Upgrading Websense® Web Security Software

Websense Web Security
Websense Web Filter

v7.5

Published 2010
Printed in the United States of America and Ireland

Trademarks

WinPcap

Contents

1 Upgrading Websense Web Security or Web Filter

Perform an upgrade by running the Websense Web Security/Websense Web Filter 7.5 installer (Websense installer) on a machine with previous-version Websense components installed. The installer detects the presence of the components and upgrades them (with the exception of Remote Filtering Client) to the current version. For instructions on upgrading Remote Filtering Client, see the *Remote Filtering Software* technical paper.

> **Note**
> Technical papers and documents mentioned in this supplement are available Websense Technical Library: www.websense.com/library.

Versions 7.x of Websense Web Security or Websense Web Filter may be directly upgraded to version 7.5.

> **Important**
> Sites upgrading from version 7.1.1 should study the section titled *Backing up files* to see a list of variables that are returned to their default values during an upgrade from version 7.1.1 to version 7.5.0. Before you upgrade from version 7.1.1, please make a note of any custom values you have given these few variables, so that you can reset them after the upgrade.

New features for version 7.5 are described in the *Release Notes* for Websense Web Security and Websense Web Filter, Version 7.5. Information specific to this release is also available in the Upgrading User Quick Start tutorial, accessible from within TRITON - Web Security (which replaces Websense Manager) once it is installed.

This supplement provides an overview of the upgrade process, plus:

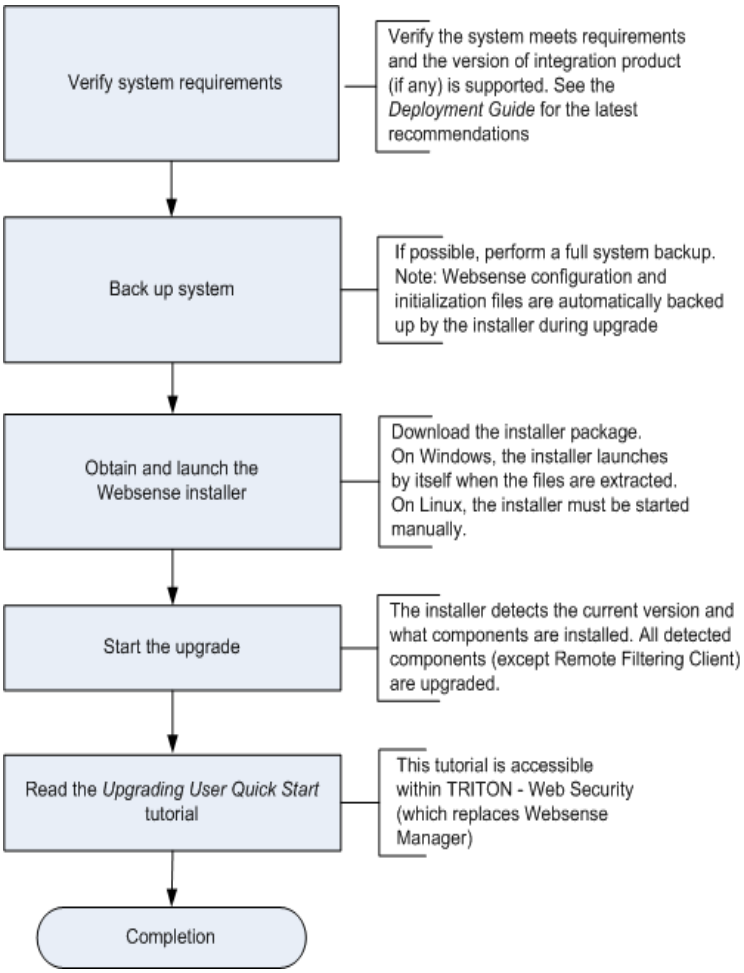
- *Versions supported for upgrade*
- *Preparing for the upgrade*
- *Upgrade instructions*
- *Adding components*

- *Changing IP addresses of installed components*

For information about upgrading Websense software when integrated with a third-party product, refer to the Websense *Installation Guide* supplement for your integration product.

