Upgrading from v7.7.x to v7.8.x

Websense® Data Security

v7.8

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2010

Printed in the United States and Ireland

Contents

1 Upgrading Data Security from v7.7.x to v7.8.x

Websense Data Security must be at least version 7.7.0 in order to upgrade to v7.8.x.

To upgrade v7.7.x to v7.8.x, do the following:

1. *Upgrade the Data Security Management Server*
2. *Upgrade any supplemental Data Security servers and standalone agents*
3. *Upgrade protectors and mobile agents*
4. *Upgrade endpoints*

Perform the upgrade in the order described. This sequence is critical, because if you upgrade supplemental servers or agents before the management server, they stop communicating. If you upgrade the management server first, it continues communicating with the components until they are upgraded.

This guide describes how to upgrade stand-alone installations of Data Security v7.7.x to v7.8.x. For information on upgrading systems that include Websense Web Security and/or Email Security as well as Data Security, refer to the Deployment and Installation Center in the Websense Technical Library.

For high-level flow charts of the Data Security upgrade process, see:

- Manager upgrade
- Servers and agents upgrade
- Protector/mobile agent upgrade
- Endpoint upgrade

Upgrade the Data Security Management Server

You upgrade your management server using the TRITON installation package, **WebsenseTRITON78*x*Setup.exe**, where *x* is the version number. This is the same executable used for scratch installations.

The installation package detects that earlier versions of the product are installed, and automatically starts a series of upgrade wizards—one for each of the installed components.

The Data Security portion of the unified upgrade wizard upgrades all necessary components on the Data Security Management Server.

After upgrade, your system has the same configuration as before the upgrade. The upgrade process does not allow you to change your configuration or settings.

Preparing for upgrade

- Unless instructed otherwise by Websense Technical Support, ensure your system is functional prior to upgrade.
- Make sure your base version is 7.7.x.
- Perform a full backup of your system before upgrading.
  a. Use the TRITON backup utility to back up your TRITON Settings information (administrator accounts, for example).
     - On the TRITON management server machine, go to **Start > Administrative Tools > Task Scheduler**, then select **Task Scheduler Library**.
     - If the Triton Backup task is disabled, right-click the task and select **Enable**.
     - Right-click the Triton Backup task and select **Run**.
  b. Back up Data Security software as described in How do I back up and restore Data Security software?
- Stop all discovery and fingerprinting tasks.
- Route all traffic away from the system.
- Ensure that your supplemental fingerprint repositories are fully synchronized with the primary repository.
- Make sure all settings are deployed successfully. Log onto the Data Security manager. If the **Deploy** button is highlighted, click it.
- If Websense supplied your organization with custom file types, change the name of 2 configuration files located in the \policies_store\custom_policies\config_files folder where Data Security is installed; otherwise they will be overwritten during upgrade.
  a. Change **extractor.config.xml** to **custom_extractor.config.xml**.
  b. Change **extractorlinux.config.xml** to to **custom_extractorlinux.config.xml**.

  The filenames are case-sensitive.
- If you have custom policies provided by Websense, submit a request for updated versions before proceeding.

Note that the speed and success of your upgrade are affected by many factors, including:

- Number of online incidents.
- Size of the forensics folder.
- Number of policies or rules in use
- User directory import size

- Whether GPO restrictions are enforced on the server in domain membership scenarios

Upgrade steps

To upgrade TRITON management server components, use the v7.8 TRITON unified installer (Windows only): **WebsenseTRITON78xSetup.exe**, available from:

www.websense.com/MyWebsense/Downloads/

Select **Data Security**, **version** (7.8), and **operating system** (Windows), then click **download** next to the installer description.

When you launch the installer, it detects that earlier versions of the product are installed, and automatically starts a series of upgrade wizards—one for each of the modules included on the management server.

For best practice, log on as the service account.

> **Note**
> If TRITON management components run on a virtual machine, restart the server after the upgrade is complete.

TRITON Infrastructure

The TRITON infrastructure provides basic framework for all of the management components that make up TRITON Unified Security Center (TRITON console). This framework includes a central settings database that stores shared configuration (like administrator directory and account information) for all management modules, as well as other internal shared services.

The infrastructure upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Welcomes you to the installation and upgrade wizard. 1. Click **Next** to begin the upgrade process. The system checks disk space requirements. 2. When prompted, click **Next** to launch the installation wizard.
Pre-Installation Summary	Shows: • The destination folder for the installation files. • The name of the SQL Server machine and the user name of an authorized database administrator. • The IP address of the TRITON management server and administrator credentials. Click **Next** to accept the properties.

Wizard Screen	Fields
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more. A popup message appears at this stage,warning that you must also upgrade all modules. This popup may be hidden behind the main installer window, so if your installation appears to freeze, locate the hidden popup by moving the main installer window, and click **OK** to proceed with the installation.
Summary	When module upgrade is complete, summarizes your system settings, including: • The destination folder for the installation files. • The name of the SQL Server machine and the user name of an authorized database administrator. • The IP address of the TRITON management server and administrator credentials. Click **Finish** to complete the upgrade for this module.

Data Security

The Data Security upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	This screen welcomes you to the installation and upgrade wizard for Data Security. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
Installation Confirmation	Verify your system settings and click **Install** to continue the upgrade.
Installation	This screen shows the progress of the installation. The system stops processes, checks ports, copies new files, updates component registration, removes unused files, and more.
Summary	When installation of this module is complete, this screen summarizes your system settings. 1. Click **Done** and you're prompted to update your predefined policies and content classifiers. 2. Click **OK** to install the updates. You're shown the status of the updates, the items being updated, and details such as how many policies are updated, deleted, or added. 3. Click **Close** when the updates are complete.

