Migrating from v7.5.x to v7.8.x

Websense® Data Security

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

Published 2010

Printed in the United States and Ireland

Contents

1 Overview

If you are running Websense Data Security v7.5.x and you want to upgrade it to v7.8.x, you must take a few interim steps first. You cannot upgrade directly to v7.8.x.

Before you can upgrade to v7.8.x, you must migrate to v7.6.0 and then upgrade v7.7.2.

The required upgrade path is as follows:

7.5.x > 7.6.0 > 7.7.2 > 7.8.x

Perform the upgrade in the order described and make sure you upgrade the entire system for one version, and it is running, before upgrading to another.

The sequence is critical, because if you upgrade components out of order, they stop communicating.

This guide describes how to upgrade stand-alone installations of Websense Data Security from various versions 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.

2 Migrating Data Security from v7.5.x to v7.6.0

To migrate your system to Data Security v7.6.0, perform the following steps in order.

1. *Migrating the Data Security Management Server*, page 5
2. *Upgrade any supplemental Data Security servers and standalone agents*, page 16
3. *Upgrade the protector*, page 17
4. *Upgrade Content Gateway*, page 18
5. *Upgrade endpoints*, page 18
6. *Notes and Exceptions*, page 19

Exceptions

- Version 7.6 has a new permission structure. When upgrading, roles are reset to support the new structure.
- Exchange Agent is no longer supported in version 7.6. Upon upgrade, it is removed.
- If the SMTP agent was installed previously on the Data Security Management Server, it will no longer be present if you upgrade the Data Security Management Server to a Windows 2008 R2 or Windows Server 2012 machine.
- The Traffic Log screen may display the following actions incorrectly for version 7.5 traffic:
  - Block
  - Encrypt
  - Endpoint confirm allow
  - Endpoint confirm denied
- If you choose to use SQL Server 2008 R2 Express to store Data Security data, only the 4 most recent partitions will be online. All other partitions are archived.

See *Notes and Exceptions*, page 19, for full details.

Preparing for migration

Redirect traffic

Prior to upgrading Data Security (Suite) to version 7.6, it is a best practice to redirect traffic to not be monitored by Data Security (Suite).

- Re-route email traffic so exchange servers send email directly, rather than through Data Security agents or protectors.
- Bypass any inline protectors.
- Disable the ISA Agent if installed on an ISA Server machine.

If you are running Data Security in monitoring only mode, it is not necessary to redirect traffic.

Decide on TRITON management server location

Starting with v7.6, management of a Websense deployment is concentrated on one machine, the TRITON management server. All management interfaces (Web Security, Data Security, and Email Security) and components run on this machine.

In v7.8.x, the TRITON management server must be running on one of the following operating system environments:

- Windows Server 2008 (64-bit) Standard or Enterprise R2
- Windows Server 2012 (64-bit)

With a remote (standard or enterprise) reporting database, the management server must meet the following hardware requirements for stand-alone Data Security installations.

Server hardware	Recommended
CPU	4 CPU cores (2.5 GHz)
Memory	8 GB
Disk space	140 GB

With local (express) reporting database, it must meet the following hardware:

Server hardware	Recommended
CPU	4 CPU cores (2.5 GHz)
Memory	8 GB
Disk space	240 GB

Before beginning, obtain a machine meeting these operating system and hardware requirements.

Install SQL Server

For the most common deployments, Microsoft SQL Server must be installed and operational somewhere in your network before you can upgrade to Data Security 7.6. Starting with v7.6, the system uses SQL Server instead of Oracle Database to store and maintain Data Security data.

- For evaluations and small deployments, the TRITON Unified Installer can be used to install Microsoft SQL Server 2008 R2 Express on the TRITON management server machine.

  If you will use SQL Express, it is not necessary to install it before upgrading. You can choose to install it during installation.

  If you want to install SQL Server Express on a machine separate from the management server, be sure install it prior to upgrading Data Security.

- Larger organizations are advised to use Microsoft SQL Server Standard or Enterprise. These SQL Server editions cannot reside on the TRITON management server.

  If you will be using one of these database versions, be sure to install it before performing the upgrade.

  SQL Server clustering may be used with all supported standard and enterprise versions of Microsoft SQL Server for failover or high availability.

