



McAfee® Total Protection Service

for Microsoft Windows Home Server

COPYRIGHT

Copyright © 2008 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, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, MCAFFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, 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 ACCOMPANIES 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 WEB SITE 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.

License Attributions

Refer to the product Release Notes.

Contents

Total Protection Service User Guide	5
What is Total Protection Service?	5
Installing your software	6
Activating your software	6
Purchasing or renewing a full subscription	7
Using the Total Protection Service console	7
Accessing the features	8
Checking notifications	9
Checking the status of Total Protection Service	9
Configuring settings for Total Protection Service	10
Launching the SecurityCenter	10
Updating Total Protection Service	11
Scanning for threats	11
Scanning manually (on-demand scans)	12
Scheduling scans	12
Managing potentially unwanted program detections	13
Managing quarantined files	15
Troubleshooting	16
Testing your virus protection	16
Uninstalling and reinstalling Total Protection Service	17
Frequently asked questions	18
Error messages and notifications	19
Index	21

Total Protection Service User Guide

This guide provides basic instructions for using McAfee® Total Protection Service for WHS to safeguard your Microsoft Windows Home Server against a variety of threats.

- [What is Total Protection Service?](#)
- [Installing your software](#)
- [Using the Total Protection Service console](#)
- [Launching the SecurityCenter](#)
- [Updating Total Protection Service](#)
- [Scanning for threats](#)
- [Managing potentially unwanted program detections](#)
- [Managing quarantined files](#)
- [Troubleshooting](#)

What is Total Protection Service?

Total Protection Service is a comprehensive security management solution that:

- Checks for viruses, spyware, unwanted programs, and other potential threats. Every time a file is accessed on your server, Total Protection Service scans the file to make sure it is free of viruses and spyware.
- Sends security status information for your server to an administrative website that is unique to your account, known as the McAfee SecurityCenter. You can visit the SecurityCenter to check detection reports or set up security rules.
- Updates itself automatically at regular intervals with the latest versions of components and detection definition (DAT) files. This ensures that Total Protection Service is always able to protect you against the latest threats.

Typically, Total Protection Service operates in the background without any interaction on your part. Occasionally, however, you might need to interact with it. For example, you might want to schedule a weekly scan of all the files on your server. This guide explains how to use your basic security features and troubleshoot problems.

Optimized for WHS

Total Protection Service is optimized for your WHS multimedia environment. It continually monitors activity on the server to ensure that scanning operations do not interfere. When another activity places high demand on the server's processing capabilities, Total Protection Service pauses its scan, then resumes it when greater processing capability becomes available. This means that, for example, a scheduled scan might take longer than you anticipate, but will never degrade the performance of another activity, such as viewing a movie.

Installing your software

Total Protection Service is delivered to your server as an add-in.

To install Total Protection Service:

- 1 Click **Settings** in the upper right corner of the WHS console.
- 2 In the dialog box, click **McAfee Total Protection Service**.
- 3 Click **Add-ins**.
- 4 Click the **Available** tab.
- 5 Click **Install**.
- 6 When uninstallation is complete, you are notified that you need to close the WHS console, then restart it.

After installation, a trial period begins. Your copy of Total Protection Service updates the detection definition (DAT) files used to detect threats. Then the on-access scanning feature is activated to check all files automatically as you access them, and you can perform on-demand scans to check all the files on your server for threats. To continue receiving updates that protect you against new threats or to schedule scans, you need to activate your copy of Total Protection Service. On or before the end of the trial period, you must purchase a full subscription to extend protection beyond the trial period.

- [Activating your software](#)
- [Purchasing or renewing a full subscription](#)

Activating your software

Activate your copy of Total Protection Service to continue receiving DAT file updates that protect against the latest threats. An activated copy checks for updates automatically at regular intervals and allows you to schedule scans. After activating a trial version, you will also have an option to purchase a full subscription that extends protection beyond the trial period.

To activate your software:

- 1 In the **Common Tasks** area of the Total Protection Service console, select **Activate Now**.
- 2 Follow the instructions in the Activation wizard to enter information that identifies your account.