Wrapping up

1. Log onto the TRITON console (https://<IP_address_or_hostname>:9443/triton/).
2. Select the Data Security tab.

3. You are prompted to update your policies. Follow the prompts. Websense research teams stay abreast of regulations across many industries and you should keep your policies and classifiers up-to-date. Depending on the number of policies you have, this can take up to an hour. During this time, do not restart the server or any of the services.
4. Click **Deploy**.
5. If you are upgrading from v7.7.2 to v7.8.3 or 7.8.4, run the reporting upgrade tool attached to knowledge base article 7472 on the machine where SQL server is installed. This prevents issues that are sometimes encountered with Scheduled Tasks after upgrade.

Upgrade any supplemental Data Security servers and standalone agents

Complete these steps to upgrade a supplemental Data Security server or stand-alone agent to v7.8.x.

Important

Starting with v7.8.2, supplemental Data Security servers must be on 64-bit platforms. Those running on Windows 2003 have their policy engines removed during the upgrade and only the agent is upgraded.

Starting with 7.8.3, all support for Windows 2003 has been dropped. As a result, the printer agent, SMTP agent, and ISA agent, which are dependent on Windows 2003, are no longer available.

Although you cannot upgrade these agents to the latest version, you can use existing 7.8.1 and 7.8.2 agents with the v7.8.x management server.

Websense does offer the TMG agent as a replacement for ISA.

1. If you are upgrading a Windows 2003 agent to v7.8.1 or 7.8.2, launch the installer, **WebsenseTRITON78*y*Setup.exe**, where *y* is the version number. The software is detected, and the upgrade wizard appears.

   If you are upgrading an agent to v7.8.1 or v7.8.2 on a 64-bit machine, launch **WebsenseDataSecurityAgents78*y*-x64.msi**.

   Use this same 64-bit installer to upgrade the TMG agent and supplemental servers to the latest 7.8.x version.
2. Click **Next** until you complete the wizard.

   Any v7.7.x Data Security components found on this machine are upgraded.

3. After the upgrade has successfully completed, deploy the agents and supplemental servers by logging on to the TRITON console, selecting the Data Security tab, and clicking **Deploy**.

It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

When you upgrade a Data Security server it takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in:

- Potential false positives and negatives.
- File-system discovery starts but immediately indicates "completed with errors".

Upgrade protectors and mobile agents

Do the following to upgrade your protector or mobile agent from version to v7.8.x.

Important

If you are upgrading your protector to new hardware, be sure to keep the original IP address/host name if you want to retain settings and information from the original machine.

If you assign a new IP, the protector's settings are cleared to default when it registers with the management server. In this case, you should manually delete the protector with the original IP address from the system modules page of the Data Security manager.

1. Download the protector update script from www.websense.com/MyWebsense/Downloads/.
2. Copy the file, protector-update-7.8.*x-yyyy*, into the directory `/tmp` where *x-yyyy* is the latest version and build number, such as 7.8.4.35.
3. Enter the command:

   ```
   chmod +x /tmp/protector-update-7.8.x-yyyy
   ```

4. Run the following command:

   ```
   bash /tmp/protector-update-7.8.x-yyyy
   ```

5. Answer **Y** on the "Are you sure?" question, and complete the wizard, accepting the defaults.
6. Restart the protector or mobile agent machine when the wizard completes.
7. If you have not already, log onto the machine as *root*. If you are using the appliance as a mobile agent and want to get root privileges by running "su", be sure to keep the same environment by running "su -" and not just "su".

8. Run the following command to re-register the protector or mobile agent with the management server, then follow the prompts in the wizard:

   ```
   wizard securecomm
   ```

9. In the Data Security manager, click **Deploy**.
10. It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

    When you upgrade a protector, it takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in false positives and negatives.

Upgrade endpoints

Version 7.7.x endpoints are fully compatible with the v7.8 management server and can take advantage of the new predefined policies. To gain access to new endpoint features, however, you should upgrade your endpoints to v7.8.

For best practice, upgrade a handful of endpoints and ensure that they're working before upgrading all of the endpoints in your deployment.

Windows

After you have upgraded the Data Security Management Server and all supplemental Data Security servers:

1. Select **Start > Programs > Websense > Data Security > Endpoint Package Builder** on the management server to launch the endpoint client package builder.
2. Choose Windows 32- or 64-bit when prompted.
3. Deploy the v7.8.x package to each endpoint using GPO, SMS, or a similar deployment method. You can install v7.8.x on top of earlier versions without uninstalling and re-installing them.
4. Restart the endpoint after installation is complete.

For best practice, deploy an endpoint auto-update server. This can be used to push an endpoint installation package to client machines and silently install the package in the background.

Linux

After you have upgraded the Data Security Management Server and all supplemental Data Security servers:

1. Select **Start > Programs > Websense > Data Security > Endpoint Package Builder** on the management server to launch the endpoint client package builder.
2. Choose Linux when prompted.
3. To upgrade Data Endpoint software on a Linux computer, copy the correct installer to the machine and run it as root.

- **LinuxEndpoint_SFX_installer_el5** - should be used with Red Hat Enterprise Linux version 5.x.

No reboot is necessary. The endpoint software starts automatically. You can install v7.7.x on top of earlier versions without uninstalling and re-installing them.

Mac

After you have upgraded the Data Security Management Server and all supplemental Data Security servers:

1. Select **Start > Programs > Websense > Data Security > Endpoint Package Builder** on the management server to launch the endpoint client package builder.
2. Unzip the WebsenseEndpoint.zip package onto your Mac systems.
3. Run the WebsenseEndpoint.pkg from the unzipped folder WebsenseEndpoint.
4. Follow the steps in the installation wizard.
5. End users may be prompted to log out and re-log on to their desktops.

See Installing and Deploying the Data Endpoint or more information.