The supported database engines are:

- SQL Server 2008

  All editions except Web, Express, and Compact; all service packs, 32- and 64-bit, but not IA64.

- SQL Server 2008 R2 Express (installed by the TRITON Unified Installer)
- SQL Server 2008 R2

  All editions except Web and Compact; all service packs, 32- and 64-bit, but not IA64.

- SQL Server 2012

If you have an earlier version of SQL Server on the management server, remove it before proceeding.

Migrating the Data Security Management Server

Complete these instructions to upgrade a Data Security Management Server from version 7.5 to 7.6.

The following process is different from a fresh install; it describes how to migrate incidents, reports, and more from your existing system to the new one.

Before you begin

1. Make sure your current Data Security deployment has hotfixes applied for its version. You must update Data Security 7.5.x to 7.5.9 prior to upgrade to 7.6.
2. Check the System Health screen to make sure your system is functioning properly. If you suspect it is not, please contact Websense Technical Support before proceeding.
3. Perform a full backup of the machine. See 7.5 TRITON - Data Security Help for information on backing up Data Security data.
4. Relocate your forensics data.

> **Note**
> If your forensics repository is large (more than approximately 3 GB) upgrading Data Security can take a very long time. It is strongly recommended you relocate forensics data prior to using the export tool described in this procedure and then copy the data back to the appropriate location after upgrading. It is a best practice to relocate forensics a day prior to upgrading Data Security to allow sufficient time to complete this task.

> **Warning**
> If you have archived partitions, you *must* relocate forensics prior to using the upgrade export tool. Otherwise, the archived partitions will not be available in the upgraded system.

Note: in the following steps, the Websense folder is typically C:\Program Files\Websense.

a. Stop the DSS watchdog service:
   i. Select **Start > Programs > Accessories > Scheduled tasks**.
   ii. Right-click **DSS Watchdog** and select **Properties**.
   iii. De-select **Enabled**.
   iv. Click **OK**.
b. In the Windows Services console, stop the **Websense DSS Manager** service.
   Alternatively, issue the command `net stop tomcat6` in a Command Prompt.
c. Rename **Websense\Data Security\forensics_repository\data** to **Websense\Data Security\forensics_repository\oldData**
d. Create a new folder named **Websense\Data Security\forensics_repository\data**
e. Create a new folder named **Websense\Data Security\archive_mng\oldStorage**

f. Move all folders starting with **FR-ARC-**
from **Websense\Data Security\archive_mng\storage**
to **Websense\Data Security\archive_mng\oldStorage**

g. In the Windows Services console, start the **Websense DSS Manager** service.

Alternatively, issue the command **net start tomcat6** in a Command Prompt.

h. Move or copy the following folder to a location outside the Websense folder:
Websense\Data Security\forensics_repository\oldData

i. Search the **oldData** folder for files with the name **`*.ser`** and delete those files.

j. Move or copy all folders starting with **`FR-ARC-`**
from **Websense\Data Security\archive_mng\oldStorage**
to a location outside the Websense folder

Run the upgrade export tool

1. Download and extract the Data Security Export Tool v7.6, **WebsenseDataSecurityUpgradeExportTool.zip**, from www.mywebsense.com. Select the product Websense Data Security Suite and the version 7.6.0.
2. Copy the upgrade_export_tool folder to a temporary folder on the Data Security Management Server (this folder is referred to as the *export tool folder* in the rest of these instructions).

   Copy to a location outside the Websense folder (typically, C:\Program Files\Websense) for example C:\temp\upgrade_export_tool.
3. Run the export script:

Important

Data Security 7.5 will continue to operate, but new data generated after running the export tool will not be imported to Data Security 7.6.

Note

Prior to running the export script, see *Estimating export data size*, page 19 to estimate the amount of data that will be generated.

a. Open a command prompt.

b. From the export tool folder, enter the following command:

```
python export.py
```

Note the above command generates export data in %dss_home%/archive_mng/export-data. You can specify a different location by specifying a path in the command:

```
python export.py <path>
```

where <path> is local; it cannot be a network path or a location on a mapped network drive. If you specify <path>, substitute it for %dss_home%/archive/mng/export-data in the remaining steps below.

c. Wait for the script to complete.

Depending on the amount of data, this process may take a long time.

Important

If the script fails, do *not* run it again (running it again may corrupt the data). Contact Websense Technical Support before proceeding.