Purchasing or renewing a full subscription

Once you have activated a trial of Total Protection Service, you can extend protection by purchasing a full subscription during the trial period. A full subscription ensures you continue to receive updates and retain access to features such as on-demand scans and scheduled scans.

When a full subscription nears expiration, you can renew it to ensure uninterrupted protection.

To purchase or renew a subscription:

- 1 In the **Common Tasks** area of the Total Protection Service console, select **Buy Now**.
- 2 Enter your contact and payment information when prompted.



If your trial or full subscription has expired, Total Protection Service is no longer protecting your computer against new threats with updated DAT files. When you attempt to access a feature, a dialog box notifies you that your copy has expired and offers you the opportunity to purchase or renew a full subscription.

Using the Total Protection Service console

Total Protection Service provides a centralized interface for accessing and managing security for your Windows Home Server.

- [Accessing the features](#)
- [Checking notifications](#)
- [Checking the status of Total Protection Service](#)
- [Configuring settings for Total Protection Service](#)

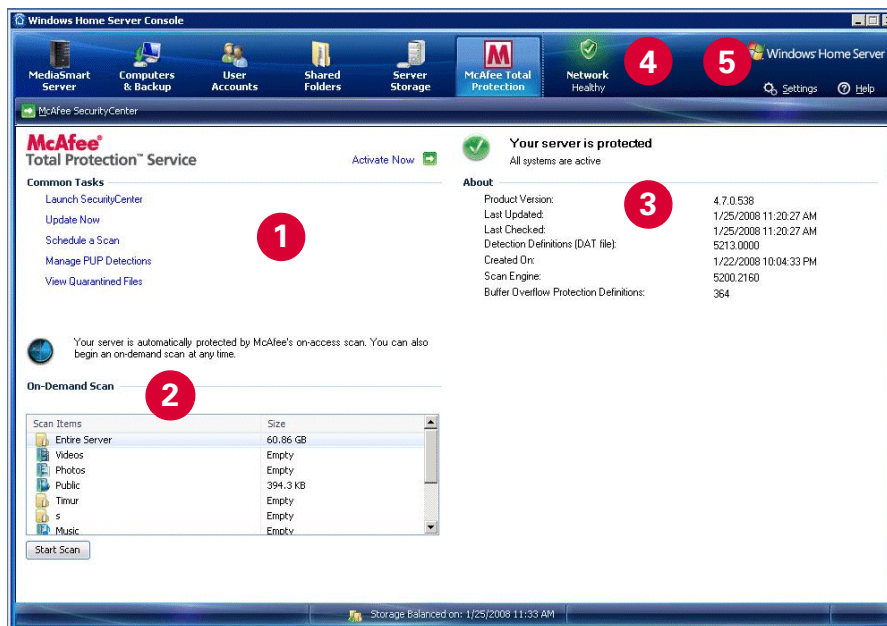
Accessing the features

Access Total Protection Service features through the Total Protection Service area of the WHS console.

To view the Total Protection Service console:

Click **McAfee Total Protection** at the top of the console window.

Figure 1-1



Use this area of the console...	To do this...
<p>1</p> <p>Common Tasks</p>	<p>Perform common tasks:</p> <ul style="list-style-type: none"> ■ Activate or purchase your software (see Activating your software and Purchasing or renewing a full subscription). ■ Visit the administrative website for your account (see Launching the SecurityCenter). ■ Check for updates to Total Protection Service components and threat detection files (see Updating Total Protection Service). ■ Schedule a time for a scan to occur (see Scanning for threats). ■ Respond to a potentially unwanted program detection (see Managing potentially unwanted program detections). ■ View the folder where detected threats are stored (see Managing quarantined files).
<p>2</p> <p>On-Demand Scan</p>	<p>Scan one or more shares on your server (see Scanning for threats).</p>
<p>3</p> <p>Status and About</p>	<p>Check the current status of your server and your software's components (see Checking the status of Total Protection Service).</p>
<p>4</p> <p>Network Health</p>	<p>Check notifications about the health of your system (see Checking notifications).</p>
<p>5</p> <p>Settings</p>	<p>Open the Settings dialog box, where you can schedule a scan or access Add-Ins to install, uninstall, or reinstall Total Protection Service (see Scheduling scans, Installing your software, and Uninstalling and reinstalling Total Protection Service).</p>

Checking notifications

Total Protection Service displays important information about your network's health in two locations:

- Using the **Network** icon at the top of the console.
- In popup messages in the bottom right corner of the screen. These messages appear on client computers where the notifications feature is enabled.