> **Note**
> In this supplement, the term *Websense software* is used to refer to both Websense Web Security and Websense Web Filter collectively. Either product is named individually if information pertains to it only.

The following diagram provides an overview of the upgrade process.



Versions supported for upgrade

Direct upgrades to version 7.5 are supported from version 7.0 or higher of Websense software. Configuration and policy settings are preserved (with a few exceptions for sites *Upgrading from v7.1.1*.).

> **Note**
> If you have a localized installation of v7.0.1, keep in mind that v7.5 is an English-only release. Localization is not preserved in the upgrade.

Upgrades from versions prior to 7.0 require intermediate upgrades:

- version 5.5 > version 6.1 > version 6.3.2 > version 7.1 > version 7.5

> **Important**
> After upgrading from version 6.3.2 to 7.1, reboot the machine before upgrading it to version 7.5.

Configuration and policy settings are preserved across the intermediate upgrades. To perform an intermediate upgrade, download the installer package for the intermediate version from the Websense Downloads site:

www.websense.com/MyWebsense/Downloads/

> **Important**
> When performing intermediate upgrades, be sure to read the Websense Web Security and Websense Web Filter *Installation Guide* and its upgrade supplement for each upgrade version. They contain important information specific to upgrading between particular versions that may not be found in this version of the upgrade supplement.

Upgrading versions prior to 5.5

Perform a fresh installation rather than upgrade Websense software that is prior to version 5.5. Uninstall the prior version (be sure to remove all components from all machines in the network) and then install version 7.5. For uninstallation instructions, see the installation guide for your version available here (http://www.websense.com/applications/docsarchive).

If you have a complicated policy configuration, contact Websense Technical Support for assistance.

Preparing for the upgrade

This section describes important tasks to perform or issues to consider before upgrading Websense software:

System requirements

Before upgrading Websense software, make sure the installation machine meets the system recommendations in the *Deployment Guide* for Websense Web Security Solutions, including hardware specifications, operating system, browser, and database engine.

Backing up files

Before upgrading to a new version of Websense software, it is a best practice to perform a full system backup. This makes it possible to restore the current production system with minimum downtime, if necessary.

Upgrading from v7.x

If you are upgrading a v7.x system, Websense Backup Utility on each machine that contains Websense software:

1. Stop Websense services. See “Stopping and starting Websense services” in the Websense Web Security and Websense Web Filter *Installation Guide*.

2. Do one of the following:
   - *Windows*: Open a command window (Run > cmd) and navigate to the Websense **bin** directory (C:\Program Files\Websense\bin, by default).
   - *Linux*: Navigate to the Websense installation directory (/opt/Websense/, by default).
3. Use the following command to run the Backup Utility:
   - *Windows*:

     ```
     wsbackup -b -d <directory>
     ```
   - *Linux*:

     ```
     ./WebsenseTools -b -b -d <directory>
     ```

   For these commands, <*directory*> is the path where the backup file will be stored.

   The Backup Utility saves the essential Websense software files on the machine on which it is run, including any custom block pages. A complete list of the files saved can be found in the v7.x Websense Manager Help.

   Repeat this process on **all** machines on which Websense software is installed, and make sure that the files are stored in a safe and accessible location.
4. Start the Websense services. The Websense services must be running when you start the upgrade.

Upgrading from v7.1.1

Sites upgrading to version 7.5.0 from Websense Web Filter or Web Security version 7.1.1 should run the backup utility described above and should also carefully read the following list. This is a short list of configuration variables affected by the upgrade from v7.1.1.

These variables are returned to their default values during an upgrade from version 7.1.1 to version 7.5.0. They must be reset to your custom values.

Before you upgrade from version 7.1.1, please make a note of any custom values you may have given these variables or settings, so that you can reset them after the upgrade.