4. Check the following files for any errors:
   - dbexport.log (in export tool folder you created in step 2, for example C:\temp\upgrade_export_tool)
   - db.log (in export tool folder you created in step 2, for example C:\temp\upgrade_export_tool)
   - %dss_home%/archive/mng/export-data/DataExport.log

   If you find errors, contact Websense Technical Support.
5. If you provided an alternate path in step 8b, skip to step 10. Otherwise, move the data exported by the export script to the target machine (i.e., the one to which you want to upgrade Data Security Management Server).

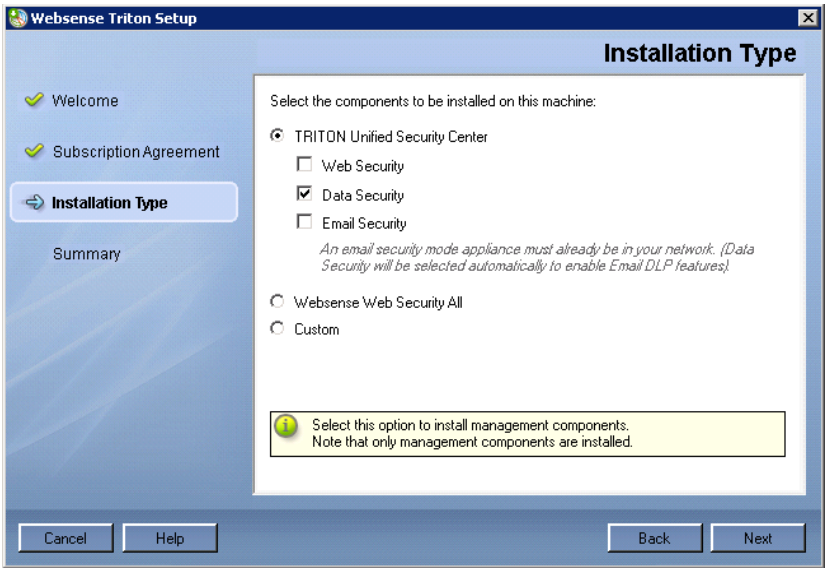
   The exported data is located in %dss_home%/archive_mng/export-data.

   Note the export-data folder should contain the following (if it does not, try running the export script again; see step 3).
   - Certs (folder)
   - DSS_FILES (folder)
   - Forensics_repository (folder)
   - OldPolicyXMLs (folder)
   - Onlinetables (folder)
   - Partitiontables (folder)
   - **Backup.txt** (this file is required when restoring data to the upgraded system)
   - Dataexport.log
   - Crawlers (folder)
   - Policies_backup (folder)
   - PreciseID_DB (folder)
   - RunCommands (folder; only present if you had *remediation script* resources)
   - Ep-profile-keys.zip
   - Subscription.xml
   - Wbsn-pairing-map.txt

Install the TRITON infrastructure

On the target machine (i.e., the one to which you want to upgrade Data Security Management Server), install the TRITON management server software.

1. Download the Websense installer, **WebsenseTRITON76Setup.exe**, from www.mywebsense.com. Select the product Websense Data Security Suite and the version 7.6.0.
2. Download the **TRITON Console System Requirements Tool** found in the same are of MyWebsense and run it to ensure your system is prepared for installation.
3. Launch the Websense installer. A progress dialog box appears, as files are extracted.
4. On the Welcome screen, click **Start**.
5. On the Subscription Agreement screen, select **I accept this agreement** and then click **Next**.
6. On the **Installation Type** screen, be sure to select **Data Security** (under TRITON Unified Security Center). Note that you can install the other modules if you want, but TRITON - Data Security is the only one necessary for a Data Security deployment.



7. On the **Summary** screen, click **Next** to continue the installation. TRITON Infrastructure Setup launches.
8. On the **Installation Directory** screen, specify the location where you want TRITON Infrastructure to be installed and then click **Next**.

> **Important**
> The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

To accept the default location (recommended), simply click **Next**. By default the installation directory is C:\Program Files\Websense\ (32-bit machines) or C:\Program Files (x86)\Websense\ (64-bit machines).

To specify a different location, use the **Browse** button.