If the notification feature has been disabled:

Click the WHS icon in the system tray, then select **Display Network Health Notifications**.

Notification dialog boxes alert you to specific situations. Read each notification carefully to determine whether you need to respond. Notifications can indicate that:

- A threat has been detected, such as a virus or spyware. To view a threat detection notification, click the yellow **Network** icon at the top of the console. See [Managing potentially unwanted program detections](#) and [Managing quarantined files](#) for information on responding to detections.
- You need to activate your trial (see [Activating your software](#)).
- Your trial period is expiring (see [Purchasing or renewing a full subscription](#)).
- Your server is not fully protected due to one of these problems (see [Error messages and notifications](#)):
 - Threat detection files have not been updated in the last 14 days.
 - Total Protection Service is not running.
 - One or more components of Total Protection Service, such as the on-access scanning or automatic update feature, are not operational.

Checking the status of Total Protection Service

At the top of the status area, Total Protection Service displays your server's status:

Your server is protected	All Total Protection Service components are active and functioning properly.
Total Protection Service is performing an update	Total Protection Service is checking the update website for new versions of components or threat detection files. You should not disconnect from the Internet or turn off your server until the update is complete.
Your server is not protected	<p>Possible causes are:</p> <ul style="list-style-type: none"> ■ Threat detection files have not been updated in the last 14 days. ■ Total Protection Service is not running. ■ One or more components of Total Protection Service, such as the on-access scanning or automatic update feature, are not operational. <p>See Error messages and notifications for more information.</p>

The **About** area of the Total Protection Service console displays messages to indicate the status of all components.

	Description
Product version	The version of your virus and spyware protection software.
Last updated	The last date when your server downloaded updated files.
Last checked	The last date when your server checked for updated files.
Detection definitions (DAT file)	The version of the file that defines virus and spyware threats.
Created on	The date when your DAT file was created.
Scan engine	The version of the component that scans files to check for threats.
Buffer overflow protection definitions	The version of the file that defines buffer overflow threats.

Configuring settings for Total Protection Service

Access Total Protection Service settings from the **Windows Home Server Settings** dialog box.

To open the Windows Home Server Settings dialog box:

- 1 Click **Settings** in the upper right corner of the WHS console.
- 2 In the dialog box, click **McAfee Total Protection Service**.

From the dialog box, you can:

- Schedule a scan (see [Scheduling scans](#)).
- Install, uninstall, and reinstall Total Protection Service (see [Installing your software](#) and [Uninstalling and reinstalling Total Protection Service](#)).

Launching the SecurityCenter

Total Protection Service sends security status information for your server to an administrative website that is unique to your account. You can visit this site, known as the SecurityCenter, to check detection reports or set up security rules.

To open the SecurityCenter:

In the **Common Tasks** area of the Total Protection Service console, select **Launch SecurityCenter**.

To learn more about the SecurityCenter:

- View an audio-based overview of using the SecurityCenter to manage your computers, available at www.mcafeeasap.com/downloads/index.html?cid=37248.
- Get detailed instructions for all SecurityCenter features in the product guide, available from the SecurityCenter's **Help** tab as a printable PDF file or as online help.

Updating Total Protection Service

Total Protection Service 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 appear.
- Upgrades to software components. (To simplify product terminology, both updates and upgrades are referred to as updates.)

Updates usually occur automatically in the background. By default, they occur 5 minutes after you turn on your server and every 12 hours thereafter. In addition, Total Protection Service checks every hour for a special DAT file released by McAfee in response to a threat outbreak.

A message in the Total Protection Service console indicates when an update is in progress, and you should not disconnect from the Internet or turn off your server until the update is complete. You might also need to check for updates manually.