Windows-specific variables and settings that assume default values

- If you customized the charts displayed on the Today page in Websense Manager, or changed the values of the Time or Bandwidth Estimate options, you must re-do these customizations on the Today page in the TRITON console for Web Security.
- If you have set up Active Directory on the **Settings** > **General** > **Directory Services** page, you need to re-enter the information after the upgrade.
- If you customized the name of the folder used to output scheduled presentation reports, your customized folder name does not persist after the upgrade to v7.5. Check the name of this folder inside the file **mng.xml** in this path: C:\Program Files\Websense\tomcat\conf\Catalina\. The filename is the value for the parameter: **reportsOutput**.
- Reporting preferences on the page **Settings** > **Reporting** > **Preferences** do not persist after an upgrade to v7.5.This includes the **SMTP server IP address** or

name, the **email recipients** for scheduled reports, and the **Allow self-reporting** check box. Note the values before the upgrade and reset them afterwards.

- Note the Active Directory values configured in Websense Manager on the **Settings > Directory Service** page. You need to specify these again after the upgrade.
- Navigate to the **Manage Custom LDAP Groups** page, and note any custom groups you have set up, based on attributes defined in your directory service. This option is available only if you have configured Websense software to communicate with an LDAP-based directory service. After the upgrade to v7.5, custom LDAP groups created by delegated administrators need to be re-created.
- If you specified a non-standard port on which Network Agent monitors HTTP traffic, the setting does not persist after an upgrade to v7.5. This paragraph explains how to check this setting. Navigate to the **Settings > Network Agent > Local Settings** page to see the settings for a selected instance of Network Agent. The IP address of the selected Network Agent instance appears in the title bar of the content pane, and is highlighted in the left navigation pane. Use the **Network Interface Cards** list to see the configuration for the individual NICs. Click on a NIC in the **Name** column to view (and then make note of) custom details. If HTTP requests in your network are passed through a non-standard port, click **Advanced Network Agent Settings** to see the ports that Network Agent monitors. By default the Ports used for HTTP traffic are 8080, 80.
- If you customized the HTTPS port value for Websense Manager, the custom value does not persist after upgrade. To check the value, or to reset the value after the upgrade:
  - On the machine where the manager console runs, use the Windows Services dialog box (Start > Administrative Tools > Services) to stop the ApacheTomcatWebsense service.
  - In a text editor, open the file **server.xml** from the folder C:\Program Files\Websense\tomcat\conf.
  - Change the value of the HTTPS port to the desired port.
- After upgrade, you must manually set the version number to 7.5 (in place of 7.1.1) in the container \EIMServer\Global\Version\ in the file **config.xml**. This file is located by default in the directory C:\Program Files\Websense\bin\.

Linux-specific variable that assumes default value

The value of DNSLookup in the file **eimserver.ini** should be noted before upgrade and restored afterwards.

This file is located by default in the directory /opt/Websense/bin/.

Variables on both Windows and Linux that assume default value

- During the process of upgrading from v7.1.1, the parameter redirect_children, in the **squid.conf** file located by default in the /etc/squid directory, is reset to default.
- The value of all parameters in the file **mng.xml**, such as **connectionsMaxActive,** should be noted before upgrade and then restored to the custom value after the upgrade.This file is located by default in the directory:

Windows: C:\Program Files\Websense\tomcat\conf\Catalina\localhost\

Linux: /opt/Websense/tomcat/conf/Catalina/localhost/

Upgrading from v5.x and v6.x

Before starting the multiple-step process required to upgrade a v5.x or v6.x system, be sure to back up (at a minimum) the following files:

1. Stop all Websense services. See “Stopping and starting Websense services” in the Websense Enterprise and Websense Web Security Suite *Installation Guide*.
2. Make a backup copy of the following files (located by default in the C:\Program Files\Websense\bin or /opt/Websense/bin directory).
   - config.xml
   - websense.ini
   - eimserver.ini
3. If you have created custom block pages, make a backup copy of the files in the **Websense\BlockPages\en\Custom** (Windows) or **Websense/BlockPages/en/Custom** (Linux) directory.
4. Save the backup copies to another location.
5. Start the Websense services. The Websense services must be running when you start the upgrade.