9. On the **SQL Server** screen, specify the location of your database engine and how you want to connect to it.

   The information you enter on this screen will be used by the Web, Data, and Email security component installers as well. The Web, Data, and Email modules of the TRITON Unified Security Center will use the database and credentials you specify here to store and retrieve their data. The Web security component installer will allow you to override this database and credential information, and specify a different database. The Data and Email security component installers will not; they will use what is specified here during TRITON Infrastructure installation.

   - **Install SQL Server Express on this machine**: Select this option to install SQL Server 2008 R2 Express on this machine. TRITON Unified Security Center will use this database engine for Websense logging data.

     The Websense installer will automatically install .NET 3.5 SP1, Powershell 1.0, and Windows Installer 4.5 if not found on the machine. These are required for SQL Server 2008 R2 Express.

     A default database instance, named mssqlserver, will be created. If a database instance named mssqlserver already exists on this machine (for example, if MSDE is installed on this machine), then an instance named TRITONSQL2K8R2X is created instead.

     If you are installing TRITON Infrastructure as part of an upgrade process from prior-version Web Security, you may have to stop Filtering Service now. If .NET 3.5 SP1 is not found on this machine, the installer needs access to windowsupdate.microsoft.com. If Filtering Service blocks this machine from accessing windowsupdate.microsoft.com SQL Server Express cannot be installed.

   - **Use existing SQL Server on another machine**: Select this option to specify the location and connection credentials for a database server located elsewhere in the network.
   - **Server Name**: Enter the hostname or IP address of the SQL Server machine. To use a SQL Server instance, other than the default, specify it here. Note that the instance you want to use must already exist. Refer to Microsoft documentation for information about creating instances.

   After selecting one of the above options (for installing SQL Server Express or using existing SQL Server) specify an authentication method, and user name and password; see below.

   - **Authentication**: Select how Websense components on this machine should connect to the database engine. Select SQL Server Authentication to connect using a SQL Server account. Select Windows Authentication to connect using a Windows trusted connection.

- **User Name**: If you are installing SQL Server Express on this machine, a user name of *sa* is automatically specified (this is the default system administrator account); enter the password you want for *sa*. This account must be configured to have system administrator rights in SQL Server.

  Otherwise, the currently logged in user that launched the Websense installer is taken as the Windows account to use to connect to SQL Server when Windows authentication is chosen. This account must have certain roles assigned. See *Roles*, page 20.

  You cannot specify a different account in the SQL Server screen when installing TRITON Infrastructure. If you want to use a different account, cancel the installation. Log onto the machine as the user you want used for SQL Server Windows authentication and then restart the Websense installer.

  In some organizations, policies are in place where service accounts (i.e., accounts used to run Windows services) cannot be interactive (i.e., used by a user for general login) and interactive accounts cannot be used to run services. In such a case, if possible, allow a service account to be interactive for the duration of installing Websense products. Log onto the machine with the service account, so services are properly installed to run as a service user, and then revoke the interactivity for that account after installation is complete.

- **Password**: Enter the password for the specified account. If you chose to install SQL Server Express on this machine, confirm the password.

When you click **Next**, connection to the database engine is verified if you chose to use an existing SQL Server installation on another machine. If the connection test is successful, the next installer screen appears.

If the test is unsuccessful, the following message appears:

Unable to connect to SQL
Make sure the SQL Server you specified is currently running. If it is running, verify the access credentials you supplied.

Click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

10. On the **Server & Credentials** screen, select the IP address of this machine and specify network credentials to be used by TRITON Unified Security Center.

    - **IP Address**: Select an IP address for this machine. If this machine has a single network interface card (NIC) then only one address will be listed.

      The IP address selected here is the one to use when accessing the TRITON Unified Security Center (via Web browser). This is also the IP address you should specify to any Websense component needing connection to the TRITON Unified Security Center machine.

      If you chose to install SQL Server 2008 R2 Express, when installing Web Security Log Server or Email Security Log Server on another machine, specify this IP address for the database engine location.

- **Server/Domain**: Specify the server or domain of the user account to use be used by TRITON Infrastructure and TRITON Unified Security Center. By default, this field is filled with the server/domain of the account you logged into this machine with. If you want to specify a different account, be sure to use the Browse button.
- **User Name**: Specify the user name of the account to be used by TRITON Unified Security Center. By default, this field is filled with the user name of the account you logged into this machine with. If you want to specify a different account, be sure to use the Browse button.