If a scheduled or on-demand scan is in progress when an update is scheduled to occur, the scan will be canceled. Be sure to schedule scans so they will not conflict with updates.

To manually check for new updates:

In the Total Protection Service console, select **Update Now**.

- A dialog box shows the progress of the update.
- When the update is completed, the **About** section of the console displays **Last Update**, the date, and a list of files that were downloaded.

Scanning for threats

Total Protection Service scans information on your Windows Home Server at these times:

- When you access files, folders, and programs, referred to as an *on-access scan*. You can specify which types of file are scanned on access by configuring a policy in the SecurityCenter.
- When you request a manual scan, referred to as an *on-demand scan*. After you install Total Protection Service for the first time, we recommend running an on-demand scan of all your server's shares before proceeding.
- When you specify a future time to perform a manual scan, referred to as a *scheduled scan*. If your server is powered off when a scan is scheduled to occur, the scan takes place five minutes after you power it up again.



If a scheduled or on-demand scan is in progress when an update is scheduled to occur, the scan will be canceled. Be sure to schedule scans so they will not conflict with updates.

Scanning manually (on-demand scans)

Use this feature to scan one or more shares on your server at any time.

To perform an on-demand scan:

- 1 In the **On-Demand Scan** section of the Total Protection Service console, select the share you want to scan.

To select more than one share, press **Ctrl** while you click each one.

- 2 Click **Start Scan**.

Status and results for the scan appear in the **On-Demand Scan** area of the console.



If another activity is placing a high demand on the server's processing capabilities, Total Protection Service pauses the scan, then resumes it when greater processing capability becomes available. A message appears in the **On-Demand Scan** area of the console to indicate the scan is paused.

Scheduling scans

Use this feature to specify a future time to perform a scan. You can schedule a single or a recurring scan.

To schedule a scan:

- 1 In the **Common Tasks** area of the Total Protection Service console, select **Schedule a Scan**.

OR

In the Total Protection Service console, click **Settings**, then click **McAfee Total Protection Service**.

- 2 Specify when you want the scan to run.

- 3 Click **OK**.



When another activity places high demand on the server's processing capabilities, Total Protection Service pauses its scan, then resumes it when greater processing capability becomes available. This means that a scheduled scan might take longer than you anticipate, but will never degrade the performance of another activity, such as viewing a movie.

Managing potentially unwanted program detections

Total Protection Service notifies you when it detects a potentially unwanted program attempting to run. The **Network** icon at the top of the console turns yellow to indicate that your network is at risk.

To respond to a detection notification:

- 1 Click the yellow **Network** icon.
- 2 In the dialog box, click **Close**.
- 3 In the **Common Tasks** area of the Total Protection Service console, select **Manage PUP Detections**.
- 4 In the **Potentially Unwanted Programs Viewer**, review the detection and select a response (see [To manage detections of potentially unwanted programs](#)).
- 5 After closing the **Potentially Unwanted Programs Viewer**, click the yellow **Network** icon again, select **Ignore this issue**, then click **Close**.



If you select **Ignore this issue** without approving the detected program, Total Protection Service detects the program each time it is accessed. To prevent the program from being detected again, you must open the **Potentially Unwanted Program Viewer** and approve the program.

To manage detections of potentially unwanted programs:

- 1 In the **Common Tasks** area of the Total Protection Service console, select **Manage PUP Detections**.

The **Potentially Unwanted Programs Viewer** lists each detected item that requires action. Items can include program files, registry keys, and cookies.

- 2 Select one or more items, then click an action.
 - **Clean**: Place an original copy of each selected item in a quarantine folder in a binary proprietary format, then attempt to clean it. If it cannot be cleaned, delete the item.
 - **Approve**: Add each selected item 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 your server.

- 3 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 binary proprietary format.

- **Quarantined:** The item could not be cleaned. The original item was deleted and a copy was placed in a quarantine folder in a binary proprietary 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 your server. These items are deleted after 30 days. You can manage these items using the **Quarantine Viewer** (see [Managing quarantined files](#)).

- **Delete failed:** The item could not 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. Total Protection Service has prevented the original item from accessing your server, but it cannot delete the item. Any items copied to your system have been cleaned.