Changes to integration product

If you plan to modify your integration product (for example, upgrading it), it is a best practice to make the change before upgrading Websense software. See the Websense *Installation Guide* supplement for your integration product for more information.

Websense Master Database updated

The Websense Master Database is removed when you upgrade from version 7.x; Websense Filtering Service downloads a new Master Database after the upgrade is completed.

All traffic permitted or blocked during upgrade

If Websense software is integrated with another product or device all traffic is either unfiltered and permitted, or completely blocked during the upgrade, depending on how your integration product is configured to respond when Websense filtering is unavailable.

When you upgrade a stand-alone installation of Websense software, filtering stops when Websense services are stopped. Users have unfiltered access to the Internet until the Websense services are restarted.

Relocating components

If you want to move any Websense component in your deployment to a different machine, it is a best practice to do so before upgrading.

Remove the component and then install it on the new machine, **using the installer for your current version**. See the Websense Web Security and Websense Web Filter *Installation Guide,* for your version, for instructions.

Important

When moving components, make sure the associated Websense Policy Server is running. Policy Server keeps track of the location of components in a deployment. See the *Installation Guide*, for your version, for more information.

Once components are distributed to their final locations, run the new version installer on each machine to upgrade the components to the new version. See *Upgrade instructions*, page 16.

Log Server using trusted connection

If you are upgrading Websense Log Server and it uses a Windows trusted connection to access the Log Database, you must log on to this machine with the same trusted account before running the Websense installer to perform the upgrade.

Use the Windows **Services** dialog box to find which account is used by Log Server:

a. Start the Windows **Services** dialog box (typically, **Start** > **Administrative Tools** > **Services**).

b. View the **Log On As** column entry for Websense Log Server. This is the account you should use.

Functioning deployments only

The upgrade process is designed for a properly functioning deployment of Websense software. Upgrading does not repair a non-functional system.

Version 6.x Audit Log

If you must perform an intermediate upgrade (see *Versions supported for upgrade*, page 7) from version 6.3.2 to 7.1, be aware that the Audit Log for the version 6.3.2 installation will not carry across to version 7.1. To preserve your 6.x Audit Log, use Websense Manager to export the log to a tab-separated text file prior to upgrading. Then, move the exported file to a directory that will not be affected by the upgrade

(i.e., outside the Websense installation directory: C:\Program Files\Websense or /opt/Websense, by default).

> **Note**
> If you upgraded to version 7.1 without exporting the 6.x Audit Log, you may still be able to retrieve it. Search the Websense Knowledge Base (support.websense.com) for the terms *Upgrading from v6.x does not preserve the audit log*.

Check for hostname on Linux

If you are running an upgrade on Linux, make sure that the **hosts** file includes the host name for the machine on which you are running the upgrade. This file is located in the **/etc** directory, by default. Add a hostname for the machine, if one is not included. See the Websense Web Security and Websense Web Filter *Installation Guide* for instructions.

Previous version configuration files

Do not install version 7.5 Websense software on a separate machine and then copy a previous version's configuration files to that machine.

Non-English language versions

This version is available in English only. The screens, alerts, messages, and other text associated with new features and functions have not been localized.

Upgrading distributed components

To upgrade Websense software, run the Websense installer on each machine running Websense components. Distributed components must be upgraded in a particular order. Start with the machine running Policy Broker. See the order for upgrading components in *Upgrade instructions*, page 16.

Upgrading a filtering plug-in

If your Websense software is integrated with a third-party product requiring a Websense filtering plug-in (Microsoft ISA Server, Citrix Presentation Server, or Squid Web Proxy Cache), the plug-in must be upgraded as well.

> **Note**
> Prior to upgrading Websense software and the filtering plug-in, make sure your version of integration product is supported by the new version of Websense software. See the *Installation Guide* supplement for your integration product for supported versions.

Run the Websense installer on the integration product machine. The installer detects Websense integration-specific components and upgrades them.