  Important

  Account names must include only ASCII characters– i.e. English-based letters, numbers and some special characters such as # and &.

- **Password**: Enter the password for the specified account.

11. On the **admin Account** screen, enter an email address and password for the default administration account for TRITON Unified Security Center, and then click **Next**.

    Administrator accounts in TRITON Unified Security Center must have an email address. System notification and password reset information is sent to this address (only after SMTP configuration is done; see next step).

    It is a best practice to use a strong password as described on-screen.

12. On the **Email Settings** screen, enter information about the SMTP server to be used for system notifications and then click **Next**. Note that this is optional, you can configure these settings after installation in the TRITON Unified Security Center. If you do not want to configure these settings now, clear the **Configure email settings** check box and then click **Next**.

    Important

    If you do not configure an SMTP server now and you lose the **admin** account password (set on previous screen) before logging into TRITON Unified Security Center and configuring an SMTP server, the *Forgot my password* link on the login page will not provide password recovery information. SMTP server configuration must be completed before password recovery email can be sent by the system.

    - **IP address or hostname**: IP address or host name of the SMTP server through which email alerts should be sent. In most cases, the default Port (25) should be used. If the specified SMTP server is configured to use a different port, enter it here.
    - **Sender email address**: Originator email address appearing in notification email.

- **Sender name**: Optional descriptive name that can appear in notification email. This is can help recipients identify this as a notification email from the TRITON Unified Security Center.

13. On the **Pre-Installation Summary** screen, verify the information and then click **Next** to begin the installation.

    Important

    If you chose to install SQL Server Express, depending on whether certain Windows prerequisites are installed, your machine may be automatically restarted up to two times during the installation process. Restarts are not required if the prerequisites are already installed.

    Note

    When you click **Next**, if you chose to install SQL Server Express on this machine, it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

14. If you chose to install SQL Server Express, .NET Framework 3.5 SP1, PowerShell 1.0, and Windows Installer 4.5 will be installed if not already present. Wait for Windows to configure components.

    a. If the following message appears during this process, click **OK**:

    Setup could not restart the machine. Possible causes are insufficient privileges, or an application rejected the restart. Please restart the machine manually and setup will restart.

    b. A software update installation wizard completion screen may appear for Hotfix for Windows Server 2003 (KB942288-v4). This is for Windows Installer 4.5. The machine must be restarted. Click Finish to restart now (do not select Do not restart now). Note that it may take approximately 1 minute for the restart to occur. Wait for the restart.

    - If you are upgrading prior-version Web Security or Data Security the following message appears after restart. Click OK.

      An older version of Web Security (or *Data Security*) *is installed on this machine.*
      Press OK to upgrade it or Cancel to exit the installation.

    - If TRITON - Web Security is installed on this machine, the following message appears. Click Yes.

Keep TRITON - Web Security on this machine and upgrade it to version 7.6 TRITON Unified Security Center?
Selecting No will launch the current-version uninstaller. Uninstall the current-version TRITON - Web Security. After uninstall, remaining components will be upgraded to version 7.6.

c. Websense installer starts again. In the TRITON Infrastructure Setup Welcome screen, click **Next**.

d. The Ready to Resume EIP Infra installation screen appears. Click **Next**.

> **Note**
> When you click **Next**, if you chose to install SQL Server it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

15. If you chose to install SQL Server Express on this machine, SQL Server 2008 R2 Setup is launched. Wait for it to complete.

    The Setup Support Files screen appears and then an Installation Progress screen appears. Wait for these screens to complete automatically. It is not necessary to click or select anything in these screens.

    Note that it may take approximately 10-15 minutes for the SQL Server 2008 R2 Express installation to complete.

16. Next, the Installation screen appears. Wait until all files have been installed.

    If the following message appears, check whether port 9443 is already in use on this machine:

    Error 1920. Server 'Websense TRITON Central Access' (EIPManagerProxy) failed to start. Verify that you have sufficient privileges to start system services.

    If port 9443 is in use, release it and then click Retry to continue installation.