If you are not sure why the item could not be cleaned, a risk might still exist.

- 4 Click **OK** to close the dialog box.



At the start of an on-demand scan, previous detections of potentially unwanted programs are cleared from the **Potentially Unwanted Program Viewer**. For on-access scans, previous detections remain in the **Potentially Unwanted Program Viewer**, and new detections are appended to the existing list.

To display a list of approved programs excluded from spyware scans:

- 1 In the **Common Tasks** area of the Total Protection Service console, select **Manage PUP Detections**.
- 2 In the **Potentially Unwanted Programs Viewer**, click **Approved**.

Managing quarantined files

When Total 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 in a binary proprietary format and cannot harm your server. By default, items in the quarantined folder are deleted after 30 days. Until then, you can view these files in the **Quarantine Viewer**.

To access files in the Quarantine Viewer:

- 1 In the **Common Tasks** area of the Total Protection Service console, select **View Quarantined Files**.

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

- 2 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 your server. The restored item will overwrite any other items with the same name in that location.



Total Protection Service 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 your computer.

- 3 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 binary proprietary 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. Total Protection Service has prevented the original item from accessing your server, but it cannot delete the item. Any items copied to your system 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.

- 4 Click **OK** to close the **Quarantine Viewer**.

Troubleshooting

The following sections contain information to assist you in detecting and resolving problems with Total Protection Service.

- [Testing your virus protection](#)
- [Uninstalling and reinstalling Total Protection Service](#)
- [Frequently asked questions](#)
- [Error messages and notifications](#)

Testing your virus protection

Test the virus detection feature at any time by downloading the EICAR Standard Anti-Virus Test File. Although it is designed to be detected as a virus, the EICAR test file is not a virus.

To run a test:

- 1 From a computer that has WHS connector software installed and is connected to your server, visit the following site in your browser:

<http://www.eicar.org>

- 2 Click **Anti-Malware Testfile**.
- 3 Right-click **eicar.com.txt**, select **Save Target As**, and save to the desktop.
- 4 Open a share on the computer. (From the WHS tray icon, select **Shared Folder** and log on if necessary.)
- 5 Copy the EICAR.TXT file to a WHS share (for example, \\SERVER\Software).

If installed properly, Total Protection Service interrupts the download and displays a detection notification.



The Network Health Notifications feature must be enabled. See [Checking notifications](#) for more information.

- 6 Click **OK**, then select **Cancel** in the file download dialog box.



If installed incorrectly, Total Protection Service **does not** detect the virus or interrupt the download process. In this case, delete the EICAR test file, then reinstall Total Protection Service and test the new installation.

Uninstalling and reinstalling Total Protection Service

For testing purposes or before reinstalling, you might need to uninstall Total Protection Service from your server.

To uninstall Total Protection Service:

- 1 Click **Settings** in the upper right corner of the WHS console.
- 2 In the dialog box, click **McAfee Total Protection Service**.
- 3 Click **Add-ins**.
- 4 Click the **Installed** tab.
- 5 Click **Uninstall**.
- 6 When uninstallation is complete, you are notified that you need to close the WHS console, then restart it.



If you uninstall Total Protection Service, your server is no longer protected. We recommend that you reinstall as soon as possible.

To reinstall Total Protection Service:

- 1 Click **Settings** in the upper right corner of the WHS console.
- 2 In the dialog box, click **McAfee Total Protection Service**.
- 3 Click **Add-ins**.
- 4 Click the **Available** tab.
- 5 Click **Install**.
- 6 When installation is complete, you are notified that you need to close the WHS console, then restart it.

Frequently asked questions

- *Can I stop a scheduled scan once it has started?*
- *I copied a virus to my server as a test and nothing seemed to happen. Why didn't my virus and spyware protection service detect it?*
- *Can I push the Total Protection Service firewall or browser protection service (SiteAdvisor™) to my Windows Home Server?*
- *Will policy settings I configure on the SecurityCenter override my local settings in Total Protection Service?*
- *Why does Total Protection Service detect the same potentially unwanted program multiple times?*
- *Why did my scheduled scan take much longer than expected to complete?*
- *Why did my scheduled scan end prematurely?*

Can I stop a scheduled scan once it has started?