> **Note**
> If you are changing your integrated firewall, proxy server, caching application, or network appliance, modify that product before upgrading Websense software. See the Websense Web Security and Websense Web Filter *Installation Guide* and *Installation Guide* supplement for the integration product and your current version of Websense software.

Do not use remote control utilities

Upgrading Websense software via a remote control utility such as Terminal Services is **not** supported.

Websense services must be running

Websense services must be running when the upgrade process begins. The installer stops and starts these services during the upgrade.

If these services have been running uninterrupted for several months, the installer may not be able to stop them before the upgrade process times out.

To ensure the success of the upgrade, manually stop and start all the Websense services before beginning the upgrade. See *Stopping or starting Websense services* in the Websense Web Security and Websense Web Filter *Installation Guide* for instructions.

Important

In the Windows Services dialog box, if you have set the **Recovery** properties of any of the Websense services to restart the service on failure, you must change this setting to **Take No Action** before upgrading.

Matching locales

When upgrading Websense Filtering Service installed on a machine separate from Websense Manager, you must upgrade Filtering Service in the same locale environment (language and character set) as Websense Manager.

- Before upgrading Filtering Service on Windows, open **Control Panel** > **Regional Options**, and change the locale to match that of the Websense Manager machine.
- When upgrading on Linux, log on to the Filtering Service machine with the locale appropriate to Websense Manager.

After the upgrade is complete, Websense services can be restarted with any locale setting.

Upgrade instructions

The standard Websense Web Security/Websense Web Filter 7.5 installer (Websense installer) is also used for upgrades. After it starts, the installer detects when an older version of the product is installed. The installer also detects which Websense components are installed and need to be upgraded, and checks the version of the database engine to ensure it is compatible with the new version of Websense software.

- *Upgrade order*, page 16
- *Upgrade steps*, page 17

Important

- Filtering and logging services are not available while running the upgrade. To reduce the impact on network users, run the upgrade after hours, or during a quiet time on the network.
- The *Installation Guide* supplement for your integration product contains information about any additional steps needed to upgrade and configure Websense software to run with your product. Refer to the supplement before performing the following procedures.

Upgrade order

If Websense components are distributed across multiple machines, they must be upgraded in the following order due to dependencies between them.

1. Policy Broker
2. Policy Server
3. User Service
4. Filtering Service
5. Network Agent
6. Transparent identification agents
7. Filtering plug-in (on integration product machine)
8. Log Server
9. Websense Manager

If multiple components are installed on a machine, the installer upgrades them in the proper order.

Upgrade steps

Perform the following procedure on each machine running Websense components.

Important

If Websense components are installed on multiple machines, see *Upgrade order*, page 16, for important information about the required upgrade sequence. All components that interact in a deployment must be upgraded to the same version.

1. If you performed an intermediate upgrade from version 6.3.2 to 7.1, and you have not done so yet, reboot the machine before upgrading from version 7.1 to 7.5.
2. Close all instances of Websense Manager.
3. Log on to the installation machine with administrator privileges:
   - Linux—log on as **root**.
   - Windows—log on with **domain** and **local** administrator privileges.

   If you are upgrading User Service, DC Agent, or Logon Agent, this ensures that those components have administrator privileges on the domain.

Important

If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account. See *Log Server using trusted connection*, page 12.

4. Perform a full system backup.

   If a full backup is not feasible, make backup copies of the **websense.ini**, **eimserver.ini**, and **config.xml** files, and move them to a different location. These files are located in the Websense **bin** directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).
5. Close all applications and stop any antivirus software.

Warning

Be sure to close the Windows Event Viewer, or the upgrade may fail.

6. On Linux:
   a. Check the **etc/hosts** file. If there is no host name for the machine, add one.

      See the Websense Web Security and Websense Web Filter *Installation Guide* for instructions.

   b. Create a setup directory for the installer files, such as **/root/Websense_setup**.

