option is not selected, firewall protection approves only applications you specify.
- Firewall Status**
 - On
 - Off
- Firewall Protection Mode**
 - Report (do not block suspicious network activity, but record what would have been blocked)
 - Prompt (ask the user what to do if suspicious network activity is detected)
 - Protect (block all suspicious network activity)
- Connection Type**
 - Untrusted network (directly connected to the Internet through a dial-up, DSL, or cable modem; or connected to a public coffee shop, hotel, or airport)
 - Trusted network (indirectly connected to the Internet through a router or hardware firewall in a home or office network)
 - Custom settings [[edit](#)]
- Firewall Reporting Configuration**
 - Report blocked events

For the highest level of security, we recommend that administrators configure settings for the firewall protection service. If you allow users to configure the settings, it is important to educate them about threats and strategies for avoiding risk.

Configuring the settings enables you, the administrator, to control which applications and communications are allowed on your network. It provides the means for you to ensure the highest level of security.

You can also allow users to configure their own firewall protection settings. In this case, no other firewall policy options are available for you to select. This is the default setting.

Interaction between user and administrator policy settings

The firewall protection service handles the settings that you and users configure in a special way. This enables settings to be controlled by either you or the users at different times.

Settings that users select are never discarded, but whether they are used depends on the policy settings assigned to their computers. These also determine whether options for configuring the firewall protection service are displayed in the client console.

If the administrator configures...	The user settings are...	Options available for users to configure?
No policy settings	Active	Yes
<ul style="list-style-type: none"> Protect mode — Automatically block unrecognized Internet applications Report mode — Report unrecognized Internet applications but take no other action 	Inactive	No
Prompt mode — Prompt users for a response when unrecognized Internet applications are detected	<p>Merged with administrator settings. When they differ, user settings take precedence.</p> <p>For example, if a user approves a program, it is allowed even if the administrator has not approved it.</p>	Yes

Configuring policy options

Use these tasks to select policy options for firewall behavior on client computers.

Tasks

- [Selecting general firewall settings on page 99](#)
Use this task to configure the general settings for the firewall protection service.
- [Configuring options for Internet applications on page 100](#)
Use this SecurityCenter task to configure the way the firewall protection service responds to detections of Internet applications.
- [Tracking blocked communications on page 101](#)
Use this SecurityCenter task to track communication attempts (known as *events*) between client computers and network resources that the firewall protection service blocks.

Selecting general firewall settings

Use this task to configure the general settings for the firewall protection service.

- Who configures the firewall
- Connection type



To ensure the highest level of security, we recommend that administrators configure firewall settings. If you allow users to configure the settings, it is important to educate them about threats and strategies for avoiding risk.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Firewall Protection**, then click the **General Settings** tab.
- 3 Under Firewall Configuration, select **Administrator configures firewall** or **User configures firewall**.
If you select the administrator option, additional policy options are displayed for you to configure.
- 4 Under Connection Type, select an option.
- 5 If you selected Custom, click **Edit** to configure related options.
These are described in another section of this document.
- 6 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

[Configuring custom connections on page 101](#)

[Connection type and detections of incoming communications on page 92](#)

Configuring options for Internet applications

Use this SecurityCenter task to configure the way the firewall protection service responds to detections of Internet applications.

These policy option settings determine:

- Whether the firewall protection service checks the list of Internet applications that McAfee has determined to be safe at the www.hackerwatch.org website.
- Whether the firewall protection service blocks an unrecognized application, prompts users for a response, or simply reports it to the SecurityCenter.
- Specific applications to allow or block.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Firewall Protection**, then click the **General Settings** tab.
- 3 Under Firewall Configuration, select or deselect the **Use Smart Recommendations to automatically approve common Internet applications** option.
- 4 Under Firewall Protection Mode, select an option.
To help identify applications required for your users to conduct business, you can use Report mode as a "learn" mode, then view unrecognized programs in a report. You can also select Prompt mode, then look at the applications users have approved on their systems and add them to a policy.
- 5 Click the **Allowed Internet Applications** tab.
This tab lists all the Internet applications detected on the computers in your account.

- 6 Select options as needed.

Select this...	To do this...
Allow	Allow the application.
Allow All	Allow all the applications listed.
Block	Block the application.
Block All	Block all the applications listed.

- 7 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

[Viewing user-approved programs and applications on page 86](#)

[Viewing unrecognized programs detected on the account on page 87](#)

[Firewall protection mode and detections of unknown applications on page 94](#)

Tracking blocked communications

Use this SecurityCenter task to track communication attempts (known as *events*) between client computers and network resources that the firewall protection service blocks.

View information about these events in the report entitled Inbound Events Blocked by the Firewall.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Firewall Protection**, then click the **General Settings** tab.
- 3 Under Firewall Reporting Configuration, select **Report blocked events**.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

[Viewing blocked communications on page 106](#)

Configuring custom connections

Use these tasks to configure system service ports and IP addresses for custom connections.

Tasks

- [Configuring system services and port assignments on page 102](#)
Use this SecurityCenter task to configure system service port assignments for a custom connection.
- [Configuring IP addresses on page 103](#)
Use this SecurityCenter task to add or remove a range of IP addresses in a custom connection.

See also

[Selecting general firewall settings on page 99](#)

[Connection type and detections of incoming communications on page 92](#)

[Custom connections on page 93](#)

Configuring system services and port assignments

Use this SecurityCenter task to configure system service port assignments for a custom connection.

This task allows you to add, remove, or modify a service by specifying its name and the ports through which it communicates with client computers using the policy.

Opening a system service port on a client computer allows it to act as a server on the local network or Internet. Closing a port blocks all communications through the ports with client computers using the policy.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Firewall Protection**, then click the **General Settings** tab.
- 3 Under Connection Type, select **Custom settings**, then click **edit**.
- 4 On the Firewall Custom Settings panel, under Allowed Incoming Connections, configure a service by using one of these methods.

To do this...	Perform these steps...
Allow an existing service by opening its ports	<ol style="list-style-type: none"> 1 Select the checkbox for a service listed in the table. 2 Click OK. <p>Computers using this policy will accept communications through the ports assigned to the service.</p>
Add a new service and open its ports	<ol style="list-style-type: none"> 1 Click Add Connection. 2 In the Add or Edit Incoming Connection panel, type a name for the service, type the ports through which the service will communicate with computers using this policy, then click OK.
Modify an existing service	<ol style="list-style-type: none"> 1 For a service listed in the table, click edit. 2 In the Add or Edit Incoming Connection panel, modify the name for the service and/or the ports through which the service will communicate with computers using this policy, then click OK.
Block an existing service and close its ports	<ol style="list-style-type: none"> 1 For a service listed in the table, click Block. 2 Click OK. <p>The service is removed from the list, and computers using this policy will not accept communications through the ports assigned to the blocked service.</p>

- 5 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

[The role of system service ports on page 96](#)

[Standard assignments for system service ports on page 97](#)

Configuring IP addresses

Use this SecurityCenter task to add or remove a range of IP addresses in a custom connection.

Client computers using this policy will accept communications originating only from the IP addresses you add.



Specify IP addresses and system service ports through which to communicate by using separate tasks.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Firewall Protection**, then click the **General Settings** tab.
- 3 Under Connection Type, select **Custom settings**, then click **edit**.
- 4 On the Firewall Custom Settings panel, under Allowed Incoming Addresses, configure a range of IP addresses for computers using this policy by using one of these methods.

To do this...	Perform these steps...
Accept communications from any IP address	<ol style="list-style-type: none"> 1 Select Any computer. 2 Click OK.
Accept communications from IP addresses on the subnet where the computers are located	<ol style="list-style-type: none"> 1 Select My network (the subnet only). 2 Click OK.
Accept communications from the specified addresses	<ol style="list-style-type: none"> 1 Select Specific address range. 2 Type a beginning and ending IP address range in either IPv4 or IPv6 format. 3 Click Approve. The IP address range is displayed in a the list of allowed addresses. 4 Click OK. <p>Computers using this policy will accept communications originating from all IP addresses in the list you approved.</p>
Block an existing range of IP addresses	<ol style="list-style-type: none"> 1 For the IP address range, click Block. The IP address range is removed from the list of allowed addresses. 2 Click OK. <p>Computers using this policy will not accept communications originating from the IP addresses you removed from the list.</p>



When using a computer in multiple locations, you might want to specify more than one range of IP addresses. For example, you might want one IP address range for office use and another for home use. To specify multiple address ranges, repeat step 4, enter another address range, then click **Add** again.

- 5 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

See also

The role of IP addresses on page 95

Installing and enabling firewall protection at the policy level

Use these tasks to install or enable the firewall protection service automatically for all computers using the policy.

Tasks

- *Installing firewall protection during policy updates on page 104*
Use this task to install the firewall protection service automatically whenever client computers check for an updated policy.
- *Enabling and disabling firewall protection on page 104*
Use this task to enable or disable the firewall protection service on all client computers using the policy.

Installing firewall protection during policy updates

Use this task to install the firewall protection service automatically whenever client computers check for an updated policy.

You might want to use this feature for adding the firewall protection service on computers where the client software for other protection services is already installed. By default, this option is disabled.



Enabling this feature can result in unattended installations on computers where no one is available to authorize communications that are consequently blocked by the firewall protection service. If this feature is used to install the firewall protection service on a server, it is important to configure essential system services first, to prevent disruptions.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Firewall Protection**, then click the **General Settings** tab.
- 3 Under Firewall Configuration, select **Automatically install firewall protection on all computers using this policy**.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Enabling and disabling firewall protection

Use this task to enable or disable the firewall protection service on all client computers using the policy.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Firewall Protection**, then click the **General Settings** tab.

- 3 Under Firewall Status, select **On** or **Off**.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Managing detections

Use these tasks to view and manage suspicious activity and unrecognized applications detected by the firewall protection service.

Tasks

- [Viewing unrecognized programs detected on the account on page 87](#)
Use this SecurityCenter task to view the Unrecognized Programs report, which lists potentially unwanted programs detected on all the client computers on your account.
- [Viewing user-approved programs and applications on page 86](#)
Use this SecurityCenter task to see which applications users have approved to run on their computers.
- [Viewing blocked communications on page 106](#)
Use this SecurityCenter task to view a list of communications that the firewall protection service prevented from reaching client computers.

Viewing unrecognized programs detected on the account

Use this SecurityCenter task to view the Unrecognized Programs report, which lists potentially unwanted programs detected on all the client computers on your account.

Task

For option definitions, click ? in the interface.

- 1 Click the **Reports** tab, then click **Unrecognized Programs**.
- 2 In the Unrecognized Programs report, view detailed information about unrecognized programs and the computers where they were detected by using one of these methods.

When you want to...	Do this...
Display computers or detections	Click the triangle icon next to a name. <ul style="list-style-type: none"> • Under a computer name, show which programs were detected. • Under a program name, show the computers where it was detected. Click a group name to display computers in that group.
View details about detections	Click the name of a potentially unwanted program to display detailed information from the McAfee Labs Threat Library.
View details about a computer where a detection occurred	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.
Approve a program	Click Allow , select one or more programs, select one or more policies where the programs will be approved, then click Save . The selected programs will no longer be detected as threats on computers using the selected policies.

See also

[Approving and unapproving programs in a policy on page 82](#)

[Configuring options for Internet applications on page 100](#)

Viewing user-approved programs and applications

Use this SecurityCenter task to see which applications users have approved to run on their computers.

You can also add the applications to one or more policies so they will not be detected as unrecognized programs on computers using the policies.

Task

For option definitions, click ? in the interface.

- 1 From the SecurityCenter, do any of the following:
 - Click the **Computers** tab, then click a number in the User-Approved Applications column to view applications for the associated computer.
 - Click the **Computers** tab, then click the name of a computer. In the Computer Details page, under Detections, click a number in the User-Approved Applications column to view applications.
- 2 To add the application to one or more policies, in the User-Approved Applications list, under Actions click **Allow**.
- 3 In the Add Approved Application page, select each policy where you want to add the application, then click **Save**.

See also

[Approving and unapproving programs in a policy on page 82](#)

[Configuring options for Internet applications on page 100](#)

Viewing blocked communications

Use this SecurityCenter task to view a list of communications that the firewall protection service prevented from reaching client computers.

Before you begin

The **Report blocked events** option must be enabled on the General Settings tab of the Firewall Protection policy page.

For the purposes of this report, each attempt to communicate is called an *event*.

Task

For option definitions, click ? in the interface.

- 1 Click the **Reports** tab, then click **Inbound Events Blocked by Firewall**.
- 2 In the report, view detailed information about detections and the computers where detections occurred by using one of these methods.

When you want to...	Do this...
Display computers or detections	<p>Click the triangle icon next to a name.</p> <ul style="list-style-type: none"> • Under a computer name, show which detections were found. • Under a detection name, show the computers where it was found. <p>Click a group name to display computers in that group.</p>
View details about events	<p>Click a quantity under Events to display the Inbound Event List, which shows the name of the event, the number of occurrences, and the date on which it was detected.</p>
View details about a computer	<p>Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.</p>

See also

[Tracking blocked communications on page 101](#)

Reports for the firewall protection service

You can view information about firewall detections in administrative reports available from the SecurityCenter on the Reports page. Reports provide details about the specific threats detected over the past year.

- **Unrecognized Programs** — Lists programs detected on client computers that are not recognized by the virus and spyware protection service and the firewall protection service. Allows you to approve Internet applications from within the report.
- **Inbound Events Blocked by Firewall** — Lists the incoming communication attempts that the firewall protection service prevented client computers from receiving, where they originated, and to which computer they were sent.

See also

[Viewing user-approved programs and applications on page 86](#)

[Viewing unrecognized programs detected on the account on page 87](#)

[Viewing blocked communications on page 106](#)

Best practices (firewall protection)

To effectively manage your strategy for guarding against suspicious activity, we recommend that you proactively track the types of threats being detected and where they are occurring.

- 1 Check your status emails or the SecurityCenter website for an overview of your account's status. Ensure that protection is installed on all computers.
- 2 To centralize management and more easily monitor the types of applications and communications allowed on client computers, configure client settings for the firewall protection service in a policy.
- 3 Use McAfee's recommendations for commonly used, safe Internet applications. When this option is enabled, applications rated safe on McAfee's www.hackerwatch.org site are approved automatically, minimizing the need for you or users to approve applications manually.
- 4 Check the Unrecognized Programs report frequently to monitor the Internet applications that users are allowing on client computers. If you know some of the applications are safe and do not want them to be detected as threats, add them to policies.
- 5 If you want to monitor the inbound communications that firewall protection has blocked, select the **Report blocked events** policy option, then check the Inbound Events Blocked by Firewall report regularly.
- 6 Use "learn" mode to identify which Internet applications to allow. This ensures that no applications required for your business are blocked before you have the opportunity to authorize their use. Then change the protection mode to Protect.
- 7 If particular types of suspicious activity are occurring frequently or certain computers appear vulnerable, update the policy to resolve these issues.
 - Ensure that the firewall protection service is enabled.
 - Carefully specify the environment where client computers are used. For users with mobile computers, ensure that they know how to select the correct connection type each time their environment changes and that their policy allows them to do so.
 - Before installing the firewall protection service on a server, ensure that the server's system services and Internet applications are configured correctly. If there is a possibility that the firewall protection service might be installed when no user is present to monitor the installation, disable the policy setting for **Automatically install the desktop firewall on all computers using this policy**.
 - When running the firewall protection service on a server, ensure that system service ports are configured correctly to prevent disruption of system services. Ensure that no unnecessary ports are open.
 - For maximum protection, set firewall protection mode to **Protect** to automatically block suspicious activity.
- 8 If your account includes computers that are operated in multiple environments, such as in the office and in unsecured public networks, update the policy appropriately.
 - Configure policy options that allow users to select their connection type to match their environment. Be sure they know when and how to select the appropriate connection type.
 - If you configure custom connections that include IP addresses, specify ranges of IP addresses appropriate for all their working environments.

6

Using the Browser Protection Service and Web Filtering

The browser protection service displays two types of information in the web browser window on client computers to safeguard users against web-based threats.

- A safety rating for each website.
- A safety report for each website that includes a detailed description of test results and feedback submitted by users and site owners.

The web filtering module, available with some versions of McAfee SaaS Endpoint Protection, provides features for regulating access to websites. Policy options allow administrators to control access to sites based on their safety rating, the type of content they contain, and their URL or domain name.

Contents

- ▶ *Browser protection features*
- ▶ *How safety ratings are compiled*
- ▶ *Safety icons and balloons protect during searches*
- ▶ *SiteAdvisor menu protects while browsing*
- ▶ *Safety reports provide details*
- ▶ *Information that browser protection sends to McAfee*
- ▶ *Installing browser protection during policy updates*
- ▶ *Web filtering features*
- ▶ *Enabling and disabling browser protection via policy*
- ▶ *Enabling and disabling browser protection at the client computer*
- ▶ *Block and warn sites by safety ratings*
- ▶ *Block and warn sites by content*
- ▶ *Authorize and prohibit sites by URL or domain*
- ▶ *Customizing messages for users*
- ▶ *Viewing browsing activity*
- ▶ *Web Filtering report*
- ▶ *Best practices (browser protection)*

Browser protection features

As the browser protection service runs on client computers, it notifies users about threats they might encounter when searching or browsing websites by displaying icons and reports.

Safety rating for each site and site resource

- When searching, a safety rating designated by a green, yellow, red, or gray icon appears next to each site listed on a search results page.
- When browsing, the SiteAdvisor menu button appears in the browser window in the color that matches the safety rating for the current site.

Safety report for each site

- The report includes a detailed description of test results and feedback submitted by users and site owners.
- Users access safety reports to learn more about how the safety rating for a site was calculated.

The browser protection service supports these browsers:

- Microsoft Internet Explorer browser (versions 6.0, 7.0, and 8.0)
- Mozilla Firefox browser (versions 2.0, 3.0, and 3.5)



The only difference in functionality between the browsers is that Firefox does not allow users to hide the SiteAdvisor menu button with the **View | Toolbars** command or check file downloads.

Web filtering features

Some versions of McAfee SaaS Endpoint Protection include the web filtering module, which provides features that enable administrators to monitor and regulate browser activity on network computers.

- Control user access to websites and file downloads, based on their safety rating or type of content.
- Create a list of authorized and prohibited sites, based on their URL or domain.
- Block user access to phishing pages.
- Customize the message that browser protection displays on computers that attempt to access a blocked website.

Web filtering policy options also allow administrators to disable the browser protection service at the policy level or from an individual client computer.

How safety ratings are compiled

A McAfee team derives safety ratings by testing a variety of criteria for each site and evaluating the results to detect common threats.

Automated tests compile safety ratings for a website by:

- Downloading files and checking for viruses and potentially unwanted programs bundled with the download.
- Entering contact information into signup forms and checking for resulting spam or a high volume of non-spam emails sent by the site or its affiliates.






- Checking for excessive popup windows.
- Checking for attempts by the site to exploit browser vulnerabilities.
- Checking for deceptive or fraudulent practices employed by a site.

The team assimilates 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, bad shopping experiences, and selling services that can be obtained without cost from other sources.
- Additional analysis by McAfee professionals.

Safety icons and balloons protect during searches

When users type keywords into a popular search engine such as Google, Yahoo!, MSN, Ask, or AOL.com, color-coded safety icons appear next to sites listed in the search results page.

- | | |
|---|---|
|  (Green, checkmark) | Tests revealed no significant problems. |
|  (Yellow, exclamation point) | Tests revealed some issues users should know about. For example, the site tried to change the testers' browser defaults, displayed popups, or sent them a significant amount of non-spam email. |
|  (Red, x) | Tests revealed some serious issues that users should consider carefully before accessing this site. For example, the site sent testers spam email or bundled adware with a download. |
|  (Red, bar) | This site is blocked by a policy option. |
|  (Gray, question mark) | This site is unrated. |

Placing the cursor over an icon displays a safety balloon that summarizes the safety report for a site. Click **Read site report** for a detailed safety report.

Using site safety balloons

Before visiting a site listed on a search page, check safety information about the site.

Use this task to view safety information about a site through its safety rating icon.

Task

- 1 Hold the cursor over the site's safety icon. A safety balloon displays a high-level summary of the site's safety report.
- 2 For additional details, either:
 - Click **Read site report** in the safety balloon to view details of the site's safety report.
 - Click **Troubleshoot** when a communication error occurs, which results in no safety rating being displayed. No rating for a site might be caused by a broken Internet connection or a problem with the server maintained by McAfee where ratings information is stored.

Testing communication problems

Use this task from a client computer to determine why the browser protection service is not communicating with the server that provides safety ratings information.

Communication problems are indicated by a gray SiteAdvisor menu button with disconnected cables.






Task

- 1 Hold the cursor over the SiteAdvisor menu button to display the safety balloon.
- 2 In the safety balloon, click **Troubleshooting**.
Three connectivity tests run to verify that:
 - The computer can connect to the Internet.
 - The server where site safety ratings information is stored is running.
 - The server is responding to requests for site safety ratings information.
- 3 Check the results when they are displayed and follow any instructions to resolve the problem.
- 4 If you have taken steps to resolve the problem and want to test the connection, click **Repeat Tests**.

SiteAdvisor menu protects while browsing

When users browse to a website, a color-coded menu button appears in the top-left corner of the window. The color of the menu button corresponds to the site's safety rating.

Placing the cursor over this button displays a safety balloon that summarizes the safety report for the site, with a link to the detailed site report page. The menu button next to the icon displays the SiteAdvisor menu.

This button...	With this color and symbol...	Indicates this...
	Green, checkmark	The site is safe.
	Yellow, exclamation point	There might be some issues with the site.
	Red, x	There might be some serious issues with the site.
	Gray, question mark	No rating is available for the site.
	Gray, disconnected cables	Your browser is not communicating with the SiteAdvisor website that contains rating information.

- When the browser protection service is disabled, the menu button is gray.
- When visiting a site on your network's intranet, the menu button is gray. The browser protection service does not report visits to intranet sites to the server where safety ratings information is stored.
- When a communication error occurs with the server where safety ratings information is stored, the menu button is gray with disconnected cables.
- In Internet Explorer, users can display or hide the menu button by using the **View | Toolbars | McAfee SiteAdvisor** menu option. This does not affect the functional status (enabled or disabled) of the client software for the browser protection service.





Firefox users cannot hide the menu button while the browser protection service is enabled.

Using the SiteAdvisor menu

Use this task to display menu options for accessing features of the browser protection service

Task

- Click the down arrow on the SiteAdvisor menu button to view the SiteAdvisor menu.