No. Once a scheduled scan has started, you cannot stop the scan unless you restart the server.

I copied a virus to my server as a test and nothing seemed to happen. Why didn't my virus and spyware protection service detect it?

Total Protection Service is designed to quietly detect and clean threats without interrupting you. Most types of viruses are cleaned without you being notified. Threat detection is always noted on the reports available from the SecurityCenter, and you can check quarantined detections in the **Quarantine Viewer**. If you do not receive a notification when downloading the EICAR.TXT test file, check to be sure the notifications feature is enabled (see [Testing your virus protection](#)).

Can I push the Total Protection Service firewall or browser protection service (SiteAdvisor™) to my Windows Home Server?

No. Do **not** install these applications on your server.

Will policy settings I configure on the SecurityCenter override my local settings in Total Protection Service?

Yes. If you configure a policy (security rules) that does not include a scheduled scan, or if your policy includes a scan scheduled for a different time than one you have configured locally, your policy settings will override your local scheduled scan.

Why did my scheduled scan take much longer than expected to complete?

When Total Protection Service detects another activity placing a high demand on system resources, it pauses the scan until more resources are available. It is possible that a scan of multiple shares might be paused more than once to accommodate other activity on the server. If this happens, your scan can take longer to complete than you anticipated.

Why did my scheduled scan end prematurely?

If an update is scheduled to begin while an on-demand scan is in progress, the update takes precedence and the scan is canceled. Be sure to schedule scans for times when they will not conflict with updates.

Why does Total Protection Service detect the same potentially unwanted program multiple times?

Possible causes and solutions are:

- You have responded to a threat detection prompt by selecting **Ignore this issue**. Total Protection Service detects the program each time it is accessed unless you open the **Potentially Unwanted Program Viewer** and clean the program or approve it to run on your server (see [Managing potentially unwanted program detections](#)).
- The disk duplication (DEMigrator) feature in WHS has backed up the program on multiple shares. Each time a program is accessed on one of these shares, Total Protection Service detects it. (Check the **Shared Folders** area of the console to see which shares have the duplication feature enabled.) To prevent a detected program from being detected multiple times, open the **Potentially Unwanted Program Viewer** and clean the program or approve it to run on your server (see [Managing potentially unwanted program detections](#)).

Error messages and notifications

- *Your software is not up-to-date. Please activate to receive the latest updates.*
- *Your trial expires in 45 days.*
- *Detection: PUP. Resolve your detections using the Manage PUP Detections task, then select "Ignore this issue."*
- *Detection: VIRUS.*
- *Your server is not protected.*

Your software is not up-to-date. Please activate to receive the latest updates.

You have not activated a trial copy of Total Protection Service. You cannot receive updates against the latest threats or schedule scans until you activate. To activate, select **Activate Now** in the Total Protection Service console.

Your trial expires in 45 days.

Your activated trial will expire. To purchase a full subscription, select **Buy Now** in the Total Protection Service console.

Detection: PUP. Resolve your detections using the Manage PUP Detections task, then select "Ignore this issue."

A potentially unwanted program has been detected. See [Managing potentially unwanted program detections](#) for information on resolving it.

Detection: VIRUS.

A virus or other threat has been detected. This message includes the name of the detected item, the type of threat, the location of the threat, and the action taken. See [Managing quarantined files](#) for information.

Your server is not protected.

Possible causes and solutions are:

- DAT files have not been updated in the last 14 days. Select **Update Now** to download the latest files (see [Updating Total Protection Service](#)). If your trial or subscription has expired, buy or renew your subscription to continue receiving updated DAT files (see [Purchasing or renewing a full subscription](#)).
- Total Protection Service is not running. Reboot your server. If the problem persists, contact support.
- One or more components of Total Protection Service, such as the on-access scanning or automatic update feature, are not operational. Reboot your server. If the problem persists, contact support.