> **Important**
>
> If your Websense services have been running uninterrupted for several months, the installer may have difficulty stopping them.
>
> To prevent the upgrade process from timing out and failing, stop the services manually and start them again before beginning the upgrade. For instructions, see *Stopping or starting Websense services* in the *Websense Web Security and Websense Web Filter Installation Guide*.

7. Download the installer package for Websense Web Security/Web Filter and start the installer. See the Websense Web Security and Websense Web Filter *Installation Guide* for instructions.

   The installer detects any Websense components from an earlier version and asks how you want to proceed. You can upgrade the current system or exit the installer.

> **Note**
>
> If you want to add components, see *Adding components*, page 20.

8. On the **Introduction** screen, click Next.

> **Note**
>
> These instructions refer to installer screens. In the command-line Linux installer, prompts are displayed that correspond to each screen. Instructions for a screen also apply to the corresponding command-line prompt. The main difference is how options are selected. Rather than clicking items in a screen, you will enter menu-item numbers or characters.

9. On the **Subscription Agreement** screen, choose to accept the agreement and click Next.

   If you do not accept the agreement, you cannot proceed with the upgrade.

10. On the **Websense Upgrade** screen, select **Start the upgrade** and then click Next.

    > **Important**
    > Be sure to close all instances of Websense Manager, on all machines, before clicking **Next**.

    When you click Next, a *Stopping All Services* progress message appears.

11. Wait for Websense services to be stopped. The **Pre-Upgrade Summary** screen appears when the services have been stopped.

    In some cases, the installer may be unable to stop the Websense services. If the services have not been stopped after approximately 10 minutes, then stop them manually. You can leave the installer running when you do so. On Windows, use the Windows Service dialog box to stop the services. On Linux, use the `WebsenseAdmin` command. See the *Websense Web Security and Websense Web Filter Installation Guide* for instructions. Once you have manually stopped the services, return to the installer.

12. On the **Pre-Upgrade Summary** screen, review the list of Websense components that will be upgraded, and then click **Install**.

    A *Websense Web Security is being configured* progress message appears.

    Wait for the **Upgrade Complete** screen to appear.

13. Click **Done** to exit the installer.
14. Reboot the machine.

    > **Important**
    > The machine must be rebooted to complete the upgrade process.

15. If you stopped your antivirus software, restart it.
16. If you have an integration product installed, check the *Installation Guide Supplement* for your integration to see if further upgrade steps are needed.
17. Repeat the upgrade procedure on the each machine running Websense components, in the recommended order (see *Upgrade order*, page 16).

    All components that interact must be upgraded to the same version.

    If you have complete installations in separate locations that do not interact, they do not have to run the same Websense software version.

18. After all components have been upgraded, launch TRITON - Web Security (replaces Websense Manager):
    - On any machine in your network, open a Web browser and enter the following:

      `https://<IP address>:9443/mng`

      Replace <*IP address*> with the IP address of the TRITON - Web Security machine.
    - If TRITON - Web Security is installed on a Windows machine, double-click the TRITON - Web Security desktop icon on that machine, or go to **Start** > **Programs** > **Websense** > **TRITON - Web Security**.

    Notes
    - See the *Deployment Guide* for Websense Web Security Solutions for which versions of Internet Explorer and Firefox are supported by TRITON - Web Security.
    - In some cases, after upgrade, the Windows Desktop icon for TRITON - Web Security still appears as the Websense Manager icon. See *TRITON - Web Security icon still appears as Websense Manager*, page 24.

19. After you start TRITON -Web Security, run the *Upgrading User Quick Start* tutorial for an overview of the new features and changes in the current version.
20. Be sure to reset specific custom values if you are *Upgrading from v7.1.1*.

Adding components

To add components to a machine on which Websense components are already installed, first upgrade the pre-existing components (see *Upgrade instructions*, page 16). The first time you run the Websense installer, it will upgrade the existing components. After upgrading, run the Websense installer again on the same machine. This time, the installer will ask if you want to add components. See the *Installation Guide* for instructions on adding components.