Select this command...	To do this...
View Site Report	Display the safety report for the current site (not available when the browser protection service is disabled).  You can also click Read site report in the site safety balloon.
Show Balloon	Display the current site's safety balloon (not available when the browser protection service is disabled). The balloon disappears after a few seconds, or you can click the close button.  The site safety balloon also appears by placing the cursor over the menu button.
Disable/Enable SiteAdvisor	Turn the client software for the browser protection service off or on (available only when a policy option is configured to allow this functionality).
About	Access a brief description of the browser protection service, its license agreement, and its privacy policy.

Safety reports provide details

Users can supplement the color-coded safety information for a site by viewing its detailed safety report. These reports describe specific threats discovered by testing and include feedback submitted by site owners and users.

Safety reports for sites are delivered from a dedicated server maintained by McAfee. They provide the following information:

Item	Explanation
Summary	The overall rating for the website. We determine this rating by looking at a wide variety of information. First, we evaluate a website's email and download practices using our proprietary data collection and analysis techniques. Next, we examine the website itself to see if it engages in annoying practices such as excessive pop-ups or requests to change your home page. Then we perform an analysis of its online affiliations to see if the site associates with other sites flagged as red. Finally, we combine our own review of suspicious sites with feedback from our volunteer reviewers and alert you to sites that are deemed suspicious.
Established	The year the domain name was registered. More recently registered websites have had less time to prove their safety and trustworthiness.
Country	The country where a domain is registered. Keep in mind that it's sometimes more difficult to get good customer service or resolve disputes with websites registered outside of your country of residence.
Popularity	The level of how popular the website is. Don't assume, however, that popularity always goes hand in hand with safety. For example, some very popular prize sites send lots of spam, and some very popular file-sharing programs bundle adware. Likewise, many personal websites, blogs, and small business sites that do not get a lot of traffic can be safe to browse and use. That's why the analysis behind McAfee's overall verdict is so useful.

Item	Explanation
Email Results	<p>Overall rating for a website's email practices. We rate sites based on both how much email we receive after entering an address on the site as well as how spammy the email we receive looks. If either of these measures is higher than what we consider acceptable, we'll give the site a yellow warning. If both measures are high, or one of them looks particularly egregious, we'll give the site a red warning.</p> <p>Each email link opens a detailed email analysis page.</p>
Downloads	<p>Overall rating about the impact a site's downloadable software had on our testing computer. Red flags are given to sites that have virus-infected downloads or that add unrelated software which many people would consider adware or spyware. The rating also takes note of the network servers a program contacts during its operation, as well as any modifications to browser settings or a computer's registry files.</p> <p>Each download link opens a detailed download analysis page.</p>
Online Affiliations	<p>Indication of how aggressively the site tries to get you to go to other sites that we've flagged as red. It is a very common practice on the Internet for suspicious sites to have many close associates with other suspicious sites. The primary purpose of these "feeder" sites is to get you to visit the suspicious site. A site can receive a red warning if, for example, it links too aggressively to other red sites. In effect, a site can become "red by association" due to the nature of its relationship to red flagged domains.</p>
Annoyances	<p>Common web practices that users find annoying, such as excessive popups, requests to change a user's home page, or requests to add a site to the browser's favorites list. We also list third-party cookies (sometimes known as "tracking cookies") in this section. If a website has a lot of popups and, in particular, if it engages in practices such as popping up more windows when you try to close them, we will give that website a red flag.</p>
Exploits	<p>Rare but extremely dangerous security threats caused by a website "exploiting" a browser's security vulnerability. The exploit can cause the user's computer to receive programming code which can cause adware infections, keystroke spying, and other malicious actions which can leave a computer essentially unusable.</p>
Reviewer and Site Owner Comments	<p>Reviewers and site owners can provide additional information and commentary to supplement McAfee's automated test results.</p>
Results	<p>Summary of the comments made by the entire reviewer community of SiteAdvisor users. Reviewers can rate sites for downloads, email practices, shopping experiences, and more. This input is particularly important in helping the community of SiteAdvisor users guide each other to trustworthy e-commerce websites. Anonymous input alone is not enough to change a site's overall rating, but sufficient votes from registered users can affect a site's rating.</p>
Website owner comments	<p>Allows owners of analyzed websites to address our ratings. Owners are free to comment, disagree, or clarify. These comments are posted unedited after we verify the authenticity of the person leaving the comment. We manually review all owner comments and if an error was made, we will try our best to promptly correct it. We don't allow sites to pay to be rated or to change or improve their ratings.</p>
Reviewer comments	<p>What our volunteer reviewers have to say about this website. These comments are posted unedited.</p>

Viewing safety reports

Use this task to view safety reports to obtain more information about a site's safety rating.

Task

- Do any of the following to view a safety report for a site:

From this location...	Do this...
Website	<ul style="list-style-type: none">• Click the SiteAdvisor menu button, then select View Site Report.• Hold the cursor over the SiteAdvisor button, then select Read site report.• Click the SiteAdvisor button.
Search results page	Click the safety icon following the web page link.
Home page (www.siteadvisor.com) or Analysis page for the SiteAdvisor product line	Type a URL in the Look up site report box.

Information that browser protection sends to McAfee

The client software sends the following information to the SecurityCenter for use in the Web Filtering report.

- Type of event initiated by the client computer (site visit or download).
- Unique ID assigned by McAfee SaaS Endpoint Protection to the client computer.
- Time of event.
- Domain for event.
- URL for event.
- SiteAdvisor site safety rating for the event's site.
- Whether the event's site or site resource is added to the Exceptions list as an authorized or prohibited site.
- Reason for action (allow, warn, or block) taken by the browser protection service.

The browser protection service sends the following information to the server maintained by McAfee to store SiteAdvisor site safety rating information:

- Version of the browser protection client software running on the client computer.
- Version of the operating system running on the client computer.
- Language and country locale selected for the operating system and browser running on the client computer.
- Host name and part of the URL for each website the client computer requests to access.
- MD5 algorithm for each application the client computer requests to download.

When a client computer visits a website, the browser protection service tracks the site's *domain specifier*. The domain specifier is the smallest amount of information required for the browser protection service to uniquely identify the site being rated for security. The focus of the browser protection service is protecting your client computers; no attempt is made to track personal Internet usage.



The browser protection service does not send information about your company's intranet site to the server where SiteAdvisor site safety ratings information is stored.

See also

[Viewing browsing activity on page 125](#)

[Web Filtering report on page 125](#)

Installing browser protection during policy updates

Use this task to install the client software for the browser protection service automatically whenever client computers check for an updated policy.

You might want to use this feature for adding the browser protection service on computers where the client software for other protection services is already installed. By default, this option is enabled.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection**, then click the **General Settings** tab.
- 3 Under Firewall Configuration, select **Automatically install browser protection on all computers using this policy**.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Web filtering features

If you purchased a version of McAfee SaaS Endpoint Protection that includes the web filtering module, the Policies page in the SecurityCenter displays an expanded set of policy options labeled **Browser Protection & Web Filtering**.

The additional policy options enable you to configure these features.

- Regulate user access to websites, based on their safety rating (for example, block access to red sites and display a warning before opening yellow sites).
- Regulate user access to phishing pages.
- Regulate access to site resources, such as file downloads, based on their safety rating.
- Regulate user access to websites based on their content (for example, block access to shopping or gambling sites).
- Create a list of authorized and prohibited sites, based on their URL or domain.
- Customize the message that the browser protection service displays on computers that attempt to access a blocked website.

- Enable and disable the browser protection service at the policy level.
- Specify whether the browser protection service can be disabled from a client computer.

Enabling and disabling browser protection via policy

Use this task to enable and disable the browser protection service on all client computers using the policy.

This feature is available only in versions of the browser protection service that include the web filtering module.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
- 3 Under Browser Protection Status, select or deselect the option **Disable browser protection on all computers using this policy**.
This feature takes effect on client computers the next time they update their policy.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Enabling and disabling browser protection at the client computer

Use this task to specify whether the browser protection service can be disabled from a client computer.

When this capability is enabled, the **Enable SiteAdvisor** or **Disable SiteAdvisor** option appears on the SiteAdvisor menu.



If the browser protection service remains disabled, it is re-enabled automatically the next time the client computer checks for policy updates. (This presumes that the browser protection service is enabled at the policy level.)

This feature is available only in versions of the browser protection service that include the web filtering module.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
- 3 Under Browser Protection Status, select or deselect **Allow users to enable or disable browser protection**.
- 4 Specify whether a password is required on the client computer. If so, type the password.
- 5 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Block and warn sites by safety ratings

Web filtering adds policy options that allow you to use the site safety ratings provided by the browser protection service to determine whether users can access a site or resources on a site, such as download files.

- For each yellow, red, or unrated site, specify whether to allow, warn, or block the site.
- For each yellow, red, or unrated download file, specify whether to allow, warn, or block the download. This enables a greater level of granularity in protecting users against individual files that might pose a threat on sites with an overall green rating.
- For each phishing page, specify whether to block or allow access. This enables a greater level of granularity in protecting users from pages that employ phishing techniques on a site with an overall green rating.

Dashboard Computers » Reports » Policies » My Account » Utilities Help » Feedback Log Off

Actions Save Cancel

Lab Policy

Client Settings

Virus & Spyware Protection

Firewall Protection

Browser Protection & Web Filtering

General Settings Content Rules Exceptions

Automatic Installation

Automatically install browser protection on all computers using this policy

Access to Sites

Configure access to sites based on their overall safety rating.

Yellow Red Unrated

Overall site access: Warn Block Allow

Access to Downloads

Configure access to individual file downloads based on their ratings.

Note: Failure to block downloads rated yellow or red might permit dangerous file downloads from authorized sites.

Yellow Red Unrated

File download access: Warn Block Allow

Access to Phishing Pages

Select this option to block all phishing pages.

Note: When this option is not enabled, users might be able to access known phishing pages within authorized sites.

Block phishing pages

Enforcement Messaging

Enter explanatory messages (up to 200 characters) to display when users attempt to access sites you have configured access rules for.

Language: English

Message: An unacceptable security risk is posed by this site.

Browser Protection Status

Disable browser protection on all computers using this policy

Allow users to enable or disable browser protection

Without password

With password

Password:

When you block a site, users are redirected to a message explaining that the site is blocked. A policy option allows you to customize the message that is displayed.

When you configure a warning action for a site, users are redirected to a message explaining that there might be threats on the site. They can then decide whether to cancel or continue their navigation to the site.



To ensure users can access specific sites that are important to your business, no matter how they are rated, add them to the Exceptions list as an authorized site. For authorized sites, the browser protection service ignores the safety rating.

Blocking or warning site access based on safety ratings

Use this task to block users from accessing sites that contain threats or to warn users about potential threats on sites.

This feature is available only in versions of the browser protection service that include the web filtering module.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
- 3 Under Access to Sites, select a separate level of access for red, yellow, and unrated sites.
 - **Block** — Block access to all sites with the specified rating.
 - **Warn** — Display a warning when users attempt to access a site with the specified rating.
 - **Allow** — Allow access to all sites with the specified rating.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Blocking or warning file downloads based on safety ratings

Use this task to block users from downloading files that contain threats or to warn users about potential threats from downloads.

A site with an overall safety rating of green can contain individual download files rated yellow or red. To protect users, specify an action that is specific to the rating for an individual file.

This feature is available only with versions of the browser protection service that include the web filtering module.



This feature is not available in Firefox browsers because Firefox is unable to recognize safety ratings for individual site resources.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.

- 3 Under **Access to Downloads**, select a separate level of access for red, yellow, and unrated files.
 - **Block** — Block all downloads of files with the specified rating.
 - **Warn** — Display a warning when users attempt to download a file with the specified rating.
 - **Allow** — Allow all downloads of files with the specified rating.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Blocking phishing pages

A site with an overall safety rating of green can contain phishing pages. To protect users, use this web filtering task to block access to these pages.

This feature is available only with versions of the browser protection service that include the web filtering module.

Task

For option definitions, click ? in the interface.

- 1 On the **Policies** page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
- 3 Under **Access to Phishing Pages**, select **Block phishing pages**.
- 4 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Block and warn sites by content

Web filtering allows the browser protection service to retrieve content classifications for a site. These are stored on the server maintained by McAfee where site safety ratings information is also stored. Use policy options to allow, warn, or block access to sites based on the type of content they contain.

This feature is available only with versions of the browser protection service that include the web filtering module.

Dashboard Computers » Reports » Policies » My Account » Utilities Help » Feedback Log Off

Actions

Save Cancel

Lab Policy

General Settings Content Rules Exceptions

Browser protection can regulate user access to sites based on their content. Use this list to specify the types of content for which browser protection allows access, blocks access, or displays a warning.

Filters

Use the options at the top of the list to filter and sort the content listing. Then select categories of content and click Allow, Warn, or Block.

Functional group: Risk/Fraud/Crime

Risk group: Security

Status: All

Allow Warn Block

<input type="checkbox"/>	Content Category	Functional Group	Risk Group	Status
<input type="checkbox"/>	Anonymizers	Risk/Fraud/Crime	Security	Blocked
<input type="checkbox"/>	Anonymizing Utilities	Risk/Fraud/Crime	Security	Blocked
<input type="checkbox"/>	Hacking/Computer Crime	Risk/Fraud/Crime	Security	Blocked
<input type="checkbox"/>	Malicious Sites	Risk/Fraud/Crime	Security	Blocked
<input type="checkbox"/>	P2P/File Sharing	Risk/Fraud/Crime	Security	Allowed
<input type="checkbox"/>	Spyware/Adware	Risk/Fraud/Crime	Security	Blocked
<input type="checkbox"/>	Phishing	Risk/Fraud/Crime	Security	Blocked
<input type="checkbox"/>	Spam URLs	Risk/Fraud/Crime	Security	Blocked
<input type="checkbox"/>	Parked Domain	Risk/Fraud/Crime	Security	Blocked

Allow Warn Block

The approximately 100 site content categories are grouped by function and risk, which allows for easy application of the policy settings based on content alone or on content functional groups (the functions that users can perform by accessing the content) or content risk groups (the risks that the content might present to your business).

For example, select a functional group of Risk/Fraud/Crime and a risk group of Security to view all the categories of content that might pose a threat to user security due to fraud or criminal intent. Select a risk group of Productivity to display all the categories of content that might impact users' productivity adversely, such as shopping or gaming. These filters assist you in locating all the content categories for which you might want to configure actions.

Blocking or warning site access based on content

Use this task to block users from accessing sites that contain particular types of content.

This feature is available only with versions of the browser protection service that include the web filtering module.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection & Web Filtering**, then click the **Content Rules** tab.
- 3 Select one or more filtering options to customize the content categories listed. (*Optional*)
 - **Functional group** — Display content categories that are used to perform similar functions.
 - **Risk group** — Display content categories that present similar risks to users.
 - **Action** — Display the content categories for which you have configured an allow, block, or warn action.
- 4 In the list, select the content categories for which you want to select an action.
- 5 Click **Allow**, **Block**, or **Warn**.
This action will be applied when users attempt to access websites that contain the selected categories of content.
- 6 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Authorize and prohibit sites by URL or domain

Web filtering allows you to set up an Exceptions list containing a list of sites that users can or cannot access.

- Authorized sites that users are always allowed to access, regardless of their safety rating or type of content. Add authorized sites to ensure access to sites that are important to your business.
- Prohibited sites that users are never allowed to access. Add prohibited sites to block access to sites that are not related to job performance or do not conform to company security standards.



By authorizing a site, the browser protection service ignores the safety rating for that site. Users can access authorized sites even if threats have been reported on these sites and they have a safety rating of red. Users can also access unsafe downloads and phishing pages on authorized sites. It is important to exercise caution when adding authorized sites to an Exceptions list.

How site patterns work

The Exceptions list uses *site patterns* to specify a range of sites that are authorized or prohibited. This enables you to authorize or prohibit a particular domain or a range of similar sites without entering each URL separately.

When a client computer attempts to navigate to a site, the browser protection service checks whether the URL matches any site patterns configured in the Exceptions list. It uses specific criteria to determine a match.

A site pattern consists of a URL or partial URL, which the browser protection service interprets as two distinct sections: *domain* and *path*.

Site pattern: www.mcafee.com/us/enterprise	
http:// www.mcafee.com	<p>This is the domain. The domain consists of two parts:</p> <ul style="list-style-type: none"> • Protocol. In this case: http:// • Internet domain. In this case: www.mcafee.com <p>Domain information is matched from the <i>end</i>. A matching URL's domain must <i>end</i> with the site pattern's domain. The protocol can vary.</p> <p>These domains match:</p> <ul style="list-style-type: none"> • http:// ftp.mcafee.com • https://mcafee.com • http://www.info.mcafee.com <p>These domains do not match:</p> <ul style="list-style-type: none"> • http:// www.mcafee.downloads.com • http://mcafee.net • http://www.mcafeeasap.com • http://us.mcafee.com
/us/enterprise	<p>This is the path. The path includes everything that follows the / after the domain.</p> <p>Path information is matched from the <i>beginning</i>. A matching URL's path must <i>begin</i> with the site pattern's path.</p> <p>These paths match:</p> <ul style="list-style-type: none"> • /us/enterpriseproducts • /us/enterprise/products/security <p>These paths do not match:</p> <ul style="list-style-type: none"> • /emea/enterprise • /info/us/enterprise

Site patterns must be at least six characters in length, and they do not accept wildcard characters. The browser protection service does not check for matches in the middle or end of URLs.

Use the "." character at the beginning of a site pattern to match a specific domain. For convenience, the "." character disregards the protocol and introductory characters.

Example: **.mcafee.com**

Matches	Does not match
<ul style="list-style-type: none"> • http://www.info.mcafee.com • http://mcafee.com • http://ftp.mcafee.com 	<ul style="list-style-type: none"> • http://www.mcafeeasap.com • http://salesmcafee.com • http://ftp.mcafee.net

Adding authorized and prohibited sites

Use this web filtering task to create and manage an Exceptions list for browser protection.

An Exceptions list contains:

- Authorized sites that users are always allowed to access.
- Prohibited sites that users are never allowed to access.

This feature is available only with versions of the browser protection service that include the web filtering module.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection & Web Filtering**, then click the **Exceptions** tab.
- 3 Click **Add to Exceptions List**.
- 4 Type a URL or site pattern into the text box, then click an action to associate with the site.
 - **Authorize** — Add the site to the Exceptions list as an authorized site, which users are always allowed to access.
 - **Prohibit** — Add the site to the Exceptions list as a prohibited site, which users are not allowed to access.
 - **Cancel** — Close the text box without adding the site to the list.
- 5 Repeat step 4 for each site you want to add to the list.
- 6 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Customizing messages for users

Use this task to create a message that displays when users attempt to access sites that are blocked.

The message appears when users attempt to access a site you have blocked by ratings, by content, or by adding it to the Exceptions list as a prohibited site. Instead of navigating to the site, users are redirected to a page displaying the customized message. You might use the message to explain why the site is blocked.

The message appears on client computers in the language configured for the client software, if you have created the message in that language.

This feature is available only with versions of the browser protection service that include the web filtering module.

Task

For option definitions, click ? in the interface.

- 1 On the Policies page, click **Add Policy** (or click **Edit** to modify an existing policy).
- 2 Select **Browser Protection & Web Filtering**, then click the **General Settings** tab.
- 3 Under Enforcement Messaging, select a language for the message.
(By default, the language in which you have logged in appears. If that language is not available for messages, English is displayed.)
- 4 Type a message of up to 200 characters.

- 5 Repeat steps 3 and 4 for each language for which you want to configure a message.
- 6 Click **Save**.
(For a new policy, click **Next**, select additional options for the policy, then click **Save**.)

Viewing browsing activity

Use this task to view the Web Filtering report, which lists visits to websites by client computers and attempts to access websites for which you have configured policy options to regulate access.

Task

- 1 Click the **Reports** tab, then click **Web Filtering**.
- 2 In the Web Filtering report, view the number of green sites visited by client computers on the network. No detailed information is available for green sites.
- 3 For yellow and red sites, do any of the following.

When you want to...	Do this...
Display the sites in a domain	Click the triangle icon next to the domain name to display the sites users attempted to access in the domain.
View details about an access attempt	<p>Click a quantity to display the Event Details page:</p> <ul style="list-style-type: none"> • When View Computers is selected, click a quantity in an action column (such as Blocked). • When View Domains is selected, click a quantity under Access Count. <p>The Event Details page shows the name of the computer that attempted to access the site, the URL for the site, the type of access attempted, and the date and time of the attempted access.</p>
View details about a computer	Click a computer name to display the Computer Details page, which displays information about the computer, its service components, and its detections.

See also

[Information that browser protection sends to McAfee on page 115](#)
[Web Filtering report on page 125](#)

Web Filtering report

Use the Web Filtering report, available from the SecurityCenter, to track Internet usage and browsing activity on your network.

This report lists visits to websites and attempts to access websites for which you have configured policy options to regulate access. Use this report to view detailed information about the specific sites, their safety ratings and content categories, the computers that attempted to access them, and the action taken by browser protection.

This report is available only with versions of the browser protection service that include the web filtering module.

See also

[Viewing browsing activity on page 125](#)
[Information that browser protection sends to McAfee on page 115](#)

Best practices (browser protection)

To develop an effective strategy for guarding against web-based threats, we recommend that you proactively track browsing activity on your network and configure policy options appropriate for your users.

- 1 Check your status emails or the SecurityCenter website for an overview of your account's status. Ensure that the client software for the browser protection service is installed and enabled on all computers.
- 2 Check the Web Filtering report regularly to see what sites users are visiting, their safety ratings, and their content categories.
- 3 Using the Web Filtering report:
 - Determine whether users are visiting sites that should be added to an Exceptions list. Authorize sites that are important to productivity to ensure that users can always access them. Prohibit sites that do not comply with company policy or contribute to job performance goals to ensure users cannot access them.
 - Note the number of visits to red, yellow, and unrated sites. If appropriate, configure policy options to block sites or site resources that have particular safety ratings.
 - Note the content categories for sites being visited. If appropriate, configure policy options to block sites containing particular types of content.
 - Note which computers are visiting which sites. If appropriate, configure different policies for computers that should and should not be able to access particular sites or content.
- 4 Customize a message to display on client computers that attempt to access a site you have blocked.
- 5 To ensure that all computers are protected against web-based threats, configure policy options to enable the browser protection service via policy and prevent users from disabling the client software on their computers.

7

Using the SaaS Email Protection Service

The SaaS email protection service supplements the email scans performed on client computers by the virus and spyware protection service. Your company's email is redirected through the McAfee multi-layered spam detection system and scanned before entering the network, with less than a one-second delay in transit.