Index

A

- About area of Total Protection Service console [10](#)
- actions
 - for error messages [18](#)
 - for notifications [9](#), [18](#)
 - on potentially unwanted program detections [13](#)
 - on quarantined items [15](#)
- activating Total Protection Service [6](#)
- adding approved programs [13](#)
- Add-Ins [17](#)
- administrative website
 - defined [5](#)
 - launching [10](#)
- approved programs, potentially unwanted programs [13](#)

B

- buying trial software [7](#)

C

- clean failed, for quarantined items [15](#)
- configuring
 - Network Health Notifications [9](#)
 - security rules [10](#)
 - settings for Total Protection Service [10](#)
- console
 - About area [9](#)
 - accessing [8](#)
 - description [8](#)
 - illustrated [8](#)
 - notification area [9](#)
 - status area [9](#)

D

- DAT files
 - defined [11](#)
 - out-of-date [20](#)
 - updating [11](#)
- DEMigrator [19](#)
- demo about using SecurityCenter [10](#)
- detection definition files
 - see DAT files*

detectors

- multiple [13](#), [19](#)
- reports of [10](#)
- disk duplication feature [19](#)

E

- EICAR test virus [16](#)
- error messages
 - Detection PUP [19](#)
 - Detection VIRUS [19](#)
 - notification dialog boxes for [9](#)
 - Your server is not protected [20](#)
 - Your software is not up-to-date [19](#)
 - Your trial expires in 45 days [19](#)
- exclusions, potentially unwanted programs [13](#)

F

- frequently asked questions [18](#)

I

- ignoring potentially unwanted program detections [13](#)
- installing Total Protection Service [6](#)

L

- launching the SecurityCenter [10](#)

M

- managing
 - detections [13](#)
 - notifications [9](#)
 - potentially unwanted programs [13](#)
 - quarantined items [15](#)
- monitoring system utilization [6](#)

N

- Network Health area of Total Protection Service console [9](#)
- Network Health Notifications [9](#)
- notifications
 - also see error messages*
 - defined [9](#)
 - enabling [9](#)
 - testing virus protection and [16](#)

O

- on-access scans
 - defined [11](#)
 - trials and [6](#)
- on-demand scans
 - defined [11](#)
 - performing [12](#)
 - trials and [6](#)
 - updates and [11](#), [18](#)
- optimizing server performance [6](#)
- overview of Total Protection Service [5](#)

P

- pausing scans [6](#), [18](#)
- performance
 - optimizing [6](#)
- policies
 - defined [5](#)
 - interaction with scheduled scans [18](#)
- potentially unwanted programs
 - ignoring [13](#)
 - managing [13](#)
- purchasing trial software [7](#)

Q

- quarantined items, managing [15](#)

R

- reports, detections [10](#)
- rescan quarantined items [15](#)
- restore quarantined items [15](#)

S

- scanning
 - on-access, defined [11](#)
 - on-demand, performing [12](#)
 - pausing [6](#), [18](#)
 - scheduled, performing [12](#)
 - updates and [11](#), [18](#)
- scheduled scans
 - defined [11](#)
 - interaction with policy settings [18](#)
 - pausing [18](#)
 - performing [12](#)

- trials and [6](#)
- troubleshooting [18](#)
- security rules
 - configuring [10](#)
 - interaction with scheduled scans [18](#)
- SecurityCenter website
 - defined [5](#)
 - demo of basic features [10](#)
 - launching [10](#)
- Settings dialog box [10](#), [12](#), [17](#)
- status area of Total Protection Service console [9](#)
- system utilization, monitoring [6](#)

T

- testing your installation [16](#)
- Total Protection Service console
 - see console*
- trial software
 - activating [6](#)
 - buying [7](#)
 - features of [6](#)
- troubleshooting [16–20](#)

U

- uninstalling Total Protection Service [17](#)
- Update Now [11](#)
- updating
 - DAT files and components [11](#)
 - manually [11](#)
 - on-demand scans and [11](#), [18](#)
 - trials and [6](#)
- upgrades, defined [11](#)

V

- viewing
 - approved programs [14](#)
 - potentially unwanted programs [13](#)
 - quarantined items [15](#)

W

- website, administrative [10](#)