Changing IP addresses of installed components

If the IP address changes for a machine running Policy Server or Policy Broker after upgrade, certain configuration files must be updated. See the instructions for changing the Policy Server IP address under the *Websense Server Administration* topic in the TRITON - Web Security Help. Use the same procedure if you change the IP address

of Policy Broker (more instances of the IP address will be found in the files being updated).

Websense software handles IP address changes in the background for most other components, without any interruption to filtering.

In some cases, Websense services need to be restarted or configurations updated after changing an IP address.

Network Agent settings can be updated in TRITON - Web Security. See the TRITON - Web Security Help for more information.

2 Troubleshooting

Configured users do not appear on the Clients page

If you are using Active Directory as your directory service, you may find that user names disappear from the list of directory objects in TRITON - Web Security (formerly Websense Manager) after you upgrade. This change occurs if your user names include characters that are not part of the UTF-8 character set.

For more information, see the Troubleshooting section of the TRITON - Web Security Help. Look for the *users are missing* discussion under *Installation and subscription issues*.

TRITON - Web Security does not launch

TRITON - Web Security is the central configuration interface used to customize filtering behavior, monitor Internet usage, generate Internet usage reports, and manage Websense software configuration and settings. This Web-based tool runs on these supported browsers:

- Microsoft Internet Explorer 7 and 8
- Mozilla Firefox 3.0.x - 3.5.x

Although it is possible to launch TRITON - Web Security using some other browsers, use the supported browsers to receive full functionality and proper display of the application.

If you are unable to connect to TRITON - Web Security on the default port (9443), refer to the **knownports.properties** file on the TRITON - Web Security machine (located by default in the C:\Program Files\Websense\bin or /opt/Websense/bin/ directory) to verify the port. Look for **APACHE_HTTPS=** <*value*>. This is the configured port for TRITON - Web Security.

If you are using the correct port, and are still unable to connect to TRITON - Web Security from a remote machine, make sure that your firewall allows communication over that port.

TRITON - Web Security icon still appears as Websense Manager

The Websense installer upgrades Websense Manager to TRITON - Web Security. The Windows Desktop icon for Websense Manager is also updated to reflect TRITON - Web Security. In some cases, the Windows Desktop icon does not show the new TRITON - Web Security icon but, instead, remains the Websense Manager icon. (Note that the icon still launches TRITON - Web Security).

Reboot the machine to update the icon. If after reboot, the icon has still not been updated, refresh the Windows Desktop cache as described below.

Windows Server 2003

Refresh the Windows Desktop cache by toggling the **Use large icons** setting:

1. Select **Start** > **Control Panel** > **Display**. (Alternatively, right-click the Windows Desktop and select Properties.)

   The **Display Properties** dialog box appears.
2. Select the **Appearance** tab
3. Click **Effects**.
4. Toggle the **Use large icons** option: if it is selected, then deselect it; if it is not selected, then select it.
5. Click **OK** to return to the Display Properties dialog box.
6. Click **Apply**.

   The desktop icons will refresh and redisplay.
7. Return the **Use large icons** option to its original state:
   a. Click **Effects** again.
   b. Set the **Use large icons** option to its original state.
   c. Click **OK** to return to the Display Properties dialog box.
   d. Click **OK**.

Windows Server 2008

Refresh the Windows Desktop cache by changing icon size; then return the size to its original value if you want:

> **Note**
> This procedure may re-arrange your Desktop icons. If you have a particular arrangement, make note of it and be aware that you may have to move icons back to their original positions.

1. Right-click the Windows Desktop and select **Personalize**.

   The **Control Panel\Personalization** window appears.
2. Under Tasks, select **Adjust font size (DPI)**.

   The **DPI Scaling** dialog box appears.
3. Select whichever option is not currently selected (either **Default scale** or **Larger scale**).
4. Click **OK**.
5. Choose to restart the machine now.

   After restart and login, the correct icon should now be displayed for TRITON - Web Security.
6. Keep the new size setting or revert back to the original size by repeating this procedure to return to the original setting.

Index

U

V

W