The SaaS email protection service resides outside the network; it requires no system resources, and there's no hardware or software to install. Use the SecurityCenter and the SaaS email and web protection portal to manage web protection features.

Contents

- ▶ *Core SaaS email protection features*
- ▶ *Additional SaaS email protection services*
- ▶ *The SaaS email protection widget and portal*
- ▶ *Account activation and setup*
- ▶ *Reports and statistics for SaaS email protection*
- ▶ *Getting more information*

Core SaaS email protection features

Use the core features of the SaaS email protection service to safeguard your email communication and information integrity.

The SaaS email protection service routes all inbound email through McAfee servers to scan for threats. It checks for spam, phishing scams, viruses, directory harvest attacks, and other email-borne threats in messages and attachments before they enter your network, then blocks them. The SaaS email protection service allows you to specify whether to deny or quarantine messages detected as spam.

The SaaS email protection service provides:

Protection from email-borne threats — The flood of email threats is stopped before entering the network.

Real-time, around-the-clock email security — Email is processed all day, every day in real time through a highly secure system architecture that operates with no detectable latency.

Simplified management — Centralized, web-based policy management through the SaaS email and web protection portal allows you to configure comprehensive policies for threats and content filtering (for inappropriate words and phrases). You can also check email statistics and activity, and view reports and check quarantined messages.

Customizable scanning criteria — Policy options allow you to configure which threats and types of content should be blocked. You can allow different types of content for different users and groups of users on your account.

A robust set of core features — All accounts for the SaaS email protection service include:

- More than 20 separate filters
- Advanced spam blocking
- Virus and worm scanning
- Content and attachment filtering
- Fraud protection
- Protection from email server attacks
- Outbound email filtering
- Accurate and effective quarantine with customizable reporting
- Comprehensive email threat reporting
- Secure message delivery over Enforced Transport Layer Security (TLS)

You can customize the way these features work by configuring policy settings on the SaaS email and web protection portal. A link is provided on the Help page of the SecurityCenter to detailed information about configuring features for the SaaS email protection service.

Additional SaaS email protection services

Purchase additional services to supplement the core features set of the SaaS email protection service. Instructions for setting up these services are provided when you activate your account. They are available at any time in a welcome kit on the Utilities page of the SecurityCenter. A separate welcome kit is available for each additional service you purchase except encryption.

You can also customize the way these features work by configuring policy settings on the SaaS email and web protection portal. A link is provided on the Help page of the SecurityCenter to guides that contain detailed instructions for configuring features for the SaaS email protection service.

Archiving

Stores all internal, inbound, and outbound email messages in a centralized, secure location.

- Stores messages and message metadata in read-only format to protect them in their original state.
- Verifies that stored message copies are identical to the original.
- Protects messages on your email server from deletion until accurate copies are made and verified.
- Adds a unique numeric identifier to each message to comply with SEC requirements prohibiting tampering or deletion of messages.
- Provides tools for locating information in messages, attachments, and metadata with simple or complex search criteria, including user, date range, message content, or attachment content.
- Transports messages to storage securely via TLS or SSL and stores them using 256-bit encryption.

Continuity

Enables web-based email access, management, and use during planned or unplanned outages.

- Retains all inbound and outbound email sent or received during the outage.
- Synchronizes an accurate record of all outage-period message activity with your email servers.

Intelligent Routing

Routes filtered email to your organization's distributed email systems.

- Accepts email for a single domain and routes it to different email servers and environments (for example, different geographic locations or business units), which can use different policy settings.
- Creates email address uniformity for corporate branding purposes.
- Facilitates the addition of new local domains to the existing public domain as your company expands its workforce or locations.
- Reduces the need to purchase, administer, and maintain internal email routing equipment.
- Leverages disaster recovery when one email sites goes down, without interrupting email service for other sites that are still up and running.

Encryption

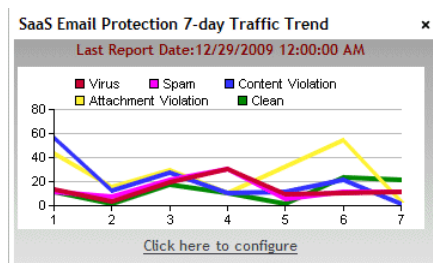
Encrypts the content of outbound messages.

- Ensures the security of email message content through encryption and by requiring account credentials for recipients.
- Allows you to define which messages to encrypt (for example, all messages that contain a specified keyword) and for which users or recipients.
- Provides recipients with two methods for retrieving the content in encrypted messages sent to them:
 - Remotely, by using a link that appears in a delivery notification.
 - Locally, by downloading a Secure Reader application to client computers.
- Allows recipients to customize the way encrypted email is delivered.

The SaaS email protection widget and portal

The SaaS email protection widget and portal allow you to view activity and configure features for your SaaS email protection service account.

When you purchase a subscription for the SaaS email protection service, a SaaS email protection widget is displayed on the Dashboard page of the SecurityCenter. The widget contains a link to activate the service. After activation, the link's text changes (**Click here to configure**); use it to access the SaaS email and web protection portal.



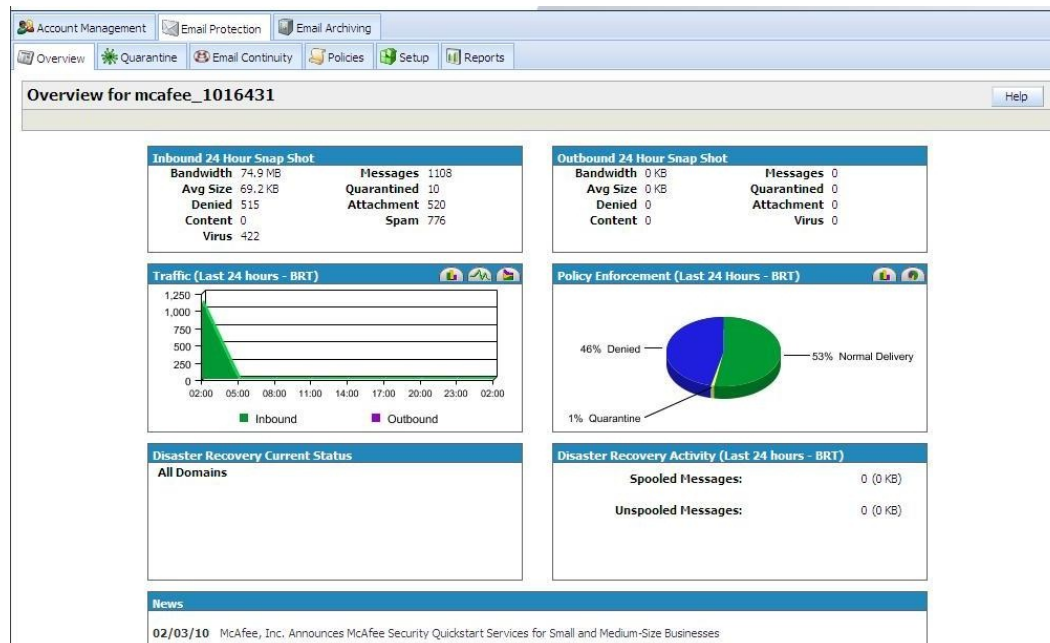
SaaS Email Protection 7-day Email Summary x

Message Type	Message Count
Clean	84
Virus	95
Spam	96
Content Violation	138
Attachment Violation	186

Click here to configure

The portal provides tools for configuring administrative features and policy options, checking email statistics and activity, and viewing reports. The portal supports these browsers running on the administrative computer:

- Internet Explorer 8.x on Windows XP, Windows Vista, and Windows 7
- Internet Explorer 7.x on Windows XP and Windows Vista
- Firefox 3.5.x on Windows XP, Windows Vista, and Windows 7
- Internet Explorer 6.x on Windows XP



See also

[Accessing the SaaS email and web protection portal on page 132](#)

Account activation and setup

To begin using the SaaS email protection service, you must activate your account, then perform some basic configuration tasks.

These tasks are required to use the SaaS email protection service.

- 1 Activate your account.



If you have already activated an account for the SaaS web protection service, you do not need to activate the SaaS email protection service.

- 2 Redirect your MX records and configure the core features you have purchased.
- 3 Configure any additional SaaS email services you have purchased.

Before you can activate your account, your company needs to have its own mail domain, such as yourdomain.com, with a static IP address and a dedicated email server, either in-house or hosted by an ISP.

When your account is ready to activate, an action item appears on the Dashboard page of the SecurityCenter website. Click the button associated with the action item to display activation instructions. A SaaS email protection widget also appears on the Dashboard page with a link to activate your account.

When activation is complete, reporting information appears in the widget along with a link to the SaaS email and web protection portal. You can view additional instructions for configuring your account in one or more welcome kits available on the Utilities page, and you can configure policy options on the portal.

After activation, use these tasks at any time to view and customize the features of the SaaS email protection service:

- 1 Access the SaaS email and web protection portal.
- 2 Customize policy options.
- 3 Check quarantined messages and adjust settings if needed.
- 4 Read encrypted messages and configure delivery options.

Activating and setting up your account

Use this SecurityCenter task to activate your account for the SaaS email protection service, then redirect your MX records and set up the features.

When your account is ready to activate, an action item appears on the Dashboard page of the SecurityCenter.

If you have purchased additional SaaS email services, you should configure them after you activate and configure the core features.



If you have already activated an account for the SaaS web protection service, you do not need to activate the SaaS email protection service.

Task

For option definitions, click ? in the interface.

- 1 On the Dashboard page of the SecurityCenter, click the button for the action item **Your SaaS email protection needs to be activated**.
(If you need to activate the SaaS web protection service too, the action item includes it.)
- 2 Type the required information.
 - **Primary domain name** — The name of the domain you want to protect (for example, yourdomain.com). If you want to protect multiple domains, type only the primary domain here. You will be able to set up additional domains later on the SaaS email and web protection portal.



Customers adding the optional intelligent routing service are required to designate one domain as the organization's public domain. All other domains should be designated as primary domains.

- **Technical contact email address** — The email address where you want McAfee to send technical and support emails for your account.
- 3 Click **Continue**.

- 4 Follow the steps for redirecting your domain's mail exchange (MX) records and configuring core features.
- 5 If you have purchased additional SaaS email services, open the welcome kit for each service and follow the instructions provided.
Links to the welcome kits for the services you have purchased are provided at the top of the page. The instructions are provided in PDF format.
(The SaaS email encryption service does not have a welcome kit. Documentation is available on the SaaS email and web protection portal by clicking the link **Guides for SaaS Email Protection** on the Help page of the SecurityCenter.)



Welcome kits for additional services also contain instructions for setting up the core features of the SaaS email protection service. If you have purchased core protection and one additional service, you can configure both by following the instructions in the optional welcome kit. If you have purchased more than one additional service, you need to open multiple welcome kits, then follow any steps you have not already completed.

Accessing the SaaS email and web protection portal

Use this task to access the SaaS email and web protection portal directly from the SecurityCenter. No separate login credentials are required.

The portal provides tools for configuring administrative features and policy options, checking email statistics and activity, and viewing reports.

Task

For option definitions, click ? in the interface.

- From the SecurityCenter, perform one of these actions.
 - Click the **Dashboard** tab, then select **Click here to configure** in a SaaS email protection widget.
 - Click the **Policies** tab, then select **Configure SaaS Email Protection Policy** from the drop-down menu.
 - Click the **Reports** tab, then select **SaaS Email Protection**.

The SaaS email and web protection portal opens in a separate browser window.

See also

[The SaaS email protection widget and portal on page 129](#)

Configuring policy settings for the SaaS email protection service

Use this task to create a policy or modify policy settings for the SaaS email protection service on the SaaS email and web protection portal.

If you do not customize policy settings, the SaaS email protection service uses default settings for inbound and outbound message filtering and additional services.

Task

For option definitions, click ? in the interface.

- 1 From the SecurityCenter, click the **Policies** tab, then select **Configure SaaS Email Protection Policy** from the drop-down menu.
- 2 On the SaaS email and web protection portal, click the **Email Protection** tab, then click the **Policies** tab.

- 3 Select the policy and settings you want to configure.
 - Click **New** to create a policy.
 - Select a policy from the list, then click **Edit** to modify an existing policy.
- 4 Click **Save**.

Checking quarantined messages

Use this task to view quarantined email detections and ensure they are being filtered appropriately.

Task

For option definitions, click ? in the interface.

- 1 From the SecurityCenter, open the SaaS email and web protection portal.
 - Click the **Dashboard** tab, then select **Click here to configure** in a SaaS email protection widget.
 - Click the **Policies** tab, then select **Configure SaaS Email Protection Policy** from the drop-down menu.
- 2 On the SaaS email and web protection portal, click the **Email Protection** tab, then click the **Policies** tab.
- 3 Select options required to display all quarantined messages.
 - **Threat** — Select **All Threats**.
 - **Day** — Select **All Days**.
 - **Direction** — Select **Inbound**, or select **Inbound and Outbound** if you also use outbound email filtering.
- 4 Click **Search**.
- 5 For each message, check the type of threat, the sender, the recipient, and the subject.
- 6 To view detailed information about a message, hold the cursor over the information displayed in the From column.
- 7 If messages are being quarantined incorrectly, add email addresses to a policy's Allow List or Deny List as needed.

Reading encrypted messages

Use this task to read the content of email messages that have been encrypted by the SaaS email protection service.

Before you begin

Account login credentials are required to access encrypted messages.

When an encrypted message has been sent to a user, the user receives a notification with a link to the message.

Task

- Use one of these methods.
 - Click the link in the notification that an encrypted message has been delivered.
 - If the subscription to SaaS email encryption has not been activated, the link allows you to activate it, then access the message.
 - If the subscription has been activated, the link allows you to access the message in the Pick-up portal.
 - Download the Secure Reader application on the user's client computer, then access the message locally. The Secure Reader application is available from the Pick-up portal. Users can configure how encrypted messages are delivered to them after installing the Secure Reader application.

Reports and statistics for SaaS email protection

View account information tracked by the SaaS email protection service in charts and administrative reports.

- Weekly statistics for email usage and detections, available in the widgets on the Dashboard page of the SecurityCenter.
- Data on email traffic, performance, and detections, available in reports on the portal.

Viewing email activity for the week

Use this task to view statistics on email activity and detections for the last seven days.

Task

For option definitions, click ? in the interface.

- 1 From the SecurityCenter, click the **Dashboard** tab.
- 2 In one of the SaaS email activity widgets, check your email statistics.
- 3 Select the widget's **Click here to configure** link to open the SaaS email and web protection portal, where you can view additional information about the number and types of threats detected.

Viewing reports

Use this task to view reports created for your SaaS email protection service account.

Task

For option definitions, click ? in the interface.

- 1 From the SecurityCenter, click the **Reports** tab, then click **SaaS Email Protection**.
- 2 On the SaaS email and web protection portal, click the **Email Protection** tab, then click the **Reports** tab.
- 3 Select the information to appear in the report.
 - Select a domain, type of report, and time period to display the corresponding report data.
 - Click **Performance Reports** to display a page where you can schedule a recurring weekly or monthly report of performance data to be distributed via email.

Getting more information

Use this task to access detailed instructions for using the features on the SaaS email and web protection portal.

Task

For option definitions, click ? in the interface.

- Select one of these options:
 - On the SecurityCenter, click the **Help** tab, click **Guides for SaaS Email Protection**, then select the appropriate guide.
 - On the SaaS email and web protection portal, click **Help** to display context-sensitive information about the current page.

8

Using the SaaS Web Protection Service

The SaaS web protection service redirects all web traffic through McAfee servers for analysis. Web-based threats and inappropriate content are intercepted before being sent to client computers on your account. Policy options allow you to define inappropriate content and specify the threats to block.

The SaaS web protection service resides outside the network; it requires no system resources, and there's no hardware or software to install. Use the SecurityCenter and the SaaS email and web protection portal to manage web protection features.

Contents

- ▶ *SaaS web protection features*
- ▶ *Multiple layers of protection against web-based threats*
- ▶ *The SaaS web protection widget and portal*
- ▶ *Account activation and setup*
- ▶ *Reports for SaaS web protection*
- ▶ *Getting more information*

SaaS web protection features

SaaS web protection protects client computers from web-based threats encountered while browsing and searching the web. All websites are checked before being delivered to the web browsers on your network. The type of threats and content blocked by the SaaS web protection service depends on the policy options configured for your account.

The SaaS web protection service includes these features:

Real-time scanning — Web content is scanned each time it is accessed; any new threats and updated content are assessed before being blocked or delivered to your network.

Up-to-date scanning criteria — Scanning criteria are updated regularly so that you are always protected against the most current threats.

Simplified management — Centralized, web-based policy management through the SaaS email and web protection portal allows you to configure comprehensive policies for threats and content filtering (for inappropriate words and phrases). You can also view reports about web traffic, statistics, and activity for your account.

Customizable scanning criteria — Policy options allow you to configure which threats and types of content should be blocked. You can allow different types of content for different users and groups of users on your account.

Support for a variety of web browsers — These browsers are supported on client and administrative computers:

- Internet Explorer 8.x on Windows XP, Windows Vista, and Windows 7
- Internet Explorer 7.x on Windows XP and Windows Vista
- Firefox 3.5.x on Windows XP, Windows Vista, and Windows 7
- Internet Explorer 6.x on Windows XP

Multiple layers of protection against web-based threats

Multiple services in McAfee SaaS Endpoint Protection work together to provide computers on your account with complete protection from web-based threats while browsing and searching.

Here's what happens when a client computer requests access to a website.

- 1 The browser protection service analyzes the request and decides whether to allow the request. Policy options that you have configured for your account determine whether the request is allowed or blocked.
For example, if the site has a red SiteAdvisor site safety rating and you have configured policy options to block all red sites, the request is blocked. If you have configured policy options to warn users against possible threats, a warning message is displayed. If the user requests a site that meets the criteria specified in your policies, the request is sent "to the clouds."
- 2 On McAfee servers, the SaaS web protection service analyzes the content and scans it for malware. If the content is safe and meets the criteria specified in your policies, the request is sent back to the network.
For example, if you have configured policy options to block phishing pages or particular types of content, sites that contain that content are blocked. If the site has developed a threat since it was tested and assigned a SiteAdvisor site safety rating, the SaaS web protection service blocks the request based on its analysis of the site's current content.
- 3 Once the request returns to the network, the virus and spyware protection service scans the website content according to the policy options you have configured.
For example, it can scan scripts running on the site or scan a file download. If no threats are found, the request is sent to the client computer's browser.

Each protection service provides an additional barrier between your computers and threats on the web.

See also

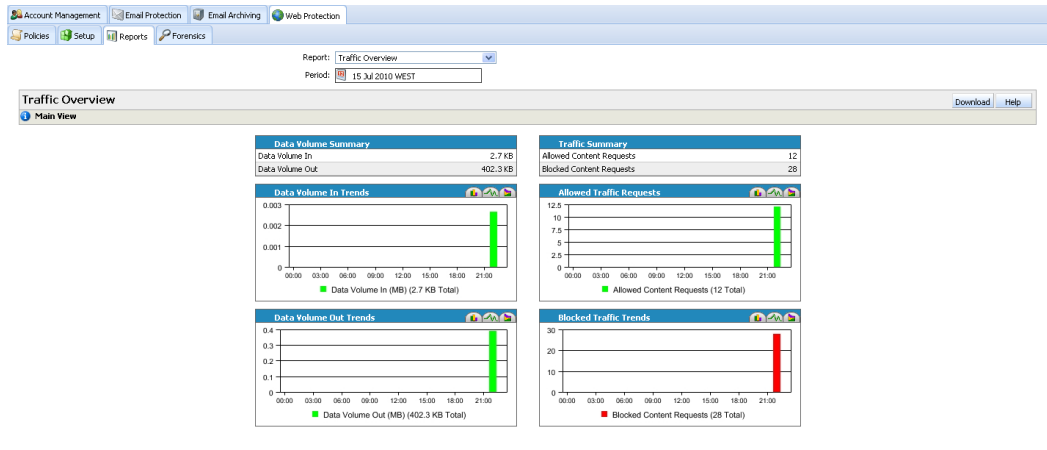
[Configuring policy settings for SaaS web protection](#) on page 141

The SaaS web protection widget and portal

When you purchase a subscription for SaaS web protection, a SaaS web protection widget is displayed on the Dashboard page of the SecurityCenter. The widget contains a link to activate the service. After activation, the link's text changes (**Click here to configure**); use it to access the SaaS email and web protection portal.

Summary data is not available in this widget; you need to click the link to view all reports for SaaS web protection.

The portal provides tools for configuring administrative features and policy options, checking web traffic statistics and activity, and viewing reports.

**See also**

Accessing the SaaS email and web protection portal on page 140

Account activation and setup

To begin using the SaaS web protection service, you must activate your account, then perform some basic configuration tasks.

These tasks are required to use the SaaS web protection service.

1 Activate your account.



If you have already activated an account for the SaaS email protection service, you do not need to activate the SaaS web protection service.

2 Redirect your web traffic.

3 Configure SaaS web protection features.

When your account is ready to activate, an action item appears on the Dashboard page of the SecurityCenter website. Click the button associated with the action item to display activation instructions. A SaaS web protection widget also appears on the Dashboard page with a link to activate your account.

When activation is complete, the widget contains a link to the SaaS email and web protection portal. You can view additional instructions for configuring your account in a welcome kit available on the Utilities page, and you can configure policy options on the portal.

After activation, use these tasks at any time to view and customize the features of the SaaS web protection service:

1 Access the SaaS email and web protection portal.

2 Customize policy options.

Activating and setting up your account

Use this SecurityCenter task to activate your account for the SaaS web protection service, then redirect your web traffic and set up the features.

When your account is ready to activate, an action item appears on the Dashboard page of the SecurityCenter.



If you have already activated an account for the SaaS email protection service, you do not need to activate the SaaS web protection service.

Task

For option definitions, click ? in the interface.

- 1 On the Dashboard page of the SecurityCenter, click the button for the action item **Your SaaS web protection needs to be activated**.
(If you need to activate the SaaS email protection service too, the action item includes it.)
- 2 Type the required information.
 - **Primary domain name** — The name of the domain you want to protect (for example, yourdomain.com). If you want to protect multiple domains, type only the primary domain here. You will be able to set up additional domains later on the SaaS email and web protection portal.



If you do not have a domain, select the checkbox for **I do not have a domain**, then leave this field blank. McAfee will create the necessary settings for you to use the SaaS web protection service, and they will be invisible to you.

- **Technical contact email address** — The email address where you want McAfee to send technical and support emails for your account.
- 3 Click **Continue**.
 - 4 Follow the steps in the activation instructions for configuring features and policy options.

Accessing the SaaS email and web protection portal

Use this task to access the SaaS email and web protection portal directly from the SecurityCenter. No separate login credentials are required.

The portal provides tools for configuring administrative features and policy options, checking web activity, and viewing reports.

Task

For option definitions, click ? in the interface.

- From the SecurityCenter, perform one of these actions.
 - Click the **Dashboard** tab, then select **Click here to configure** in the SaaS web protection widget.
 - Click the **Policies** tab, then click **Configure SaaS Web Protection Policy** from the drop-down menu.
 - Click the **Reports** tab, then click **SaaS Web Protection**.

The SaaS email and web protection portal opens in a separate browser window.

See also

[The SaaS web protection widget and portal on page 138](#)

Configuring policy settings for SaaS web protection

Use this task to create a policy or modify policy settings for the SaaS web protection service on the SaaS email and web protection portal.

Task

For option definitions, click ? in the interface.

- 1 From the SecurityCenter, click the **Policies** tab, then select **Configure SaaS Web Protection Policy** from the drop-down menu.
- 2 On the SaaS email and web protection portal, click the **Web Protection** tab, then click the **Policies** tab.
- 3 Select the policy and settings you want to configure.
 - Click **New** to create a policy.
 - Select a policy from the list, then click **Edit** to modify an existing policy.
- 4 Click **Save**.

See also

[Multiple layers of protection against web-based threats](#) on page 138

Reports for SaaS web protection

View account information tracked by the SaaS web protection service in charts and administrative reports.

From the SaaS email and web protection portal you can view the following:

- Data on web traffic, threat filtering, and allowed and blocked content.
- Specific volume and traffic trends.
- Types and numbers of threats detected.

Viewing reports

Use this task to view reports created for your SaaS web protection service account.

Task

For option definitions, click ? in the interface.

- 1 From the SecurityCenter, click the **Reports** tab, then click **SaaS Web Protection**.
- 2 On the SaaS email and web protection portal, click the **Web Protection** tab, then click the **Reports** tab.
- 3 Select the information to appear in the report.
 - Select a domain, type of report, and time period to display the corresponding report data.
 - Click **Performance Reports** to display a page where you can schedule a recurring weekly or monthly report of performance data to be distributed via email.

Getting more information

Use this task to access detailed instructions for using the features on the SaaS email and web protection portal.

Task

For option definitions, click ? in the interface.

- Select one of these options:
 - On the SecurityCenter, click the **Help** tab, click **Guides for SaaS Web Protection**, then select the appropriate guide.
 - On the SaaS email and web protection portal, click **Help** to display context-sensitive information about the current page.

9

Using the Email Server Protection Service

The email server protection service supplements the email scans performed on client computers by intercepting threats at the email server.

This chapter contains information on installing and using email server protection for Microsoft Exchange servers with McAfee SaaS Endpoint Protection.

The email server protection software is installed on email servers running Microsoft Exchange Server version 2003 or 2007 to protect them from viruses, spam, unwanted content, potentially unwanted programs, and banned file types or messages.

McAfee SaaS Endpoint Protection allows you to view summary information about email server detections in the SecurityCenter. You can also click links in the SecurityCenter to access the management console on the email server, where you can configure policy settings and manage email server protection. (The software must be installed with default options, which include a web-based user interface, to access the console from the SecurityCenter.)

Contents

- ▶ *Email server protection features*
- ▶ *The installation and setup process*
- ▶ *The email server protection widget and management console*
- ▶ *Managing the email server protection service*
- ▶ *Where to find more information*

Email server protection features

Email server protection software includes two basic types of features: those that protect your email servers from a wide variety of threats and those that help you manage the protection features.

Protection features

- **Protects against virus** — Scans all email messages for viruses and protects your Exchange server by intercepting detections and cleaning or deleting them. Uses advanced heuristic methods to identify unknown viruses or suspected virus-like items, then blocks them.
- **Protects against spam** — Assigns a spam score to each email message during scanning, then takes action based on the spam rules you configure.
- **Protects against phishing** — Detects phishing emails that fraudulently try to obtain your personal information.
- **Detects packers and potentially unwanted programs** — Detects packers that compress and encrypt the original code of an executable file. Also detects potentially unwanted programs.
- **Filters content** — Scans the content in each email message's subject line, body, and attachment.

- **Filters files** — Scans an email attachment based on its file name, file type, and file size. Also filters files with encrypted, corrupted, banned, password-protected, and digitally signed content.
- **Scans at scheduled times** — Allows you to schedule regular scan operations to occur at specific times.
- **Scans MIME messages** — Allows you to specify how Multipurpose Internet Mail Extensions (MIME) messages are handled.
- **Detects denial-of-service attacks** — Detects additional requests or attacks flooding and interrupting the regular traffic on a network. A denial-of-service attack overwhelms its target with false connection requests, so that the target ignores legitimate requests.

Management features

- **Management console** — Provides a user-friendly, web-based (if the software is installed with the default options) or standalone interface on the email server, used for configuring features and viewing reports. If the software is installed with the default options, the management console is accessible through links in the SecurityCenter.
- **Policy management** — Allows you to set up policies that determine how different types of threats are treated when detected.
- **Centralized scanner, filter rules, and enhanced alert settings** — Allows you to configure scanner settings that a policy can apply when scanning items. You can set up rules that apply to a file name, file type, and file size. You can use the alert editor to customize the text of an alert message.
- **Quarantine management** — Allows you to specify a local database to be used as a repository for quarantining infected email messages and configure maintenance settings for it. Also allows you to specify McAfee Quarantine Manager 6.0, located on a different server, as a repository for quarantining infected email messages.
- **Allows or prohibits users based on email account** — Supports lists of authorized and prohibited users at the global, group, and user level.
- **Automatic updates** — Checks for and downloads updates to the DAT files and components to ensure protection against the latest threats. You can specify the location for retrieving updates.
- **Detection reports** — Creates status reports and graphical reports that enable you to view information about the detected items.
- **Configuration reports** — Creates configuration reports that contain a summary of product configurations, such as server information, version information, license status and type, product information, debug logging information, on-access settings, on-access policies, and gateway policies. Allows you to specify when a server should send the configuration reports to an administrator or other recipient via email.
- **Customized notification emails and disclaimers** — Allows you to customize the email notification settings and disclaimers for external email messages.

The installation and setup process

Follow these guidelines to install the email server protection software on your Microsoft Exchange servers, configure settings for your account, and access reports on email activity by using the SecurityCenter.

- 1 After purchasing a version of McAfee SaaS Endpoint Protection that includes email server protection, you receive an email message with instructions for installation. The Email Server Protection widget appears on the Dashboard page of the SecurityCenter with a link to download the software. (In some cases, an action item appears, with a button that opens the Install Email Protection page.)
- 2 Clicking one of these links downloads a compressed file that contains the software and documentation. Follow the instructions in the email and the installation wizard to install protection on your email servers. During the process, you are prompted to enter the company key that is included in the email.
- 3 When installation is complete, the protection software sends identification, status, and detection information to the SecurityCenter. This usually takes about 15 minutes, and occurs for each server where the software is installed.
- 4 The next time you log on to the SecurityCenter, the Email Server Protection widget contains detection information sent by the protection software. (Initially, the widget reports that no detections have occurred.)
- 5 Clicking the **View Details** link in the widget displays a report listing identification, status, and detection statistics for each protected email server.
- 6 Protected email servers send data to the SecurityCenter every six hours to update information in the widget and the report.
- 7 In the report, clicking the IP address for an email server opens the management console for the server's protection software in a separate browser window. (This feature requires the software to be installed with the default options, which include a web-based user interface.) Use the console to configure and manage the protection software.

Installing email server protection

Use this SecurityCenter task to download and install email server protection on one or more email servers.

Task

For option definitions, click ? in the interface.

- 1 On the Dashboard page, click **Install Protection**.
- 2 Select **Install email protection**, then click **Next**.
- 3 In the email server protection section, click the URL to download the compressed file containing the software and documentation.

- 4 When prompted, enter your company key.
- 5 Follow the instructions in the email and the installation wizard to install the software on one or more email servers.



To enable access to the email server's management console from the SecurityCenter, you must install the email server protection software with the default options, which include a web-based user interface. Also, the server must be located on the same network as the computer you use to manage McAfee SaaS Endpoint Protection.

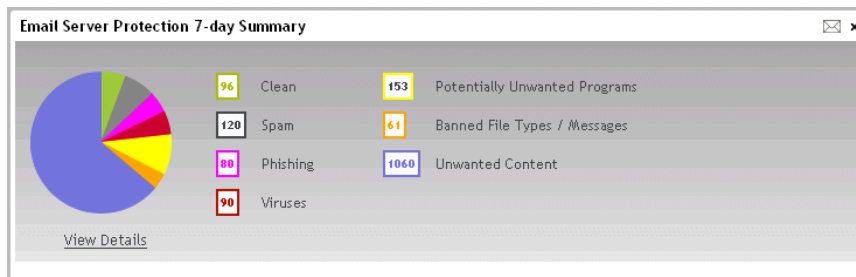
When installation is complete, the email servers send data to the SecurityCenter, and this data appears in the Email Server Protection widget on the Dashboard page. It usually takes about 15 minutes for the data to appear in the widget.

The email server protection widget and management console

When you purchase a subscription to email server protection, an email server protection widget is displayed on the Dashboard page of the SecurityCenter.

The widget reports statistics for email server activity and contains one of these links:

- **Click here to download** — Downloads a compressed file containing the software and documentation for the email server protection service. This link appears if you have not yet downloaded and installed the software.
- **View Details** — Displays a report containing data about the protected email servers on your account. This link appears after you have downloaded and installed the software.



The report includes links to the management console on each email server. The console provides tools for configuring features, checking email statistics and activity, and viewing reports. See the documentation that you downloaded with the software for information on using the management console.



The link is available only when the email server protection software is installed with its default options, which include the web-based user interface, and the email server is on the same network as the computer where you are viewing the report.

The screenshot displays the McAfee Security Service for Exchange dashboard. The main section is titled 'Statistics' and includes a 'Reset' button and a 'Graph' showing detection trends over the last 30 days. The detection data is as follows:

Category	Count	Percentage
Clean	2147	61%
Spam	273	8%
Phish	136	4%
Viruses	0	0%
Potentially Unwanted Programs	0	0%
Banned File types/Messages	2	0%
Unwanted Content	954	27%

Below the statistics, the 'Scanning' section shows an average scan time of 1 millisecond and a total of 3512 items scanned. The 'Versions & Updates' section provides details on the last successful update (Thursday, August 13, 2009 5:30:00 AM) and lists various engine updates, including the Anti-Virus Engine and Anti-Spam Engine. The 'Reports' section includes a table for 'Recently Scanned Items':

Date/Time	Sender	Recipients	Action Taken	Filename	Detection Name	Task
Tuesday, August 18, 2009 10:00 AM	sender@example.org	administrator@MANABM...	Clean			OnAccess (Transp...
Tuesday, August 18, 2009 10:00 AM	sender@example.org	administrator@MANABM...	Clean			OnAccess (Transp...
Monday, August 17, 2009 10:00 AM	SunilAnand@big.com	administrator@manab...	Clean			OnAccess (Transp...
Monday, August 17, 2009 10:00 AM	SunilAnand@big.com	administrator@manab...	Clean			OnAccess (Transp...

Managing the email server protection service

Use these tasks to view activity and status and customize protection features.

The SecurityCenter provides a centralized location for managing all the email servers in your account.

Tasks

- [Checking notifications and action items on page 148](#)
Use this task to check for new information and problems that require action from you.
- [Viewing detection and status information on page 148](#)
Use this task to open the Email Server Protection report, which lists identification, status, and detection summary information for each protected email server in your account.
- [Accessing the management console on the server on page 149](#)
Use this task to access the protection software's web-based management console on the email server, where you can view detailed information, configure protection features, and create reports.

Checking notifications and action items

Use this task to check for new information and problems that require action from you.

Task

For option definitions, click ? in the interface.

- On the Dashboard page of the SecurityCenter, check for action items pertaining to email server protection and take the appropriate action.

Type of Action Item	Description	Resolution
You have one or more alerts.	<p>An alert notifies you when:</p> <ul style="list-style-type: none"> • An email server has not sent protection data to the SecurityCenter in two days. • DAT files on the email server have not been updated in the last three days. • Critical processes are not running on the email server. <p>This type of action item is not dismissible.</p>	<ul style="list-style-type: none"> • Click the button associated with the action item to read about the alerts and how to resolve them.
You need to install software.	<p>This type of action item notifies you when updates are available for the protection software (such as patches and hotfixes).</p> <p>This type of action item is dismissible.</p>	<ul style="list-style-type: none"> • Click the button associated with the action item to open a page with a link to download the software. • Click Dismiss Alert to remove the action item from the Dashboard page without installing software.

Viewing detection and status information

Use this task to open the Email Server Protection report, which lists identification, status, and detection summary information for each protected email server in your account.

Task

For option definitions, click ? in the interface.

- 1 In the SecurityCenter, open the Email Server Protection report by either of these methods:
 - On the Dashboard page, click **View Details** in the email server protection widget.



If the widget is not displayed, click **Add Widget** to display the Dashboard Widget Gallery. Locate the email server protection widget, then click **Add to Dashboard**.

- On the Reports page, click **Email Server Protection**.
- 2 Select the period of time for which you want to view information.
 - 3 Click an email server's IP address to open its management console in a separate browser window. From there, you can view detailed information, configure features, and generate reports for the server. See the email server protection documentation for more information about using the console.



This feature is available only when the email server protection software is installed with the default options, which include a web-based user interface, and the email server is on the same network as the computer where you are viewing the report. Otherwise, manage email server protection by using the standalone user interface on the email server.

Accessing the management console on the server

Use this task to access the protection software's web-based management console on the email server, where you can view detailed information, configure protection features, and create reports.



This feature is available only when the email server protection software is installed with the default options (which include a web-based user interface), and the email server is on the same network as the computer where you are viewing the report. Depending on the level of trust configured for the two machines, you might be required to enter login credentials for the email server protection account.

Task

For option definitions, click ? in the interface.

- 1 From the Email Server Protection report, click the IP address for an email server in the listing.

The server's management console opens in a separate browser window.



Email server protection supports these browsers: Microsoft Internet Explorer 6.0 and 7.0, Mozilla Firefox 2.0, and Netscape Navigator 9.0.

- 2 In the management console, click buttons along the left side to access information:
 - **Dashboard**
 - **Graphical Reports**
 - **Statistics & Information**
 - **Detected Items**
 - **On-demand Scans**
 - **Policy Manager**

- **Status Reports**
- **Settings & Diagnostics**
- **Configuration Reports**

3 For information on using the management console, click **Help** or see the documentation you downloaded with the protection software.

Where to find more information

Documentation for email security protection is included with the software that you download:

- User guide
- Release notes (readme.txt file)
- Online help (available by clicking Help in the management console)

It is installed on the email server along with the software. Refer to these documents for information on installing, configuring, and managing email server protection.

10 Using the SaaS Vulnerability Scanning Service

The SaaS vulnerability scanning service measures the security of websites, domains, and IP addresses by testing them for thousands of risks and issues in many vulnerability classes and categories. It then reports any vulnerabilities detected, prioritizes the risks they present, and recommends remediation tasks and patches.

Contents

- ▶ *Vulnerability scanning features*
- ▶ *Certification programs*
- ▶ *The SaaS vulnerability scanning widget and portal*
- ▶ *Overview of scanning process*
- ▶ *Overview of the certification process*
- ▶ *Types of devices to scan*
- ▶ *Types of scans*
- ▶ *Managing scan devices*
- ▶ *Performing scans*
- ▶ *How detections are reported*
- ▶ *Viewing scan results*

Vulnerability scanning features

Run vulnerability scans (device audits) to locate and resolve security risks in your network devices and to confirm compliance with certification standards.

A security plan that includes regular and comprehensive device audits:

- Protects your entire network infrastructure non-invasively.
- Identifies unauthorized server applications and tracks system configuration changes.
- Looks for thousands of different vulnerabilities residing in Internet services, shopping carts, ports, operating systems, servers, key applications, firewalls, addressable switches, load balancers, and routers.
- Provides detailed reporting and specific recommendations for resolving vulnerabilities detected by more than 10,000 individual vulnerability tests plus port scans.
- Collects and updates vulnerability data around-the-clock from hundreds of sources worldwide, ensuring its ability to detect the latest risks.
- Meets the website security vulnerabilities audit requirements mandated by HIPAA, GRAMM-LEACH-BILEY, SARBANES-OXLEY, and other federal legislation.

- Complies with credit card issuers by meeting the vulnerability scanning requirements of the Payment Card Industry (PCI) data security standard.
- Provides advanced web application scanning and finds BlindSQL and Server-side Include vulnerabilities with 99% accuracy.

Types of vulnerabilities detected

The SaaS vulnerability scanning service tests for all vulnerabilities in the following general categories:

- Backdoors, Remote Controls, and Trojan Horse Programs
- CGI and Form Processing Vulnerabilities (including SQL Injection)
- Default Passwords
- All Database Servers
- All Microsoft Versions
- UNIX and Linux
- Email Services
- News and Chat Services
- Remote Administration Access
- Remote Database Access
- Remote File Access
- TCP Ports
- RPC
- SMB/NetBIOS
- ICMP
- HTTP XSS
- SNMP
- SNTP
- UDP
- FTP and Telnet
- XML Services
- Routers and Load Balancers
- Firewalls and Addressable Switches

Certification programs

The SaaS vulnerability scanning service provides optional certification programs to ensure that your website meets the highest standards for security.

PCI certification program

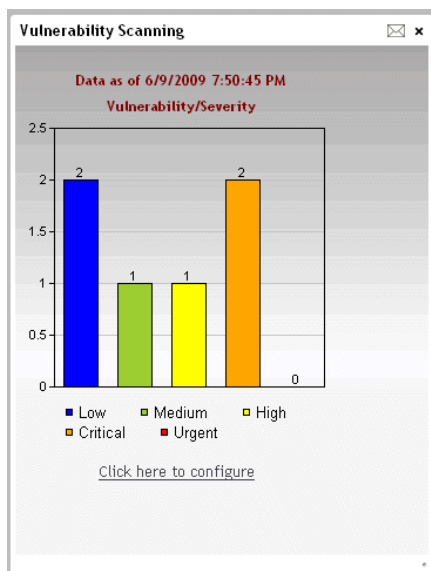
Ensures that your website always complies with the Payment Card Industry Data Security Standard (PCI DSS) by providing the tools needed to complete the PCI certification process, remain in compliance, and create quarterly validation reports.

McAfee® SECURE™ Trustmark certification program

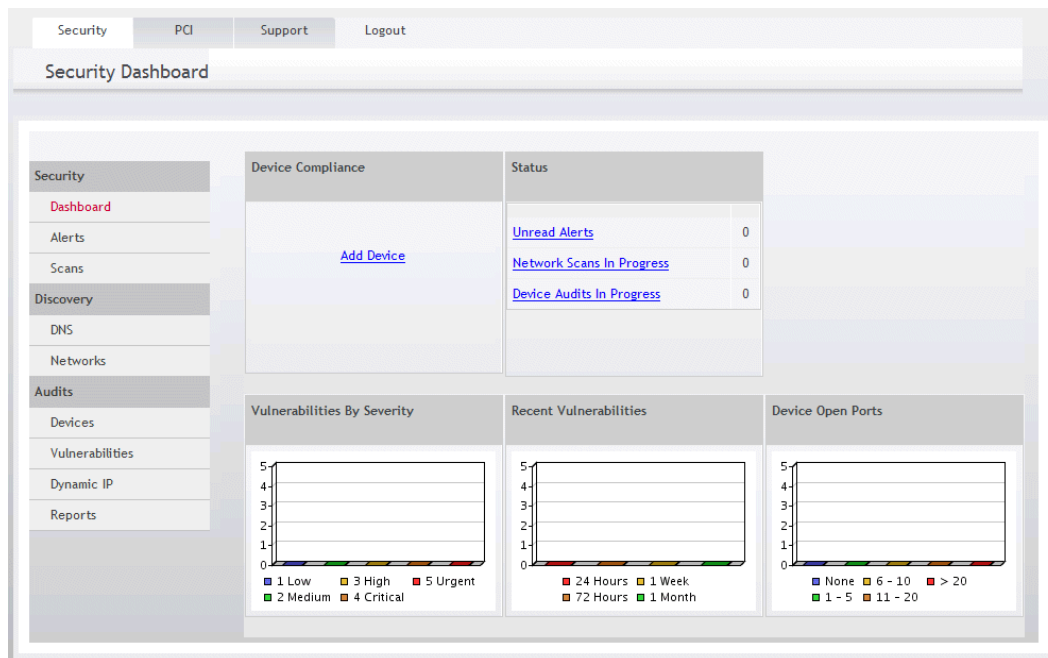
Adds the McAfee SECURE trustmark to your website as proof that it meets the rigorous certification requirements for compliance with the McAfee SECURE data security standard. This program requires daily scanning of your McAfee SECURE devices.

The SaaS vulnerability scanning widget and portal

When you purchase a subscription for the SaaS vulnerability scanning service, the SaaS Vulnerability Scanning/PCI Certification widget is displayed on the Dashboard page of the SecurityCenter. The widget contains a link ([Click here to configure](#)) to the SaaS vulnerability scanning portal.



The portal provides tools for adding the IP addresses to scan, performing scans, checking scan results, and accessing historical data for scans. If you subscribe to a certification program, access tools and reports for certification on the portal.



Accessing the SaaS vulnerability scanning portal

Use this task to access the SaaS vulnerability scanning portal, which provides tools for managing network security and certification.

Task

- 1 On the Dashboard page of the SecurityCenter, in the SaaS Vulnerability Scanning/PCI Certification widget, select **Click here to configure**.

The SaaS vulnerability scanning portal opens in a separate browser window.



If the widget is not displayed, click **Add Widget** to display the Dashboard Widget Gallery. Locate the SaaS Vulnerability Scanning/PCI Certification widget, then click **Add to Dashboard**.

- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
 - View status and alerts for devices and scans.
 - View discovery results, or add domains and networks for scanning.
 - Configure and perform scans.
 - Access scan results for information about detected vulnerabilities and remediation options.
- 3 Click **Logout** to close the portal and return to the SecurityCenter.

Overview of scanning process

This is the high-level process for configuring vulnerability scans for your network.

- 1 Log on to the SaaS vulnerability scanning portal.
- 2 Specify what to scan by one of these methods:
 - If you know which IP addresses to scan — Add one or more IP addresses.
 - If you do not know which IP addresses to scan — Add a domain, then run a discovery scan to identify the active IP addresses.

IP addresses (and ranges of IP addresses comprising networks) are called *devices* in the vulnerability scanning portal.

- 3 Configure the devices you want to scan.
This includes selecting the type of device, which determines the standard used for scanning.
- 4 Configure the devices to accept the IP addresses (maintained by McAfee) where vulnerability scans originate.
- 5 Create groups where devices can be placed. (*Optional*)
- 6 Configure and initiate scans manually, or schedule them to occur at a later time.
If your subscription includes certification, scans are required at specific intervals. Check the requirements for your subscription.
- 7 View results of the scans and suggested remediation tasks (if vulnerabilities were found).
Optionally, generate customized reports and schedule remediation tasks.

Overview of the certification process

This is the high-level process for maintaining compliance with certification standards for your network.

PCI certification

To maintain compliance with the PCI certification standards:

- 1 Take the self-assessment questionnaire.
This is available on the **PCI** tab of the SaaS vulnerability scanning portal. It helps you identify the tools used by your website to process customer payment data.
- 2 Add devices to scan and configure scanning options.
For Service Level, select **Devices PCI**. The Scan Frequency defaults to **Quarterly**, per the requirements for certification. You can also perform on-demand scans as needed.
- 3 View results of the scans and suggested remediation tasks (if vulnerabilities were found).
Results and instructions for obtaining documentation to certify your compliance are provided on the portal.

McAfee SECURE Trustmark

To maintain compliance with the standards for McAfee SECURE trustmark:

- 1 Take the self-assessment questionnaire. (*Recommended*)
This is available on the **PCI** tab of the SaaS vulnerability scanning portal. It helps you identify the tools used by your website to process secure information.
- 2 Add devices to scan and configure scanning options.
For Service Level, select **Devices McAfee SECURE**. The Scan Frequency defaults to **Daily**, per the requirements for certification. You can schedule additional scans as needed.
- 3 Copy the trustmark code and place it on your website.
The code and instructions for using it are available on the portal.
- 4 View results of the scans and suggested remediation tasks (if vulnerabilities were found).
Results and instructions for obtaining documentation to certify your compliance are provided on the portal.

If severe vulnerabilities are not resolved within 72 hours, the trustmark code becomes invisible on your site and an action item is displayed on the SecurityCenter. When the vulnerabilities are resolved and the site is scanned successfully, then the trustmark code becomes visible on your site again.

Types of devices to scan

Scans target two types of network components.

- **Device** — A single host, IP address, or domain name.
- **Network** — A range of IP addresses.

These scan targets are called *devices* on the SaaS vulnerability scanning portal. Before running scans, you must add each device you want to scan to your account on the SaaS vulnerability scanning portal. If you are unsure of the IP addresses to add, you can add a domain name and run a discovery scan to identify the IP addresses.

To ensure scans that are thorough in scope, we recommend adding your domain name as a device. If you have purchased a single domain license, you are entitled to scan all IP addresses in that domain. To scan multiple IP addresses in separate domains, you must purchase additional licenses.

About active devices

We recommend scanning all *active devices*. Active devices are those that are involved in, or connected to networks involved in, collecting, transmitting, processing, or storing sensitive information.



Compliance with the PCI certification standard requires that you scan all active devices.

Examples of active devices you should scan are:

- **Filtering devices** — These include firewalls or external routers that are used to filter traffic. If using a firewall or router to establish a DMZ (a buffer zone between the outside public Internet and the private network), these devices must be scanned for vulnerabilities.
- **Web servers** — These allow Internet users to view web pages and interact with your websites. Because these servers are fully accessible from the public Internet, scanning for vulnerabilities is critical.

- **Application servers** — These act as the interface between the web server and the back-end databases and legacy systems. Hackers exploit vulnerabilities in these servers and their scripts to get access to internal databases that could potentially store private data. Some website configurations do not include application servers; the web server itself is configured to act in an application server capacity.
- **Domain name servers (DNS)** — These resolve Internet addresses by translating domain names into IP addresses. Merchants or service providers might use their own DNS server or a DNS service provided by their ISP. If DNS servers are vulnerable, hackers can potentially spoof a merchant or service provider web page and collect private information.
- **Email servers** — These typically exist in the DMZ and can be vulnerable to hacker attacks. They are a critical element to maintaining overall website security.
- **Load balancers** — These increase the performance and the availability of an environment by spreading the traffic load across multiple physical servers. If your environment uses a load balancer, you should scan all individual servers behind the load balancer.

Types of scans

There are two basic types of scans.

- **Discovery scans** — Identify which devices to scan:
 - DNS Discovery identifies active IP addresses within a domain.
 - Network Discovery identifies active IP addresses and open ports within a network.
- **Device audits** — Examine a single host, IP address, or domain name for open ports and vulnerabilities.

Scanning standards

Vulnerability scans are based on these standards:

- **PCI standard** — Complies with credit card issuers by meeting the vulnerability scanning requirements of the Payment Card Industry (PCI) data security standard (DSS). Devices that process payment card information must be scanned and show compliance with this standard quarterly. Used for the PCI certification program.
- **McAfee SECURE standard** — Meets the website security vulnerabilities audit requirements mandated by HIPAA, GRAMM-LEACH-BILEY, SARBANES-OXLEY, and other federal legislation. Used for the McAfee SECURE trustmark certification program.

Severity levels for vulnerabilities

Vulnerabilities can be assigned different levels of severity by the different standards. Because of this, it is possible for devices to be compliant with the McAfee SECURE standard but not the PCI standard, which has specific requirements developed for devices that process payment card data.

Security level	Description
5 (Urgent)	Provide intruders with remote root or remote administrator capabilities. By exploiting these types of vulnerabilities, hackers can compromise the entire host. This category includes vulnerabilities that provide hackers full file-system read and write capabilities, and the ability for remote execution of commands as a root or administrator user. The presence of backdoors and Trojans also qualifies as an urgent vulnerability.
4 (Critical)	Provide intruders with remote user capabilities, but not remote administrator or root user capabilities. Critical vulnerabilities give hackers partial access to file systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information also qualify as critical vulnerabilities
3 (High)	Provide hackers with access to specific information stored on the host, including security settings. These vulnerabilities could result in potential misuse of the host by intruders. Examples include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services (such as mail relaying).
2 (Medium)	Expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host.
1 (Low)	Informational, such as open ports.

Manual and scheduled scans

You can run scans on demand (they are queued and completed within 24 hours of the time you configure them) or schedule them to occur daily, weekly, or monthly. Manual scans are available to test vulnerabilities identified in a previous scan that you have taken steps to resolve. These include non-invasive and "full exploit" scans.

If your subscription includes a certification program, you must comply with the scan frequency requirements of the program.

Managing scan devices

Use these tasks to set up and manage the devices on which you want to run vulnerability scans.

Tasks

- [Discovering IP addresses in a domain on page 159](#)
The DNS Discovery tool identifies active IP addresses associated with a domain.
- [Discovering IP addresses in a network on page 159](#)
The network discovery tool identifies which IP addresses within a network (a specified range of IP addresses) are active.
- [Adding devices to scan on page 160](#)
Use this task to add devices you want to scan. Devices can be IP addresses, domains, or networks that you want to scan.
- [Configuring devices to accept scans on page 161](#)
Use this task to configure devices to accept communications from the IP addresses where vulnerability scans originate.
- [Creating device groups on page 161](#)
Optionally, use this task to create groups and add devices to a group.
- [Changing device groups on page 162](#)
If you have already assigned devices to groups, use this task to move devices in and out of existing groups.
- [Deleting devices on page 162](#)
Use this task to delete devices from your account.

Discovering IP addresses in a domain

The DNS Discovery tool identifies active IP addresses associated with a domain.

Use this task to identify the IP addresses that you need to scan.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Discovery, select **DNS**.
- 4 On the DNS Discovery page, select an action.

If you want to...	Do this...
Add a domain to run discovery on	Under Add a Domain for DNS Discovery , type a domain name, select the checkbox to agree to the terms, and click Add .
Run a discovery scan (if you have already added a domain)	If no date appears in the Last Scanned column, select Not Scanned Yet , select options for the scan, then click Confirm .
View results of a discovery scan (if you have already run one)	If a date appears in the Last Scanned column, select the domain name to display results of the last discovery scan.
Delete a domain that you added	Click the red X in the right column of the Domain table.

Discovering IP addresses in a network

The network discovery tool identifies which IP addresses within a network (a specified range of IP addresses) are active.

Use this task to identify the active IP addresses you need to scan within a range of IP addresses.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Discovery, select **Networks**.
- 4 On the Discovery page, select an action:

If you want to...	Do this...
Add a network or subnet	Click Add Network , enter the name you would like to use and the IP address information, then click Add . Follow the approval instructions to complete the add process.
View detailed information for a network (if you have already added one)	Select the IP address to display information for. Then select Overview , Scans , History , or Configure to access specific types of information.
View reports	At the top of the page, select Reports , then specify options for the report you want to view.

Adding devices to scan

Use this task to add devices you want to scan. Devices can be IP addresses, domains, or networks that you want to scan.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Audits, select **Devices**.
- 4 On the top portion of the page, click **Add Device**.
- 5 On the Add Device page, select an option for Service Level.
This specifies the type of device and which set of standards the scans will be based on.

Select this option...	For scans that...
Devices McAfee SECURE	Meet the website security vulnerabilities audit requirements mandated by HIPAA, GRAMM-LEACH-BILEY, SARBANES-OXLEY, and other federal legislation. Select this option if your subscription includes trustmark certification.
Devices PCI	Comply with credit card issuers by meeting the vulnerability scanning requirements of the Payment Card Industry (PCI) data security standard. Select this option if you are scanning devices involved with processing credit card information, or if your subscription includes PCI certification.

- 6 Type a domain name or IP address.
For domain names, "http://" is not required, but "www" is required if applicable.
For example, to add the domain name http://www.mydomain.com, enter www.mydomain.com.

- 7 Select how often you want scans to occur.

Select this option...	When you want to...
OnDemand	Run scans manually whenever you want them. Either service level supports this option.
Daily	Run scans every day. The Devices McAfee SECURE service level supports this option.
Weekly	Run scans once a week. The Devices McAfee SECURE service level supports this option.
Monthly	Run scans once a month. The Devices McAfee SECURE service level supports this option.
Quarterly	Have McAfee perform a scan for each device every three months. The Devices PCI service level supports this option.

- 8 Click **Continue**, select both acknowledgment checkboxes, then click **Add Device**.
- 9 In the Scan Approval list, select the IP addresses or domain names for which you want to approve scans, select both checkboxes under Terms of Service, enter the characters displayed in the Verification area, then click **Activate**.

If you selected **OnDemand** in step 7, no scan is performed for the devices you have just added until you initiate one. If you selected a different option, McAfee begins a scan within 24 hours and notifies you by email when it is complete.

Configuring devices to accept scans

Use this task to configure devices to accept communications from the IP addresses where vulnerability scans originate.

This enables scans to be performed on devices that are protected by intrusion prevention methods such as a hardware or software firewall.



If you receive an incomplete scan error message, the mostly likely cause is that the IP address originating the scan was blocked. Use this procedure to resolve the error, or talk to your IT administrator.

Task

- Obtain the list of IP addresses from one of these sources:
 - Check the most current listing at <https://www.mcafeesecure.com/help/ScanIps.sa> (accessible from the SaaS vulnerability scanning portal).
 - Sign up for the RSS feed at <http://www.mcafeesecure.com/help/ScanIps.rss>.
- Follow the instructions provided in the documentation for your intrusion prevention method, or give this list to your IT administrator.

Creating device groups

Optionally, use this task to create groups and add devices to a group.

If your account contains a lot of devices, you can organize them into groups to manage them more easily. Assign devices to groups based on type, business function, geographic location, or any criteria that is meaningful to you. Groups can be used to drive audit schedules, alerting, remediation activities, and reporting.



To place all devices that meet specific criteria into a group, click the **Use Wizard** button at the bottom of the Add Device Group page.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Audits, select **Devices**.
- 4 On the Devices page, select the checkbox next to one or more device names, then at the bottom of the page, in the Perform on Checked drop-down list, select **Add To New Group**.
- 5 On the Device Groups page, click **Add Group**.
- 6 On the Add Device Group page, type a name for the group.
- 7 Under Devices In Group:
 - Select a device from the Not In Group list, then click **Add** to add the device to the group.
 - Select a device from the In Group list, then click **Remove** to remove the device from the group.
- 8 Under Users With Access, repeat step 6.
- 9 Click **Save** to create the group and display the Device Groups page.

The new group appears in the list.

Changing device groups

If you have already assigned devices to groups, use this task to move devices in and out of existing groups.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Audits, select **Devices**.
- 4 On the Device Groups page, for the group you want to reconfigure, click the Configure Group icon on the right side of the group table.
- 5 Under Devices In Group:
 - Select a device from the Not In Group list, then click **Add** to add the device to the group.
 - Select a device from the In Group list, then click **Remove** to remove the device from the group.
- 6 Click **Save** to return to the Device Groups page.
- 7 Repeat steps 3-5 for each group you want to reconfigure.

Deleting devices

Use this task to delete devices from your account.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Audits, select **Devices**.
- 4 Select a device using one of these methods:
 - On the Devices page, click the device name.
 - On the Device Groups page, click the name of the group containing the device, then on the Devices page, click the device name.A page listing details about the selected device is displayed.
- 5 Click **Configure**, then click the **Delete** tab.
- 6 Enter the reason for deleting the device, select the checkbox to acknowledge that you understand what happens when a device is deleted, then click **Request**.
It takes about an hour for the device to be deleted from your account.



Deleting a device permanently deletes all related security data including vulnerability reports. This data cannot be restored.

Performing scans

Use these tasks to set up and run vulnerability scans on devices you have added to your account.

Tasks

- [Starting a scan on page 163](#)
Use this task to set up a vulnerability scan to run in the next 24 hours for an IP address, domain, or network.
- [Scheduling scans for devices on page 164](#)
Use this task to configure scans to be performed once or on a recurring basis.

Starting a scan

Use this task to set up a vulnerability scan to run in the next 24 hours for an IP address, domain, or network.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Security, select **Scans**.

- 4 From the Security Scans page, click **On Demand**.
For each type of scan, the devices you have added to your account are listed.
 - IP addresses are listed under Audit. (You can filter the listing by selecting a group from the top drop-down list.)
 - Networks are listed under Port Discovery.
 - Domains are listed under DNS Discovery.
- 5 Select the devices to scan in a single category, then select **Next**.



You can set up only one type of scan at a time. Click the **Next** button that appears directly under the device listing to continue setting up that type of scan.

- 6 If you are configuring an audit, select the type of audit from the drop-down list.
 - **Hack Simulation** — Runs the standard device audit.
 - **Denial of Service** — Adds extra tests.
 - **Retest Current** — Runs the last test that ran previously. Use this to retest and verify that vulnerabilities previously reported have been resolved.



Selecting Denial of Service adds tests that might bring down a server. We recommend selecting this option during times when users are not accessing network resources.

- 7 Select a date and time for the scan, then click **Confirm**.

Scheduling scans for devices

Use this task to configure scans to be performed once or on a recurring basis.



You cannot select specific times for scans to be performed. In general, scans run at various random times on different devices. To minimize impact on network traffic, scans are not run on multiple devices at the same time.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Audits, click **Devices**.
- 4 Select a device using one of these methods:
 - On the Devices page, click the device name.
 - On the Device Groups page, click the name of the group containing the device, then on the Devices page, click the device name. (This page appears if you have set up device groups.)
 A page listing details about the selected device is displayed.
- 5 Click **Configure**.
- 6 If you are configuring a Device Audit, for **Audit Period** on the **General** tab, select an entry from the drop-down list.
Options are **OnDemand**, **Daily**, **Weekly**, **Monthly**, and **Quarterly**.

- 7 Select other options as needed.
- 8 Click **Save**.

How detections are reported

After scanning is completed, detailed server fingerprints, open ports, and vulnerability data are available on the SaaS vulnerability scanning portal.

When audit scans discover vulnerabilities, you receive an email alert (if you have configured this option) directing you to visit the portal. There you can view scan results, detailed patch recommendations applicable to your specific system configuration, historical audit data, and printable audit reports.

To access scan results, click the **Security** tab to display the Security Dashboard page.

This type of report	Shows
Audit Report	Results for audit scans run on IP addresses. To view: Under Audits, select Reports , select the type of report and the devices to include, then click View HTML . (A PDF version is also available.)
Change Report	Results for network discovery scans, including comparison to the previous scan. To view: Under Discovery, select Networks , then select Reports .
DNS Discovery Scan Result	Results for DNS discovery scans of domains. To view: Under Discovery, select DNS , select a domain that has been scanned, then select links within the report to display details.
Security Alerts	All vulnerabilities in your account detected by all types of scans. To view: Under Security, select Alerts , then select links in the listing to display details.
Security Scans	All scans set up for your account. To view: Under Security, select Scans , then select any device name to display details.
Vulnerabilities	All vulnerabilities detected on IP addresses and domains, sorted by severity rating. To view: Under Audits, select Vulnerabilities , then select the name of a vulnerability to display details about it and options for remediation.

Viewing scan results

Use these tasks to view the results of vulnerability scans.

Tasks


- [Viewing results for audit scans on page 166](#)
Use this task to view the results of audit scans performed on IP addresses and domains in your account.
- [Viewing results for DNS discovery on domains on page 166](#)
Use this task to view the scan status for domains in your account and the results of DNS discovery scans performed on those domains.
- [Viewing results for network discovery scans on page 167](#)
Use this task to view the discovery status for networks in your account and the results of discovery scans performed.

Viewing results for audit scans

Use this task to view the results of audit scans performed on IP addresses and domains in your account.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Audits, select the type of results you want to view.

Select this option	To view these results
Vulnerabilities	<p>A listing of all vulnerabilities detected for IP addresses and domains, sorted by severity rating. Select the name of a vulnerability to display details about the vulnerability and options for resolving it.</p> <p>Vulnerabilities are categorized on a five-point scale (one is low and five is critical). This enables you to prioritize the issues that need to be resolved and schedule remediation resources effectively.</p>
Dynamic IP	<p>A listing of vulnerabilities detected on network devices that do not have a domain name or permanent IP address. Select the name of a vulnerability to display details about the vulnerability and options for resolving it.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  This option appears only if you have added a dynamic IP address to your account. </div>
Reports	<p>A listing of options and devices for which reports are available. Select the type of report and the devices to report on, then click View HTML to display a detailed report. You can also view a report in PDF format, view archived reports, or export report data for viewing in other applications.</p>

Viewing results for DNS discovery on domains

Use this task to view the scan status for domains in your account and the results of DNS discovery scans performed on those domains.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.

- 3 Under Discovery, select **DNS**.
The DNS Discovery page lists the domains in your account and their scan status.
- 4 Select an option.
 - If data is listed for the last discovery scan, click a domain name to display the results of the last scan. Then select links in the results to display details.
 - If no discovery scan data is listed, click **Not Scanned Yet** to set up a scan for the domain.
 - To specify a new domain for a discovery scan, type the domain name under Add Domain for DNS Discovery, then click **Add**.
- 5 If the results for the last discovery scan show that one or more devices in the domain are not being audited, to add them click **Continue** at the bottom of the page under Provision Devices Not Currently Auditing.
- 6 On the Add Devices page, select options adding the devices for scanning.

Viewing results for network discovery scans

Use this task to view the discovery status for networks in your account and the results of discovery scans performed.

Task

- 1 Open the SaaS vulnerability scanning portal (click the link in the SaaS Vulnerability Scanning/PCI Certification widget on the Dashboard page of the SecurityCenter).
- 2 In the portal, click the **Security** tab to display the Security Dashboard page.
- 3 Under Discovery, select **Networks**.
The Discovery page lists the networks in your account and their scan status.
- 4 Select an option.

Select this option	To view these results
By Network	A listing of all networks in your account. Select a network to display details about it.
By Port	A listing of network ports in your account. Select a port to display details about it.
Reports	A listing of networks for which results of discovery scans are available. Select the type of report and the networks to report on, then click View to display a report comparing the results of the latest scan with the previous scan.

11 Troubleshooting

For help installing, using, and maintaining the product, refer to frequently asked questions or specific error messages and their solutions.

Contents

- *Frequently asked questions*
- *Error messages*

Frequently asked questions

Here are answers to frequently asked questions.

Questions about the client software

Is it okay to delete the Temp folder in my program's directory structure?

No. Updates might fail if the Temp folder does not exist. If you delete the folder inadvertently, restart the computer to re-create the folder automatically, or manually create a Temp folder in the Program Files\McAfee\Managed VirusScan folder.

I use Microsoft Windows XP Service Pack 2, and I get a message that my computer may be at risk. What does this mean?

This is a known problem with Microsoft Security Center, because it cannot determine that the client software is installed and up-to-date. If you get this message when starting your computer, click the message balloon to open the Recommendation window, select **I have an antivirus program that I'll monitor myself**, then click **OK**.

Can computers using proxy servers receive updates?

If client computers are connected to the Internet by a proxy server, you might need to provide additional information for updates to work properly. Authentication support is limited to anonymous authentication or Windows domain challenge/response authentication. Basic authentication is not supported. Automatic updates do not occur when a CHAP or NTML proxy is set up in Internet Explorer.

Questions about adding, renewing, and moving licenses

Can I move a license from one computer to another?

Yes. You can uninstall the client software from one computer and install it on a new computer without affecting the total number of licenses you are using. The old computer is automatically subtracted from your total license count on the product accounting system, and the new one added, so that your license number remains constant. To do this:

- 1 Uninstall the software from the old computer.
- 2 From the SecurityCenter, click the **Computers** tab.

- 3 For **Groups**, select **All**, then select the old computer in the listing and click **Delete**.
- 4 Install the software on the new computer.

The new computer appears in your reports after it uploads its status to the SecurityCenter. This usually takes about 20 minutes after installation.

My computer crashed and I had to reinstall the operating system and start over. Will this affect my license number?

No. The old computer is automatically subtracted from your total license count on the product accounting system, and the new one is added when you reinstall the client software. Your license number remains constant.

The new computer appears in your reports after it uploads its status to the SecurityCenter. This usually takes about 20 minutes after installation.

Questions about reporting

Why don't some of my computers show up on my reports?

If your company added more licenses, or upgraded from a trial to a full subscription, some computers might not appear in your reports.

If you upgraded or purchased additional protection using a new email address, you received a new company key and URL for a new account instead of adding licenses to your existing account. (The company key appears after the characters CK= in the URL. It also appears on the **Accounts & Keys** tab of the **My Account** page on the SecurityCenter.) Because you have two company keys, reports appear in two places. Make sure all your trial users reinstall with the installation URL associated with the new key. If you do need to merge multiple accounts, then use the **Manage Accounts** section of the **Accounts & Keys** tab.

Why do my cloned systems all report as the same computer?

The client software generates a unique system identifier when it is installed. If a drive is imaged after the software was installed, all the cloned systems have the same system identifier. To avoid this problem, the client software must be installed after the new systems are restarted. You can do this automatically by using the silent installation method, described in the installation guide.

I just installed McAfee SaaS Endpoint Protection and don't have much information on my SecurityCenter website. Can I view sample reports?

Yes. Sample reports are available at:

<http://www.mcafeesasap.com/MarketingContent/Products/SampleReports.aspx>

Sample reports are useful for new administrators who do not have many users or much detection data and, therefore, cannot view some advanced reporting features.



Sample reports are available in all product languages. Select the language from the **Global Sites** pull-down list in the upper right corner of the page.

Questions about the virus and spyware protection and firewall protection services

How can I prevent popup prompts from appearing when unrecognized programs or Internet applications are detected?

The virus and spyware protection service and the firewall protection service prompt users for a response to a detection when set to Prompt mode. To prevent popups, select Protect or Report mode. For highest protection, select Protect to automatically delete unrecognized programs.

Why would I want to specify excluded files and folders or approved programs?

Specifying excluded files and folders from scanning can be useful if you know a particular type of file is not vulnerable to attack, or a particular folder is safe. If you use a program to conduct your business, adding it to a list of approved programs keeps it from being detected as unrecognized and deleted. If you are unsure, it is best not to specify exclusions.

Can I add approved programs and allowed Internet applications to the McAfee Default policy?

No. However, you can create a new policy and add them. When you click **Add Policy** on the Policies page of the SecurityCenter, the new policy is prepopulated with the McAfee Default policy settings. Specify a name for the new policy, save it, and then add approved programs as needed. You can also designate the new policy as your default policy.

I blocked Internet Explorer on a client computer, and then temporarily disabled the firewall protection service. When I re-enabled it, why was Internet Explorer no longer blocked?

The firewall protection service uses Internet Explorer to update product components. Whenever you enable firewall protection, Internet Explorer is given full access to check for updates.

Questions about the browser protection service and web filtering

Can I run browser protection for Internet Explorer and Firefox on the same computer?

Yes. Browser protection for Internet Explorer and Firefox are compatible on the same computer. You can install protection for both browsers. (If both browsers are present on a computer when the browser protection service is installed, protection for both browsers is installed automatically.)

If Microsoft Internet Explorer is the only browser installed on a client computer when browser protection is installed, does the browser protection service need to be reinstalled after installing Mozilla Firefox?

No. The browser protection client software detects Firefox when it is installed and immediately begins to protect searching and browsing activities in that browser, while continuing to provide protection for Internet Explorer.

How does the browser protection service define a website visit? Does it track individual website pages viewed?

When a client computer visits a website, the browser protection service tracks the site's *domain specifier*. The domain specifier is the smallest amount of information required to uniquely identify the site being rated for security. For example, if a client computer visited 10 different pages on this website over the course of a single browser session:

www.mcafee.com

only a single visit would be logged to this domain:

.mcafee.com

That is the information required to locate a safety rating. A single browser session times out after 30 minutes, and a new session is then tracked.

Why is the SiteAdvisor button gray?

Several causes are possible:

- The site is not rated. Visit the www.siteadvisor.com website to submit a website for testing.
- The client software for the browser protection service is disabled. Click the arrow on the menu button to display the SiteAdvisor menu, then select **Enable SiteAdvisor**. (If the browser protection service is already enabled, the menu option changes to **Disable SiteAdvisor**. These menu options appear only if the policy assigned to the computer permits them.)
- The site is on your local intranet. The browser protection service does not report information about intranet sites to the server maintained by McAfee where site safety ratings are stored.

- Proxy server settings are configured incorrectly. Authentication support is limited to anonymous authentication or Windows domain challenge/response authentication. Basic authentication is not supported.
- The client computer is not communicating with the server maintained by McAfee where site safety ratings are stored. A communication error icon (disconnected cables) appears on the SiteAdvisor button. Hold your cursor over the menu button to display the safety balloon, then click **Troubleshooting** to test the connection.

Questions about the SaaS email protection service

After installing the SaaS email protection service, why am I not receiving email or seeing any charts on the SaaS email and web protection portal?

Check to ensure you have updated your MX records to route email messages through McAfee servers. Instructions are provided in your welcome kit.

Why are messages with inappropriate content not being blocked?

If you are using the default policies, you must enable content filtering before these messages will be blocked.

Questions about the SaaS vulnerability scanning service

To what does a single license entitle me?

A single license entitles you to perform audits on one IP address. It does not affect the number of discovery scans you can run.

What is difference between a domain and a device?

Device means computer hardware, network, storage, input/output, or electronic control devices, or software installed on such devices.

Domain means the systems accessible by the Internet that facilitate, provide, or describe services. This is often a website.

Can a domain name resolve to multiple IP addresses?

Yes. Domain names can resolve to multiple IP addresses, and each IP address will be scanned as a separate device.

How much bandwidth does an audit scan use?

On average, an audit scan uses 10 MB of bandwidth at a peak and creates a load equal to between 1 and 5 visitors.

The bandwidth usage can vary greatly depending on the number and kind of open services.

How long does scanning take?

The entire scanning process takes up to 24 hours because scans are put into a queue and performed on a first-come-first-served basis, and because multiple scans are involved. In addition, the duration of each device audit scan can vary greatly based on the characteristics of the scan target.

- **Phase 1: Port Scan.** Port scans discover all ports that are open for communication. The duration of port scan depends mostly on the type of firewall used on the target. A firewall that **rejects** packets to closed or filtered ports can be scanned quickly. A firewall that **drops** packets to closed or filtered ports can take much longer.
 - Typical: Less than 5 minutes
- **Phase 2: Network Scan.** Network scans discover all the open ports and subnets. The duration of the network scan depends mostly on the number of open ports found and the types of services found on those ports.
 - Typical: Less than 20 minutes
 - Average: 40 minutes
 - Maximum: 3 hours
- **Phase 3: Web Application Scan.** Web application scans find all the web pages. The duration of the web application scan depends mostly on the number of web pages on the site.
 - Typical: Less than 20-40 minutes
 - Average: 1 hour
 - Maximum: 4 hours

How long does a discovery scan take?

The duration of a discovery scan depends primarily on the size of the subnet and the type of firewall the IP addresses in the subnet are using.

- A firewall that **rejects** packets to closed or filtered ports will take less time.
- A firewall that **drops** packets to closed or filtered ports will take more time.
- An IP address that is not configured on any device is typically treated like a firewall that drops packets.
- A Class C subnet that **drops** packets on average takes 12 hours.

What is the difference between PCI scans and McAfee®SECURE™ scans?

The scanning process for PCI and McAfee®SECURE™ is the same. They differ in the severity levels they assign to vulnerabilities. For example, if a vulnerability is discovered and assigned a severity level of 2 by the McAfee®SECURE™ standard, that device is considered McAfee®SECURE™ compliant. If the vulnerability is assigned a severity level of 3 by the PCI standard, it is not compliant with the PCI Data Security Standard. The PCI Data Security Standard requires that you demonstrate compliance quarterly.

What does Advanced network discovery scanning do?

Advanced network discovery technology reduces the difficulty in managing the security of large public IP networks. It allows you to quickly discover, identify, and monitor large numbers of network devices, or find rogue devices and unauthorized services across any specified IP subnet range.



The PCI Data Security Standard requires that all active devices discovered within any IP ranges allocated to your company be included in your list of devices undergoing full vulnerability scanning.

Does Dynamic IP scanning perform a vulnerability audit on network devices?

Yes. Dynamic IP scanning is used to perform a vulnerability audit on network devices that do not have a domain name (URL) or static (permanent) IP address. These include networked office computers, computers used as point-of-sale payment terminals, and office, home, or mobile computers using DSL, ISDN, Cable, or dial-up Internet connections.

Why am I able to add the same dynamic IP multiple times?

The SaaS vulnerability scanning portal allows you to enter the same IP addresses for on-demand scans. Each time you add it, it will be scanned only once.

Error messages

Error messages are displayed by programs when an unexpected condition occurs that can't be fixed by the program itself. Use this list to find an error message, an explanation of the condition, and any action you can take to correct it.

Client software

Unable to connect to update server. Failed to connect to server for updates.

This error can be caused by several problems, but the most common solutions are:

- Check your connection to the network server or Internet.
- Adjust the browser's security level settings to enable Javascript. (For Internet Explorer, the setting should be **Medium** or **Medium-high**.)
- Empty the browser's cache (i.e., delete temporary Internet files). See your browser's documentation for instructions.
- Adjust your corporate firewall or proxy settings.

Update failed.

There are several reasons that updates might fail.

- Check your connection to the network server or Internet.
- When using the Windows fast user switching feature, automatic updates cannot occur when no user is logged on if the computer is a domain controller or local security policies prevent the creation of a pseudo user.
- Automatic updates cannot occur on computers that are behind an authenticating proxy server or on computers where a CHAP or NTLM proxy is set up in Internet Explorer.
- Automatic updates cannot occur where no user is logged on to computers that receive updates through a relay server.
- Updates might fail if the Temp folder does not exist on the client computer. If you delete the folder inadvertently, restart the computer to re-create the folder automatically, or manually create a Temp folder in the Program Files\McAfee\Managed VirusScan folder.

Activate your software.

You have not activated your copy of the product. You cannot receive updates against the latest threats until you activate. To activate, click the product icon in the system tray, then select **Activate**, or select the **Activate** link in a notification dialog box.

Your software is not up-to-date. Please activate to receive the latest update.

You have not activated your copy of the product. You cannot receive updates against the latest threats until you activate. To activate, click the product icon in the system tray, then select **Activate**, or select the **Activate** link in a notification dialog box.

Your subscription has expired. Your trial has expired. Renew your subscription to re-activate your software. Purchase a subscription to re-activate your software.

Your trial or subscription for the product has expired. To resolve the problem, click the product icon in the system tray, then select **Buy** or **Renew your subscription**, or select one of these links in a notification dialog box.

Virus and spyware protection

File does not exist.

This error verifies that the computer is protected from threats. When you clicked to open an infected file from Windows Explorer, the on-access scanner immediately detected and deleted the file, so that Windows could not open it.

On-access scan is currently disabled.

This error can be caused by several problems, but the most common solutions are:

- Check the computer's connection to the network server or Internet.
- This feature has been disabled. From the client computer, log on as an administrator (using the Admin Login feature), then enable it from the console on the client computer.



To prevent this problem, force the computer to re-enable on-access scanning automatically whenever it checks for updates by enabling the associated virus and spyware policy option.

SaaS vulnerability scanning

Incomplete scan.

The most likely cause is that the McAfee IP addresses where scans originate are being blocked by your network's intrusion prevention method, such as a hardware or software firewall. To fix this problem, you must configure the devices you want to scan to accept communications from these IP addresses.

- 1 Check the most current listing of IP addresses at <https://www.mcafeesecure.com/help/ScanIps.sa> (accessible from the SaaS vulnerability scanning portal) or from the RSS feed at <https://www.mcafeesecure.com/help/ScanIps.rss>.
- 2 Follow the instructions provided in the documentation for your intrusion prevention method, or give this list to your IT administrator.

Active Directory

Active Directory user does not have sufficient privileges to perform a remote installation.

The credentials entered for the Active Directory server do not allow you to install software remotely. Check with your IT administrator or contact McAfee customer support for assistance.

Invalid Active Directory credentials were provided.

The credentials entered for the Active Directory server were not valid. Check with your IT administrator or contact McAfee customer support for assistance.

Index

A

- about this guide [9](#)
- access
 - client software [27](#)
- access levels, group administrators [53](#)
- account enrollment key, locating or creating [67](#)
- account, ProtectionPilot, migration [68](#)
- account, SaaS Endpoint Protection
 - keys for [67](#)
 - multiple, merging [68](#)
 - notifications, configuring [65](#)
 - profile information, updating [65](#)
 - subscriptions and licenses, buying and renewing [66](#)
 - subscriptions and licenses, viewing [66](#)
- account, Total Protection Service
 - defined [11](#)
- accounts
 - SaaS web protection, See web protection
- accounts, SaaS email protection, See email protection
- Action menu, client software [29](#)
- Action Required status, Potentially Unwanted Programs Viewer [84](#)
- activation
 - SaaS email protection [131](#)
 - SaaS web protection [140](#)
- Active Directory
 - downloading synchronization utility [51](#)
 - importing groups and computers [51](#)
 - installing client software [51](#)
 - overview [50](#)
 - scheduling synchronization [52](#)
 - support for, overview [48](#)
 - synchronizing network and SecurityCenter [52](#)
 - viewing synchronization details [52](#)
 - viewing tree [53](#)
- ActiveX controls
 - online help and [169](#)
- add
 - allowed Internet applications (firewall protection) [100](#)
 - approved programs (virus and spyware protection) [82](#), [84](#)
 - devices in groups (SaaS vulnerability scanning) [162](#)
 - devices to groups (SaaS vulnerability scanning) [161](#)
 - devices to scan (SaaS vulnerability scanning) [160](#)
 - domains to scan (SaaS vulnerability scanning) [159](#)
- add (*continued*)
 - excluded files and folders (virus and spyware protection) [82](#)
 - group administrators (SecurityCenter) [55](#)
 - groups of client computers (SecurityCenter) [49](#)
 - IP addresses for custom connections (firewall protection) [103](#)
 - licenses and subscriptions (SecurityCenter) [66](#)
 - logo for reports (SecurityCenter) [64](#)
 - networks and subnets to scan (SaaS vulnerability scanning) [159](#)
 - policies (SecurityCenter) [59](#)
 - system service ports for custom connections (firewall protection) [102](#)
 - widgets on Dashboard page (SecurityCenter) [42](#)
- administrative features
 - logging on as administrator (client console) [34](#)
- administrative website, See SecurityCenter website
- administrator
 - group administrators, configuring account information for [55](#)
 - group administrators, overview [53](#)
 - site administrator, configuring account information [65](#)
 - site administrator, defined [11](#)
- allow
 - IP addresses for custom connections [103](#)
 - system service ports for custom connections [102](#)
- allowed Internet applications
 - configuring [100](#)
 - discovering in learn mode [95](#)
 - McAfee recommendations for [100](#)
 - viewing, user-approved [86](#), [106](#)
- allowed Internet applications (firewall protection)
 - viewing and managing [45](#), [46](#)
- applications
 - allowed Internet, See allowed Internet applications
- approved programs (virus and spyware protection)
 - adding to policies [82](#)
 - discovering in learn mode [73](#)
 - managing [84](#)
 - viewing and managing [45](#), [46](#), [82](#), [86](#), [106](#)
- Approved status, Potentially Unwanted Programs Viewer [84](#)
- archives, See compressed files
- archiving, SaaS email protection, See email protection
- authentication, support for [169](#)

- authorized sites (browser protection)
 - configuring [123](#)
 - overview [122](#)
 - safety ratings and [122](#)
 - site patterns [122](#)
- automatic updates
 - email server protection (Microsoft Exchange) and [143](#)
 - exceptions [29](#)
 - overview [29](#)
 - proxy servers and [169](#)
 - relay servers and [29](#)
- Avert Labs
 - defined [14](#)
- B**
- background tasks [169](#)
- balloons, safety information in browser protection [111](#)
- best practices
 - browser protection [126](#)
 - firewall protection [108](#)
 - virus and spyware protection [89](#)
 - web filtering [126](#)
- block
 - client computer updates (SecurityCenter) [45](#)
 - file downloads, by ratings (browser protection) [119](#)
 - Internet applications (firewall protection) [100](#)
 - Internet Explorer (firewall protection) [169](#)
 - IP addresses for custom connections (firewall protection) [103](#)
 - phishing pages (browser protection) [120](#)
 - system service ports for custom connections (firewall protection) [102](#)
 - unknown Internet applications (firewall protection) [94](#)
 - website access (SaaS web protection) [138](#)
 - website access, by content (browser protection) [121](#)
 - website access, by ratings (browser protection) [118](#), [119](#)
 - websites, customizing messages for (browser protection) [124](#)
- browser protection
 - authorized sites, configuring [123](#)
 - authorized sites, overview [122](#)
 - best practices [126](#)
 - blocking file downloads, by ratings [119](#)
 - blocking or warning website access, by content [121](#)
 - blocking or warning website access, by ratings [119](#)
 - blocking phishing pages [120](#)
 - color-coded icons [111](#)
 - color-coded menu [112](#)
 - communication problems [111](#), [112](#)
 - configuring website access, by content [121](#)
 - configuring website access, by ratings [118](#)
 - Content Settings tab [122](#), [123](#)
 - customizing messages for blocked sites [124](#)
 - defined [13](#)
 - enabling and disabling at client computer [117](#)
 - browser protection (*continued*)
 - enabling and disabling at policy level [117](#)
 - Exceptions list, configuring [123](#)
 - Exceptions list, overview [122](#)
 - intranet sites and [112](#)
 - overview [110](#)
 - prohibited sites, configuring [123](#)
 - prohibited sites, overview [122](#)
 - SaaS web protection and [138](#)
 - safety icons [111](#)
 - safety ratings, ignored for authorized sites [122](#)
 - safety reports, overview [113](#)
 - searching websites [111](#)
 - site patterns [122](#)
 - SiteAdvisor menu [112](#), [113](#)
 - tracking Internet usage [115](#), [125](#)
 - viewing browsing activity [125](#)
 - viewing safety balloons and icons [111](#)
 - viewing safety reports [115](#)
 - Web Filtering report [125](#)
 - web filtering, overview [116](#)
 - website visit, defined [169](#)
- browsers
 - browser protection client software and [169](#)
 - non-Microsoft [110](#), [137](#), [169](#)
 - supported for browser protection [110](#)
 - supported for email server protection, Microsoft Exchange [149](#)
 - supported for SaaS web protection [137](#)
 - viewing client computers and [47](#)
- browsing activity on network, viewing [125](#), [141](#)
- browsing of websites (browser protection)
 - protection for [112](#)
 - safety ratings [110](#)
 - tracking in report [125](#)
- browsing of websites (SaaS web protection)
 - protection for [138](#)
 - reports for [141](#)
- buffer overflow protection
 - Detections report and [87](#)
 - on-access scanning and [79](#)
- buy, subscriptions and licenses [66](#)
- C**
- CAB files [19](#)
- cancelled subscriptions, viewing [66](#)
- cannot clean detection [84](#)
- catalog files [19](#)
- certification, overview of process [155](#)
- CHAP proxy [29](#), [169](#)
- clean
 - potentially unwanted programs (virus and spyware protection) [84](#)
 - quarantined detections (virus and spyware protection) [85](#)

- Clean Failed status
 - Potentially Unwanted Programs Viewer [84](#)
 - Quarantine Viewer [85](#)
- client computers
 - Computer Profiles report [47](#)
 - displaying profile of [47](#)
 - Duplicate Computers report [47](#)
 - duplicates, managing [45](#)
 - group ID [47](#)
 - groups, assigning [46](#)
 - groups, managing [49](#)
 - groups, overview [21](#), [48](#)
 - managing in SecurityCenter [45](#), [46](#)
 - managing, overview [43](#)
 - multiple environments, firewall protection and [92](#), [103](#)
 - policies and, overview [56](#)
 - policies, assigning [45](#), [46](#)
 - policies, managing [59](#)
 - scan types, overview [73](#)
 - searching for [45](#)
 - selecting on SecurityCenter pages [39](#)
 - upgrading software [48](#)
- client software
 - access to [27](#)
 - Action menu [29](#)
 - communication problems (browser protection) [111](#)
 - configuring display of client features [35](#)
 - console [29](#)
 - help, displaying [28](#), [29](#)
 - icon [28](#)
 - installing on Active Directory computers [51](#)
 - language configuration [33](#)
 - notifications for operating system support [35](#)
 - operation, illustrated [12](#)
 - overview [17](#)
 - scheduling upgrades [48](#)
 - testing installation of [33](#)
 - uninstalling [35](#)
 - update frequency [31](#)
 - update methods, illustrated [18](#)
 - updates, Internet Independent Updating [19](#)
 - updates, overview [17](#)
 - updates, relay servers and [19](#)
 - updates, Rumor technology [19](#)
 - upgrading [48](#)
 - uploading detection data [17](#), [25](#)
 - viewing product details [34](#)
 - viewing status information for [34](#)
- client-based protection, defined [13](#)
- cloned systems, troubleshooting [169](#)
- close
 - system service ports for custom connections [102](#)
- color coding (browser protection)
 - icons [111](#)
 - menu [112](#)
- communication problems (browser protection) [111](#), [112](#)
- company key
 - locating [67](#)
- compressed files
 - delete failed in [84](#)
- Computer Details page
 - managing computers and [46](#)
 - using [46](#)
- Computers page
 - managing computers and [45](#)
 - overview [43](#)
 - using [45](#)
- configuration (browser protection)
 - authorized sites [123](#)
 - blocking or warning website access, by content [121](#)
 - blocking or warning website access, by ratings [119](#)
 - blocking phishing pages [120](#)
 - customized messages for blocked sites [124](#)
 - enabling and disabling at client computer [117](#)
 - enabling and disabling at policy level [117](#)
 - Exceptions list [123](#)
 - installation via policy [116](#)
 - prohibited sites [123](#)
- configuration (client software)
 - client notifications for operating system support [35](#)
 - display of client software components [27](#), [35](#)
 - language for client software [33](#)
- configuration (email server protection, Microsoft Exchange) [149](#)
- configuration (firewall protection)
 - allowed Internet applications [100](#)
 - connection type [92](#)
 - firewall protection mode [100](#)
 - IP addresses for custom connections [103](#)
 - overview [97](#)
 - Smart Recommendations for Internet applications [100](#)
 - system service ports for custom connections [102](#)
 - tracking blocked events [101](#)
- configuration (SaaS email protection)
 - encrypted email delivery [133](#)
 - MX records [131](#)
 - policies [132](#)
 - quarantine settings [133](#)
- configuration (SaaS vulnerability scanning)
 - device groups [161](#), [162](#)
 - scans [163](#)
- configuration (SaaS web protection)
 - domains [141](#)
 - policies [141](#)
- configuration (SecurityCenter)
 - account correspondence and notifications [65](#)
 - account data for site administrator [65](#)
 - administrator profile information [65](#)
 - group administrators [55](#)
 - groups of client computers [49](#)
 - logo for reports [64](#)

- configuration (SecurityCenter) *(continued)*
 - password for administrator 65
 - policies 59
 - scheduled reports 63
 - status emails 65
- configuration (virus and spyware protection)
 - approved programs 82, 84
 - excluded files and folders 82
 - on-access scans, enabling and disabling 79
 - optional virus scans 80
 - scheduled scans 80
 - spyware protection mode 82
 - spyware protection status 82
 - types of spyware to detect 82
- conflicts with user and administrator settings 99
- connection type
 - configuring 99
 - custom, overview 93
 - overview 92
- console, client software 29
- console, email server protection (Microsoft Exchange) 146, 149
- contact information
 - administrator account, configuring 65
 - group administrators, configuring 55
 - product support 70
- content categories for websites
 - browser protection 121
 - SaaS web protection 137
- continuity, *See* email protection
- conventions and icons used in this guide 9
- cookies
 - Detections report and 87
 - detections, handling 76, 84
 - scanning during on-demand scans 74
- create
 - account enrollment key (SecurityCenter) 67
 - device groups (SaaS vulnerability scanning) 161
 - group administrators (SecurityCenter) 55
 - groups of client computers (SecurityCenter) 49
 - policies (SecurityCenter) 59
- custom connections
 - configuring IP addresses for 103
 - configuring port assignments for 102
 - IP addresses and 95
 - overview 93
 - Prompt mode and 93
 - standard assignments for system service ports 97
 - system service ports and 96
- customization (browser protection)
 - messages for blocked sites 124
- customization (SecurityCenter)
 - listings and reports 39
 - widgets 42
- D**
 - Dashboard page
 - overview 40
 - tasks accessible from 42
 - using 42
 - widgets, using 42
 - DAT files
 - default file types for scans and 80
 - defined 12
 - EXTRA.DAT 29
 - outbreak DAT 29
 - overview 17
 - updates, troubleshooting 169
 - default
 - group, overview 48
 - policy assignments 56
 - policy settings, initial 56
 - policy, changing 59
 - Default Group 48
 - delete
 - approved programs (virus and spyware protection) 82
 - client computers (SecurityCenter) 45
 - devices and device groups (SaaS vulnerability scanning) 162
 - domains to scan (SaaS vulnerability scanning) 159
 - duplicate computers (SecurityCenter) 47
 - excluded files and folders (virus and spyware protection) 82
 - group administrators (SecurityCenter) 55
 - groups of client computers (SecurityCenter) 49
 - IP addresses for custom connections 103
 - logo for reports (SecurityCenter) 64
 - policies (SecurityCenter) 59
 - widgets on Dashboard page (SecurityCenter) 42
 - Delete Failed status, Potentially Unwanted Programs Viewer 84
 - delivery of encrypted email messages 133
 - demos, viewing 70
 - details, view
 - detections (email server protection, Microsoft Exchange) 148
 - detections (virus and spyware protection) 87
 - potentially unwanted programs (virus and spyware protection) 87, 105
 - unrecognized Internet applications (firewall protection) 87, 105
 - detection definition files, *See* DAT files
 - detection history (virus and spyware protection)
 - Detections report 88
 - Detection History report 88
 - detections (email server protection, Microsoft Exchange)
 - types 143
 - viewing 148
 - detections (firewall protection)
 - blocked events 101
 - inbound communications, managing 101
 - inbound communications, overview 92
 - Inbound Events Blocked by Firewall report 106

- detections (firewall protection) (*continued*)
 - Internet applications, managing [100](#)
 - Internet applications, overview [94](#)
 - popup prompts [94](#)
 - recommendations for managing [108](#)
 - viewing report [87](#), [105](#)
 - detections (SaaS email protection)
 - quarantined messages [133](#)
 - reports, viewing [134](#)
 - statistics, viewing [134](#)
 - detections (SaaS web protection)
 - reports, viewing [141](#)
 - detections (virus and spyware protection)
 - cookies [76](#), [84](#)
 - Detections report [87](#)
 - overview [72](#)
 - popup prompts [72](#)
 - potentially unwanted programs [72](#)
 - quarantined items, managing [85](#)
 - recommendations for managing [89](#)
 - registry keys [76](#), [84](#)
 - response to [72](#)
 - spyware, managing [84](#)
 - viewing historical summary [88](#)
 - viewing report [87](#), [105](#)
 - Detections report [87](#)
 - devices (SaaS vulnerability scanning)
 - adding, to scan [160](#)
 - discovering, to scan [159](#)
 - moving to and from groups [162](#)
 - types to scan [156](#)
 - disable
 - browser protection, at client computer [117](#)
 - browser protection, by policy [117](#)
 - firewall protection [104](#)
 - on-access scanning [79](#)
 - spyware protection [82](#)
 - system service ports for custom connections [102](#)
 - updates for non-logged-on users [32](#)
 - Windows firewall [169](#)
 - discovery (SaaS vulnerability scanning)
 - DNS, results [166](#)
 - duration [169](#)
 - network, results [167](#)
 - running, IP addresses in domains [159](#)
 - running, IP addresses in networks [159](#)
 - display
 - client software components [27](#), [35](#)
 - language for client software [33](#)
 - widgets on Dashboard page [42](#)
 - documentation
 - audience for this guide [9](#)
 - client software, troubleshooting display [169](#)
 - email server protection (Microsoft Exchange), viewing [150](#)
 - email server protection, accessing [13](#)
 - documentation (*continued*)
 - product-specific, finding [10](#)
 - SaaS email protection, viewing [135](#)
 - SaaS web protection, viewing [142](#)
 - typographical conventions and icons [9](#)
 - documentation, viewing [70](#)
 - domains
 - configuration (SaaS email protection) [131](#)
 - configuration (SaaS web protection) [140](#)
 - domains, discovery (SaaS vulnerability scanning) [159](#)
 - downloads
 - Active Directory synchronization utility [51](#)
 - email server protection software (Microsoft Exchange) [145](#)
 - tools and utilities [68](#)
 - duplicate computers
 - historical data [45](#)
 - managing [45](#)
 - report [47](#)
- E**
- edit
 - account profile [65](#)
 - IP addresses for custom connections [103](#)
 - MX records [131](#)
 - notification preferences [65](#)
 - password for administrator [65](#)
 - policy settings [59](#)
 - subscription information [66](#)
 - system service ports for custom connections [102](#)
 - EICAR test virus [33](#)
 - email addresses
 - administrator, updating [65](#)
 - client computers, updating [46](#)
 - group administrators, updating [55](#)
 - purchasing subscriptions and [66](#)
 - renewing subscriptions and [66](#)
 - email protection
 - activating [131](#)
 - activity, viewing [134](#)
 - archiving, defined [13](#)
 - archiving, overview [128](#)
 - continuity, defined [13](#)
 - continuity, overview [128](#)
 - defined [13](#)
 - detections, viewing [134](#)
 - documentation, viewing [70](#)
 - documentation, viewing on portal [135](#)
 - domains, configuring [131](#)
 - encrypted email, managing [133](#)
 - encryption, defined [13](#)
 - encryption, overview [128](#)
 - features, core, overview [127](#)
 - features, enhanced, overview [128](#)
 - getting started [130](#)

- email protection (*continued*)
 - intelligent routing, defined [13](#)
 - intelligent routing, overview [128](#)
 - MX records, configuring [131](#)
 - overview [127](#)
 - policies, configuring [132](#)
 - portal, accessing [132](#)
 - portal, illustrated [129](#)
 - quarantined email, managing [133](#)
 - reports, viewing [134](#)
 - setting up [131](#)
 - status, viewing [134](#)
 - troubleshooting [135](#), [169](#)
 - welcome kits [68](#), [131](#)
 - widget, illustrated [129](#)
 - email scans (SaaS email protection) [127](#)
 - email scans (virus and spyware protection)
 - automatic [75](#)
 - from Microsoft Outlook [78](#)
 - on-demand (manual) [78](#)
 - email server protection (Lotus Domino)
 - defined [13](#)
 - documentation, accessing [13](#)
 - email server protection (Microsoft Exchange)
 - action items and notifications [148](#)
 - company key, locating [145](#)
 - defined [13](#)
 - detections, types [143](#)
 - documentation, accessing [150](#)
 - downloading the software [145](#)
 - features [143](#)
 - installation options, default [145](#)
 - installation overview [145](#)
 - installing [145](#)
 - management console, illustrated [146](#)
 - management console, viewing [149](#)
 - report, viewing [148](#)
 - servers sending data to the SecurityCenter [145](#)
 - widget, illustrated [146](#)
 - emails
 - scheduling reports [63](#)
 - sending reports [63](#)
 - sending SecurityCenter pages [39](#)
 - sending to client computer users [39](#)
 - sending to group administrators [55](#)
 - enable
 - browser protection, at client computer [117](#)
 - browser protection, by policy [117](#)
 - firewall protection [104](#)
 - firewall protection via policy [104](#)
 - on-access scanning [79](#)
 - optional virus scans [80](#)
 - scheduled on-demand scans [80](#)
 - spyware protection [82](#)
 - system service ports for custom connections [102](#)
 - encrypted email messages, reading [133](#)
 - error messages
 - icon states for [28](#)
 - events (browser protection)
 - information for reports [115](#)
 - events (firewall protection)
 - overview [92](#)
 - tracking for reports [101](#)
 - viewing [106](#)
 - Exceptions list (browser protection)
 - configuring [123](#)
 - overview [122](#)
 - site patterns and [122](#)
 - exclusions
 - managing (virus and spyware protection) [82](#), [84](#)
 - expiration notifications
 - signing up for [65](#)
 - EXTRA.DAT files [29](#)
- ## F
- fast user switching
 - disabling updates for [29](#)
 - support for [31](#)
 - features, new [15](#)
 - file downloads
 - blocking or warning, by ratings [119](#)
 - filter
 - listings in SecurityCenter [39](#)
 - Firefox
 - blocking file downloads [119](#)
 - browser protection and [110](#)
 - SiteAdvisor menu and [112](#)
 - support for SaaS web protection [137](#)
 - firewall
 - troubleshooting [169](#)
 - Windows 7 [35](#), [169](#)
 - Windows Vista [35](#), [169](#)
 - Windows XP [35](#), [169](#)
 - firewall protection
 - administrator settings and [99](#)
 - allowed Internet applications, configuring [100](#)
 - best practices [108](#)
 - configuring, overview [97](#)
 - conflicts with user and administrator settings [99](#)
 - connection type, configuring [99](#)
 - connection types, overview [92](#)
 - custom connection type, overview [93](#)
 - defined [13](#)
 - enabling and disabling [104](#)
 - events, blocked, tracking [101](#)
 - events, overview [92](#)
 - Inbound Events Blocked by Firewall report [106](#)
 - installing on servers [104](#)
 - installing via policy [104](#)
 - IP addresses, configuring [103](#)

firewall protection (*continued*)

- IP addresses, overview [95](#)
- learn mode [95](#)
- overview [91](#)
- Prompt mode [94](#)
- Protect mode [94](#)
- protecting client computers in multiple environments [92](#), [103](#)
- protection mode, configuring [100](#)
- protection mode, overview [94](#)
- Report mode [94](#)
- reports, overview [107](#)
- response to detections [94](#), [100](#)
- response to events, overview [92](#)
- settings not used [99](#), [169](#)
- Smart Recommendations for Internet applications [100](#)
- system service ports, configuring [102](#)
- system service ports, overview [96](#)
- tracking blocked events [101](#)
- user settings and [99](#)
- user settings for [169](#)
- user/administrator settings and [94](#)

G

group administrators

- access levels [53](#)
- managing, tasks [55](#)
- overview [53](#)

group ID, locating [47](#)

groups

- administrators, managing [55](#)
- administrators, overview [53](#)
- assigning computers [46](#)
- configuring [49](#)
- default [48](#)
- illustrated [21](#)
- managing [49](#)
- overview [21](#), [48](#)

groups (SaaS vulnerability scanning)

- changing devices [162](#)
- creating [161](#)
- deleting [162](#)

groups, Active Directory, See Active Directory

GroupShield, See email server protection

H

help

- client software, displaying [28](#), [29](#)
- client software, troubleshooting display [169](#)
- email server protection (Microsoft Exchange), viewing [150](#)
- SaaS email protection, viewing [135](#)
- SaaS web protection, viewing [142](#)

Help page [70](#)help, viewing [70](#)historical data on detections, viewing [88](#)**I**

icon, McAfee SaaS Endpoint Protection

- defined [28](#)

icons, safety (browser protection) [111](#)import, Active Directory information [51](#)

Inbox

- scanning email (virus and spyware protection) [78](#)

incomplete scan (SaaS vulnerability scanning) [161](#)

installation

- browser protection, via policy [116](#)
- client software on Active Directory computers [51](#)
- email server protection (Microsoft Exchange) [145](#)
- firewall protection, via policy [104](#)
- testing [33](#)
- utilities for, downloading [68](#)

intelligent routing, See email protection

Internet and intranet usage, tracking [115](#)

Internet applications, See allowed Internet applications

Internet Explorer

- blocking [169](#)
- browser protection and [110](#)
- proxy server settings and updates [29](#), [169](#)
- SiteAdvisor menu and [112](#)
- support for SaaS web protection [137](#)
- troubleshooting [169](#)

Internet Independent Updating (IIU)

- overview [19](#)

Internet traffic load, reducing [19](#)intranet sites and browser protection [112](#)

IP addresses

- configuring for custom connections [103](#)
- custom connections and [95](#)
- discovery in domains (SaaS vulnerability scanning) [159](#)
- discovery in networks (SaaS vulnerability scanning) [159](#)
- domains and (SaaS vulnerability scanning) [169](#)
- dynamic (SaaS vulnerability scanning) [169](#)
- overview [95](#)
- protected email servers, viewing [148](#)

IPv4 format [95](#)IPv6 format [95](#)**K**

keys

- account enrollment, locating or creating [67](#)
- company, locating [67](#), [145](#)

L

language selection

- for account correspondence [65](#)
- for blocked website messages [124](#)
- for client software [33](#)

learn mode

- virus and spyware protection [73](#)

learn mode (firewall protection) [95](#)

- licenses
 - moving [169](#)
 - purchasing and renewing [66](#)
 - viewing [66](#)
 - Local Area Network (LAN), reducing Internet traffic [19](#)
 - log on to SecurityCenter
 - from administrative computer [38](#)
 - from client console [34](#)
 - logos, adding or removing from reports [64](#)
- M**
- management
 - Active Directory groups [50](#)
 - client computers (SecurityCenter) [47](#)
 - client computers, all (SecurityCenter) [45](#)
 - client computers, individual (SecurityCenter) [46](#)
 - client computers, overview (SecurityCenter) [43](#)
 - detections (virus and spyware protection) [89](#)
 - email servers (email server protection, Microsoft Exchange) [149](#)
 - encrypted messages (SaaS email protection) [133](#)
 - group administrators (SecurityCenter) [55](#)
 - groups, Active Directory [50](#)
 - groups, overview (SecurityCenter) [48](#)
 - groups, tasks (SecurityCenter) [49](#)
 - Internet applications (firewall protection) [45](#), [46](#), [100](#)
 - policies, overview (SecurityCenter) [56](#)
 - policies, tasks (SecurityCenter) [59](#)
 - potentially unwanted programs (virus and spyware protection) [45](#), [46](#), [84](#)
 - quarantined detections (virus and spyware protection) [85](#)
 - quarantined messages (SaaS email protection) [133](#)
 - suspicious activity (firewall protection) [108](#)
 - manual scans (virus and spyware protection)
 - from client console [77](#)
 - overview [74](#)
 - manual updates [29](#), [32](#)
 - McAfee Default policy [56](#)
 - McAfee SecurityCenter, See SecurityCenter website
 - McAfee ServicePortal, accessing [10](#)
 - memory, scanning [74](#)
 - menu, SiteAdvisor [112](#), [113](#)
 - merge accounts [68](#)
 - messages (browser protection)
 - customizing for blocked sites [124](#)
 - migration, ProtectionPilot account [68](#)
 - modes
 - firewall protection, configuring [100](#)
 - firewall protection, overview [94](#)
 - learn (firewall protection) [95](#)
 - learn (virus and spyware protection) [73](#)
 - Prompt (firewall protection) [94](#)
 - Prompt (virus and spyware protection) [72](#)
 - Protect (firewall protection) [94](#)
 - Protect (virus and spyware protection) [72](#)
 - modes (*continued*)
 - Report (firewall protection) [94](#)
 - Report (virus and spyware protection) [72](#)
 - spyware protection, configuring [82](#)
 - spyware protection, overview [72](#)
 - modification
 - device groups (SaaS vulnerability scanning) [162](#)
 - IP addresses for custom connections (firewall protection) [103](#)
 - system service ports for custom connections (firewall protection) [102](#)
 - move devices in groups (SaaS vulnerability scanning) [162](#)
 - Mozilla Firefox, See Firefox
 - MX records, updating for SaaS email protection [131](#)
 - My Account page [65](#)
- N**
- networks, discovery (SaaS vulnerability scanning) [159](#)
 - new features [15](#)
 - non-logged-on users, disabling updates for [32](#)
 - notifications
 - for operating system support [35](#)
 - language for, selecting [65](#)
 - receipt of encrypted email message [133](#)
 - signing up for [65](#)
 - NTLM proxy [29](#), [169](#)
- O**
- on-access scans (virus and spyware protection)
 - compressed files [80](#)
 - compressed files and, default settings [56](#)
 - enabling and disabling [79](#)
 - overview [74](#)
 - Potentially Unwanted Programs Viewer and [76](#)
 - on-demand scans (virus and spyware protection)
 - compressed files and, default settings [56](#)
 - default policy [74](#)
 - email [78](#)
 - from the client console [77](#)
 - from Windows Explorer [78](#)
 - overview [74](#)
 - Potentially Unwanted Programs Viewer and [76](#)
 - scheduled, overview [74](#)
 - scheduling [80](#)
 - viewing results [84](#)
 - on-demand updates [29](#), [32](#)
 - online help, viewing [70](#)
 - open
 - system service ports for custom connections [102](#)
 - open windows [169](#)
 - operating systems
 - reinstallation [169](#)
 - support notifications for [35](#)
 - viewing client computers and [47](#)

- outbreak DAT files
 - Avert Labs and [14](#)
 - overview [17](#)
 - updating [29](#)
- Outlook Inbox
 - scanning email (virus and spyware protection) [78](#)
- P**
- passwords
 - administrator, for logging on to SecurityCenter [65](#)
 - groups administrators [55](#)
 - retrieving forgotten SecurityCenter password [38](#)
- PCI certification, defined [13](#)
- PCI certification, overview of process [155](#)
- phishing (browser protection)
 - authorized sites and [122](#)
 - blocking phishing pages [120](#)
 - site safety reports and [110](#)
- phishing (SaaS web protection) [138](#)
- policies (browser protection)
 - authorized sites, configuring [123](#)
 - authorized sites, overview [122](#)
 - blocking file downloads, by ratings [119](#)
 - blocking or warning website access, by content [121](#)
 - blocking or warning website access, by ratings [119](#)
 - blocking phishing pages [120](#)
 - configuring website access, by content [121](#)
 - customizing messages for blocked sites [124](#)
 - enabling and disabling at client computer [117](#)
 - enabling and disabling at policy level [117](#)
 - installation via policy [116](#)
 - installing browser protection via policy [116](#)
 - prohibited sites, configuring [123](#)
 - prohibited sites, overview [122](#)
 - site patterns [122](#)
 - web filtering, overview [116](#)
- policies (client settings)
 - display of client software components [27](#), [35](#)
 - update frequency [31](#)
- policies (firewall protection)
 - Administrator configures firewall [99](#)
 - allowed Internet applications, configuring [100](#)
 - allowed Internet applications, overview [94](#)
 - conflicts with user and administrator settings [99](#)
 - connection type, configuring [99](#)
 - connection type, overview [92](#)
 - custom connection, overview [93](#)
 - Firewall Configuration option [104](#)
 - firewall protection mode, configuring [100](#)
 - firewall protection mode, overview [94](#)
 - installing firewall via policy [104](#)
 - IP addresses, configuring [103](#)
 - protection mode, overview [94](#)
 - Smart Recommendations for Internet applications [100](#)
 - policies (firewall protection) (*continued*)
 - system service ports, configuring [102](#)
 - tracking blocked events [101](#)
 - User configures firewall [99](#)
 - user/administrator settings and [94](#)
 - policies (general)
 - assigning to computers [45](#), [46](#)
 - configuring [59](#)
 - default settings and assignments [56](#)
 - default settings, changing [59](#)
 - illustrated [23](#)
 - managing [59](#)
 - McAfee Default [56](#)
 - overview [23](#), [56](#)
 - policies (SaaS email protection)
 - configuring [132](#)
 - quarantine settings [133](#)
 - policies (SaaS web protection), configuration [141](#)
 - policies (virus and spyware protection)
 - advanced spyware protection options [82](#)
 - approved programs [72](#), [82](#)
 - excluded files and folders [82](#)
 - on-access scans, enabling and disabling [79](#)
 - on-demand scans, scheduling [80](#)
 - optional virus scans [80](#)
 - protection mode [72](#)
 - spyware protection mode [82](#)
 - spyware types to detect [82](#)
- Policies page
 - managing policies and [59](#)
 - overview [56](#)
 - using [59](#)
- policy installation (browser protection) [116](#)
- policy installation (firewall protection) [104](#)
- popup prompts
 - preventing (firewall protection) [94](#), [169](#)
 - preventing (virus and spyware protection) [72](#)
 - troubleshooting (firewall protection) [169](#)
 - when they appear (firewall protection) [94](#)
 - when they appear (virus and spyware protection) [72](#)
- popups, See popup prompts
- popups (browser protection)
 - browsers and safety ratings [110](#)
- portal (SaaS email and web protection)
 - accessing [132](#), [140](#)
 - documentation, viewing [135](#), [142](#)
 - illustrated [129](#), [138](#)
- portal (SaaS vulnerability scanning)
 - accessing [154](#)
 - illustrated [153](#)
- ports, See system service ports
- potentially unwanted programs
 - Detections report and [87](#)
 - managing [84](#)
 - response to [72](#)

- potentially unwanted programs
 - (continued)
 - viewing [84](#)
 - Potentially Unwanted Programs Viewer
 - clearing or retaining detections [76](#)
 - managing detections [84](#)
 - preferences, notification [65](#)
 - prevention
 - popup prompts (firewall protection) [94](#), [169](#)
 - popup prompts (virus and spyware protection) [72](#)
 - user approval for programs (firewall protection) [94](#)
 - privacy concerns, browser protection [115](#), [169](#)
 - product support, contacting [70](#)
 - profile
 - account, configuring [65](#)
 - client computers, viewing [47](#)
 - programs
 - viewing unrecognized [87](#), [105](#)
 - prohibited sites (browser protection)
 - configuring [123](#)
 - overview [122](#)
 - safety ratings and [122](#)
 - site patterns [122](#)
 - Prompt mode
 - custom connections and (firewall protection) [93](#)
 - firewall protection [94](#)
 - user/administrator settings and (firewall protection) [94](#)
 - virus and spyware protection [72](#)
 - prompts, See popup prompts
 - Protect mode
 - firewall protection [94](#)
 - virus and spyware protection [72](#)
 - protection mode
 - firewall protection, configuring [100](#)
 - firewall protection, overview [94](#)
 - spyware protection, configuring [82](#)
 - spyware protection, overview [72](#)
 - ProtectionPilot migration utility, downloading [68](#)
 - proxy servers
 - CHAP or NTML [29](#)
 - updates and [169](#)
 - purchase, subscriptions and licenses [66](#)
- Q**
- Quarantine Viewer, using [85](#)
 - quarantined detections
 - managing (virus and spyware protection) [85](#)
 - quarantined email
 - SaaS email protection [133](#)
 - Quarantined status, Potentially Unwanted Programs Viewer [84](#)
- R**
- ratings, safety
 - browser protection and [110](#)
 - Read & Modify Reports access level, group administrators [53](#)
 - Read Only access level, group administrators [53](#)
 - read, encrypted email messages [133](#)
 - recommendations
 - client computers in multiple environments [92](#), [103](#)
 - Internet applications, using McAfee recommendations [100](#)
 - recommended practices
 - browser protection [126](#)
 - firewall protection [108](#)
 - virus and spyware protection [89](#)
 - web filtering [126](#)
 - registration, See activation
 - registry keys
 - detections, handling [84](#)
 - scanning during on-demand scans [74](#)
 - reinstallation
 - operating systems [169](#)
 - relay servers
 - automatic updates and [29](#)
 - overview [19](#)
 - upgrading software [48](#)
 - viewing in reports [60](#)
 - removal
 - devices and device groups (SaaS vulnerability scanning) [162](#)
 - devices in groups (SaaS vulnerability scanning) [162](#)
 - duplicate computers (SecurityCenter) [47](#)
 - excluded files and folders (virus and spyware protection) [82](#)
 - group administrators (SecurityCenter) [55](#)
 - groups of client computers (SecurityCenter) [49](#)
 - IP addresses for custom connections (firewall protection) [103](#)
 - logo for reports (SecurityCenter) [64](#)
 - policies (SecurityCenter) [59](#)
 - system service ports for custom connections (firewall protection) [102](#)
 - widgets on Dashboard page (SecurityCenter) [42](#)
 - renewal, subscriptions and licenses [66](#)
 - Report mode
 - firewall protection [94](#)
 - virus and spyware protection [72](#)
 - reports (browser protection)
 - information sent to SecurityCenter [115](#)
 - information sent to SiteAdvisor website [115](#)
 - viewing site safety reports [115](#)
 - Web Filtering [125](#)
 - website safety, content details [113](#)
 - website safety, overview [110](#)
 - reports (firewall protection)
 - Inbound Events Blocked by Firewall [106](#)
 - overview [107](#)
 - Unrecognized Programs [87](#), [105](#)
 - reports (general)
 - Computer Profiles [47](#)
 - customizing data in [39](#)
 - deleting duplicate computers in [47](#)
 - Duplicate Computers [47](#)

- reports (general) (*continued*)
 - emailing [63](#)
 - filtering or sorting data in [39](#)
 - logo, adding or removing [64](#)
 - overview [25](#)
 - overview of types [60](#)
 - samples of [169](#)
 - saving old data in [169](#)
 - scheduling [63](#)
 - troubleshooting [169](#)
 - reports (SaaS email protection), viewing [134](#)
 - reports (SaaS vulnerability scanning)
 - overview [165](#)
 - viewing, audit scans [166](#)
 - viewing, DNS discovery [166](#)
 - viewing, network discovery [167](#)
 - reports (SaaS web protection), viewing [141](#)
 - reports (virus and spyware protection)
 - Detection History [88](#)
 - Detections [87](#)
 - overview [89](#)
 - Scan Statistics [84](#)
 - Unrecognized Programs [87](#), [105](#)
 - Reports page [60](#)
 - reports, viewing (email server protection (Microsoft Exchange)) [148](#)
 - Rescan, Quarantine Viewer option [85](#)
 - restore
 - quarantined detections (virus and spyware protection) [85](#)
 - Restore, Quarantine Viewer option [85](#)
 - results
 - Active Directory synchronization [52](#)
 - audit scans (SaaS vulnerability scanning) [166](#)
 - DNS discovery (SaaS vulnerability scanning) [166](#)
 - network discovery (SaaS vulnerability scanning) [167](#)
 - on-demand scans (virus and spyware protection) [84](#)
 - spyware scans (virus and spyware protection) [84](#)
 - routing, intelligent, See email protection
 - Rumor technology [19](#)
- S**
- SaaS email protection, See email protection
 - SaaS protection, defined [13](#)
 - SaaS vulnerability scanning, See vulnerability scanning
 - SaaS web protection, See web protection
 - safety balloons and icons [111](#)
 - safety ratings
 - authorized sites and [122](#)
 - browser protection and [110](#)
 - configuring website access and [118](#)
 - file downloads and [119](#)
 - how website ratings are derived [110](#)
 - safety reports, See reports (browser protection)
 - Scan Now feature [74](#), [78](#)
 - Scan Statistics report [84](#)
 - scans (SaaS vulnerability scanning)
 - bandwidth [169](#)
 - configuring [163](#)
 - discovering IP addresses in a domain [159](#)
 - discovering IP addresses in a network [159](#)
 - duration [169](#)
 - dynamic IP addresses [169](#)
 - incomplete [161](#)
 - network scan [169](#)
 - overview [155](#)
 - port scan [169](#)
 - results, viewing [166](#), [167](#)
 - scheduling for devices [164](#)
 - selecting frequency [160](#)
 - types [157](#), [169](#)
 - web application scan [169](#)
 - scans (virus and spyware protection)
 - email, See email scans (virus and spyware protection)
 - automatic [74](#)
 - compressed files [80](#)
 - compressed files and [56](#)
 - default settings for [56](#)
 - excluding files and folders [82](#)
 - manual, default policy [74](#)
 - manual, overview [74](#)
 - on-access, configuring advanced options [80](#)
 - on-access, enabling and disabling [79](#)
 - on-access, overview [74](#)
 - on-demand, default policy [74](#)
 - on-demand, from the client console [77](#)
 - on-demand, from Windows Explorer [78](#)
 - on-demand, overview [74](#)
 - on-demand, results [84](#)
 - on-demand, scheduled, overview [74](#)
 - on-demand, scheduled, viewing [78](#)
 - on-demand, scheduling [80](#)
 - Outlook Inbox [78](#)
 - spyware, configuring [82](#)
 - spyware, overview [76](#)
 - types, overview [73](#)
 - scans, SaaS email protection [127](#)
 - schedule, Active Directory synchronization [52](#)
 - schedule, on-demand scans
 - configuring (virus and spyware protection) [80](#)
 - overview (virus and spyware protection) [74](#)
 - schedule, upgrades to client software [48](#)
 - schedule, vulnerability scans and audits [164](#)
 - scheduled reports [63](#)
 - search engines and browser protection [111](#)
 - searching of websites (browser protection)
 - protection for [111](#)
 - safety ratings [110](#)
 - tracking in report [125](#)
 - searching of websites (SaaS web protection)
 - protection for [138](#)

- searching of websites (SaaS web protection)
 - (continued)
 - reports for [141](#)
 - security settings, See policies
 - security strategy, recommended
 - browser protection [126](#)
 - firewall protection [108](#)
 - virus and spyware protection [89](#)
 - web filtering [126](#)
 - SecurityCenter
 - defined [11](#)
 - SecurityCenter website
 - action items [39](#)
 - Computers page, overview [43](#)
 - Dashboard page, overview [40](#)
 - Dashboard page, using [42](#)
 - emailing pages [39](#)
 - filtering data in [39](#)
 - Help page [70](#)
 - importing Active Directory information [51](#)
 - logging on, from administrative computer [38](#)
 - logging on, from client console [34](#)
 - My Account page [65](#)
 - operation, illustrated [12](#)
 - overview [20](#)
 - page controls, overview [39](#)
 - Policies page, overview [56](#)
 - Policies page, using [59](#)
 - printing pages [39](#)
 - Reports page, overview [60](#)
 - saving pages [39](#)
 - selecting computers in listings [39](#)
 - sorting data in [39](#)
 - tabs, overview [37](#)
 - Utilities page [68](#)
 - widgets, using [42](#)
 - send email
 - to client computer users [39](#)
 - to group administrators [55](#)
 - with attached report [63](#)
 - with attached SecurityCenter data [39](#)
 - server-based protection, defined [13](#)
 - servers
 - email (Lotus Domino), See email server protection (Lotus Domino)
 - email (Microsoft Exchange), See email server protection (Microsoft Exchange)
 - installing firewall protection on [104](#)
 - service ports, See system service ports
 - ServicePortal, finding product documentation [10](#)
 - settings, client
 - administrator settings and (firewall protection) [99](#)
 - display of client software components [27](#)
 - menu buttons and (browser protection) [112](#)
 - severity levels (SaaS vulnerability scanning) [157](#)
 - site patterns, browser protection [122](#)
 - SiteAdvisor menu [112](#), [113](#)
 - SiteAdvisor toolbar, displaying [112](#)
 - Smart Recommendations [100](#)
 - sort
 - listings in SecurityCenter [39](#)
 - spyware protection
 - advanced options [82](#)
 - approved programs [82](#)
 - detections, viewing [84](#)
 - enabling and disabling [82](#)
 - protection mode, configuring [82](#)
 - protection mode, defined [72](#)
 - response to detections [72](#), [76](#), [82](#)
 - status
 - icon and [28](#)
 - status emails
 - signing up for [65](#)
 - subscriptions
 - purchasing and renewing [66](#)
 - trial, starting [42](#), [66](#)
 - viewing [66](#)
 - support, contacting [70](#)
 - synchronization (Active Directory)
 - scheduling [52](#), [68](#)
 - utility, downloading [51](#), [68](#)
 - viewing details [52](#)
 - system service ports
 - configuring [102](#)
 - custom connections and [96](#)
 - overview [96](#)
 - standard assignments for [97](#)
 - system services, See system service ports
- T**
- tabs in SecurityCenter, overview [37](#)
 - tasks
 - running in background [169](#)
 - technical support, contacting [70](#)
 - Technical Support, finding product information [10](#)
 - terminal servers
 - disabling updates for [29](#)
 - support for [31](#)
 - test for communication problems (browser protection) [111](#)
 - test for virus protection feature [33](#)
 - threat detection definition files, See DAT files
 - threats
 - browsers and safety ratings (browser protection) [110](#)
 - SaaS web protection and [138](#)
 - toolbar, SiteAdvisor, displaying [112](#)
 - tree view, Active Directory [53](#)
 - trial subscriptions, starting [42](#), [66](#)
 - troubleshooting [161](#)
 - troubleshooting (browser protection)
 - communication problems [111](#)

- troubleshooting (client software)
 - online help [169](#)
 - proxy servers and updates [169](#)
 - updates [169](#)
- troubleshooting (email server protection, Microsoft Exchange)
 - requirements for opening management console [149](#)
- troubleshooting (firewall protection)
 - firewall, Windows [169](#)
 - Internet Explorer [169](#)
 - popup prompts [169](#)
- troubleshooting (general)
 - cloned systems [169](#)
 - computers missing from reports [169](#)
 - licenses, adding, moving, and renewing [169](#)
 - reports [169](#)
- troubleshooting (virus and spyware protection)
 - popup prompts [169](#)
 - windows open, not visible [169](#)
- Trusted network connection type [92](#)
- trustmark certification, overview of process [155](#)
- trustmark, defined [13](#)
- types of protection, overview [13](#)

U

- Uninstall utility, downloading [68](#)
- uninstallation utilities, downloading [68](#)
- unknown Internet applications (firewall protection)
 - how detections are handled [94](#)
 - managing detections [100](#)
- unrecognized programs
 - See also potentially unwanted programs
 - how detections are handled [72](#)
- unrecognized programs (firewall protection)
 - how detections are handled [94](#)
 - managing detections [100](#)
- Unrecognized Programs report
 - learn mode and [73](#), [95](#)
 - viewing [87](#), [105](#)
- Untrusted network connection type [92](#)
- update
 - account data for site administrator [65](#)
 - MX records [131](#)
- updates
 - automatic [29](#)
 - CHAP or NTML proxy and [29](#), [169](#)
 - content of updates [17](#)
 - disabling, for non-logged-on users [32](#)
 - fast user switching and [29](#)
 - frequency [31](#)
 - Internet Independent Updating [19](#)
 - methods, illustrated [18](#)
 - non-logged-on users and [29](#)
 - on-demand (manual) [29](#), [32](#)
 - overview of [29](#)

- updates (*continued*)
 - proxy servers and [29](#), [169](#)
 - relay servers and [19](#)
 - Rumor technology [19](#)
 - Temp folder and [169](#)
 - troubleshooting [169](#)
 - uploading detection data [17](#), [25](#)
 - uploading email server data [145](#)
- upgrades, client software [48](#)
- upgrades, Windows operating system [169](#)
- user-approved programs, See approved programs
- Utilities page [68](#)

V

- view
 - SiteAdvisor toolbar [112](#)
- view (Active Directory)
 - synchronization results [52](#)
 - tree structure [53](#)
- view (browser protection)
 - browsing activity [125](#)
 - safety balloons [111](#)
 - safety reports [111](#)
 - SiteAdvisor menu [113](#)
 - SiteAdvisor toolbar [112](#)
 - troubleshooting wizard [111](#)
 - Web Filtering report [125](#)
 - website safety reports [115](#)
 - website visits [125](#)
- view (client software)
 - client software components [35](#)
 - client software console [29](#)
 - date of last update [34](#)
 - version [34](#)
- view (email server protection, Microsoft Exchange)
 - detections [148](#)
 - management console [149](#)
 - management user interface [148](#)
 - report [148](#)
- view (firewall protection)
 - blocked events [101](#)
 - detections, Internet applications [100](#)
 - inbound events on network [106](#)
 - unrecognized programs detected on network computers [87](#), [105](#)
 - Unrecognized Programs report [87](#), [105](#)
 - user-approved applications [86](#), [106](#)
- view (SaaS email protection)
 - activity [134](#)
 - encrypted messages [133](#)
 - portal [132](#)
 - reports [134](#)
 - status [134](#)
- view (SaaS vulnerability scanning)
 - results, audit scans [166](#)

- view (SaaS vulnerability scanning)
 - (*continued*)
 - results, discovery scans for domains [159](#)
 - results, discovery scans for networks [159](#)
 - results, DNS discovery [166](#)
 - results, network discovery [167](#)
- view (SaaS web protection)
 - portal [140](#)
 - reports [141](#)
- view (SecurityCenter)
 - blocked website visits [46](#)
 - cancelled subscriptions [66](#)
 - client computer profiles [47](#)
 - client computers, individual [46](#)
 - client computers, list [43](#), [45](#)
 - computers in a group [49](#)
 - demos [70](#)
 - documentation [70](#)
 - duplicate computers [47](#)
 - group administrators [55](#)
 - groups, all [48](#)
 - help, online [70](#)
 - policies [59](#)
 - policies, all [56](#)
 - protection status [42](#)
 - subscription information [66](#)
 - user-approved applications [45](#), [46](#), [86](#), [106](#)
- view (virus and spyware protection)
 - cookie detections [84](#)
 - detection history on network computers [88](#)
 - Detection History report [88](#)
 - detections on network computers [87](#)
 - Detections report [87](#)
 - on-demand scans, results [84](#)
 - potentially unwanted programs [84](#)
 - quarantined detections [85](#)
 - registry key detections [84](#)
 - results, on-demand email scans [78](#)
 - results, on-demand scans [84](#)
 - scheduled scan progress [78](#)
 - unrecognized programs detected on network computers [87](#), [105](#)
 - Unrecognized Programs report [87](#), [105](#)
 - user-approved programs [86](#), [106](#)
- virus and spyware protection
 - approving programs [84](#)
 - best practices [89](#)
 - defined [13](#)
 - Detection History report [88](#)
 - Detections report [87](#)
 - detections, managing [84](#)
 - enabling and disabling on-access scanning [79](#)
 - enabling and disabling spyware protection [82](#)
 - excluded files and folders [82](#)
 - exclusions, managing [84](#)
 - learn mode [73](#)
- virus and spyware protection (*continued*)
 - on-access scans, overview [74](#)
 - on-demand scans, scheduled, overview [74](#)
 - on-demand scans, scheduling [80](#)
 - optional virus scans [80](#)
 - overview [71](#)
 - Potentially Unwanted Programs Viewer [84](#)
 - potentially unwanted programs, managing [84](#)
 - Prompt mode [72](#)
 - Protect mode [72](#)
 - Quarantine Viewer [85](#)
 - quarantined items, managing [85](#)
 - Report mode [72](#)
 - reports, overview [89](#)
 - scans, email, from Outlook [78](#)
 - scans, on-demand, from console [77](#)
 - scans, on-demand, from Windows Explorer [78](#)
 - scans, scheduled, viewing [78](#)
 - spyware protection mode, configuring [82](#)
 - spyware protection mode, overview [72](#)
 - spyware scans, configuring [82](#)
 - spyware scans, overview [76](#)
 - testing virus protection [33](#)
- vulnerabilities, See [threats](#)
- vulnerability scanning
 - active devices [156](#)
 - adding devices to scan [160](#)
 - certification, overview of process [155](#)
 - configuring devices to accept scans [161](#)
 - configuring scans [163](#)
 - creating device groups [161](#)
 - defined [13](#)
 - deleting devices [162](#)
 - detections [165](#)
 - device, defined [169](#)
 - devices to scan [156](#)
 - discovering devices in a domain [159](#)
 - discovering IP addresses in a network [159](#)
 - domain, defined [169](#)
 - domains, adding and deleting [159](#)
 - incomplete scan [161](#)
 - IP addresses where scans originate [161](#)
 - networks and subnets, adding [159](#)
 - overview [151](#), [155](#)
 - PCI certification, defined [13](#)
 - PCI certification, overview of process [155](#)
 - performing scans [163](#)
 - portal, accessing [154](#)
 - portal, illustrated [153](#)
 - reconfiguring device groups [162](#)
 - reports [165](#)
 - running discovery scans [159](#)
 - scheduling scans for devices [164](#)
 - security standards [157](#)
 - service level [160](#)

- vulnerability scanning (*continued*)
 - severity levels for vulnerabilities [157](#)
 - standards for scans [157](#)
 - trustmark certification, overview of process [155](#)
 - trustmark, defined [13](#)
 - types of scans [157](#)
 - viewing results, audit scans [166](#)
 - viewing results, DNS discovery [166](#)
 - viewing results, network discovery [167](#)
 - widget, illustrated [153](#)
- W**
- warn
 - file downloads, by ratings [119](#)
 - website access, by content [121](#)
 - website access, by ratings [118](#), [119](#)
- web filtering (browser protection)
 - authorized sites, configuring [123](#)
 - authorized sites, overview [122](#)
 - best practices [126](#)
 - blocking file downloads, by ratings [119](#)
 - blocking or warning website access, by content [121](#)
 - blocking or warning website access, by ratings [119](#)
 - blocking phishing pages [120](#)
 - configuring website access, by ratings [118](#)
 - Content Settings tab [122](#), [123](#)
 - customizing messages for blocked sites [124](#)
 - defined [13](#)
 - enabling and disabling at client computer [117](#)
 - enabling and disabling at policy level [117](#)
 - Exceptions list, configuring [123](#)
 - Exceptions list, overview [122](#)
 - overview [116](#)
 - prohibited sites, configuring [123](#)
 - prohibited sites, overview [122](#)
 - site patterns [122](#)
 - tracking Internet usage [125](#)
 - viewing browsing activity [125](#)
 - Web Filtering report [125](#)
- Web Filtering report [125](#)
- web protection (SaaS web protection)
 - activating [140](#)
 - browser protection and [138](#)
 - defined [13](#)
 - documentation, viewing on portal [142](#)
 - domains, configuring [140](#)
 - features [137](#)
 - getting started [139](#)
 - policies, configuring [141](#)
 - portal, accessing [140](#)
 - portal, illustrated [138](#)
 - web protection (SaaS web protection) (*continued*)
 - reports [141](#)
 - setting up [140](#)
 - troubleshooting [142](#)
 - widget, illustrated [138](#)
 - website access (browser protection)
 - authorizing and prohibiting sites [123](#)
 - blocking or warning, by content [121](#)
 - blocking or warning, by ratings [118](#), [119](#)
 - customizing messages for blocked sites [124](#)
 - downloads [119](#)
 - phishing pages [120](#)
 - viewing report of [125](#)
 - website access (SaaS web protection) [138](#)
- websites
 - access regulation (browser protection) [120](#)
 - access regulation (SaaS web protection) [137](#)
 - authorized and prohibited sites (browser protection) [122](#)
 - browsing protection (browser protection) [112](#)
 - search protection (browser protection) [111](#)
 - testing for safety (browser protection) [110](#)
 - viewing browser protection safety reports [115](#)
 - viewing reports (SaaS web protection) [141](#)
 - viewing visits (browser protection) [125](#)
 - viewing visits (SaaS web protection) [141](#)
- welcome kits
 - SaaS email protection [68](#), [131](#)
 - SaaS web protection [68](#), [139](#)
- widgets
 - adding to Dashboard page [42](#)
 - overview [42](#)
 - using [42](#)
- wildcard characters in searches [45](#)
- Windows 7
 - fast user switching support [31](#)
 - firewall [35](#), [169](#)
- Windows Explorer, on-demand scans from [78](#)
- Windows firewall
 - firewall protection service and [169](#)
 - log [169](#)
- Windows Vista
 - fast user switching support [31](#)
 - firewall [35](#), [169](#)
 - IP addresses, IPv6 format [95](#)
- Windows XP
 - fails to recognize virus protection [169](#)
 - fast user switching support [31](#)
 - firewall [35](#), [169](#)
 - updating computers where no user is logged on [29](#)
- windows, open [169](#)