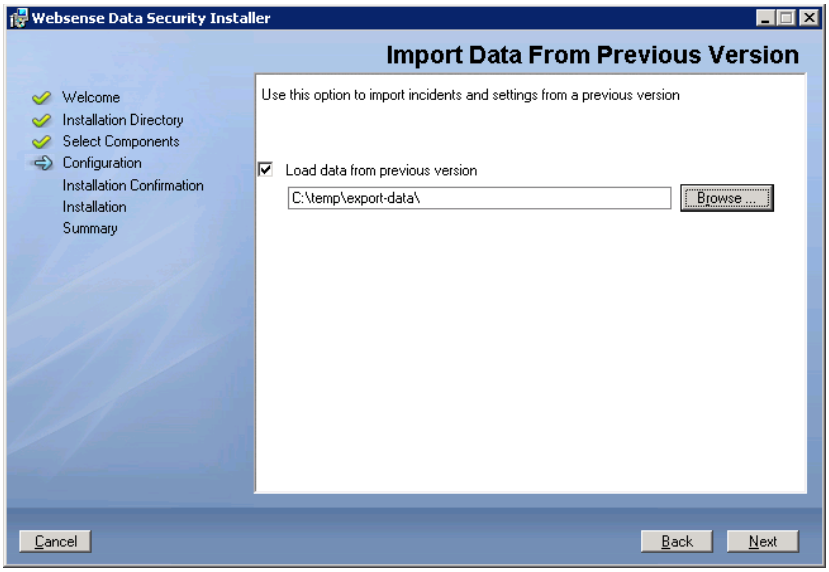
17. On the Installation Complete screen, click **Finish**.

> **Important**
> If you chose to install SQL Server Express, open the Windows Services console **before** clicking Finish (leave the the Websense installer running). In the Services console, make sure the SQL Server (MSSQLSERVER) service is enabled as automatic or manual, and then start it if it is not running.

Install Data Security

1. When you click Finish in TRITON Infrastructure Setup, the Data Security installer appears.

a. When the Data Security installer appears, on the **Import Data From Previous Version** screen, select the **Load Data From Backup** check box and then use the **Browse** button to select the location of the data exported by the export script.



2. If you meet one or more of the following conditions prior to upgrade, run the SQL script, <name> located in the /<name> directory.
   - You have more than one protector
   - You have more than one ISA/TMG agent
   - You have a Web Content Gateway agent
3. Log on to the version 7.6 TRITON Unified Security Center (on the TRITON management server you just created):
   a. Verify system settings, configuration, and modules.
   b. Click **Deploy**.

   Note that at this point the system is functional. However, if you relocated forensics data prior to upgrade, it is not present yet. You will restore this data in the next step.

Post installation

If you relocated forensics data prior to upgrade:

1. Copy the contents of **oldData** (from the location outside the Websense folder, on the old machine) to **Websense\Data Security\forensics_repository\data** on this machine (note: copy the contents and not the folder itself).
2. Copy all content moved from **Websense\Data Security\archive_mng\oldStorage** on the old machine to **Websense\Data Security\archive_mng\storage** on this machine.

3. Upgrade all other Data Security components to v7.6.0 before proceeding with the upgrade to v7.7.2.

Upgrade any supplemental Data Security servers and standalone agents

Complete these steps to upgrade a supplement Data Security server or standalone agent (e.g. SMTP, printer, discovery/crawler, ISA/TMG) to v7.6.0.

Always upgrade the Data Security Management Server **before** upgrading agents.

For best practice, upgrade the management server without changing the operating system version of supplemental machines, then perform system modifications as required.

Important

If you are upgrading a Data Security server or agent to a new Windows 2008 machine, be sure to keep the original IP address/hostname if you want to retain settings and information from the original server. This is especially important on machines where a v7.5 crawler was installed and had a fingerprinting classifier assigned to it. Using the same IP address prevents fingerprints from being lost.

You do not need to delete fingerprint tasks before upgrading Data Security servers.

1. Download the Websense installer, **WebsenseTRITON76Setup.exe**, from www.mywebsense.com. Select the product Websense Data Security Suite and the version 7.6.0.
2. Launch the Websense installer. A progress dialog box appears, as files are extracted.
3. The **Installer Dashboard** appears. Any version 7.5 Data Security components found on this machine are upgraded to version 7.6.
4. 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
   - Endpoints not receiving updated profiles
   - File-system discovery starts but immediately indicates "completed with errors"

Upgrade the protector

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 TRITON - Data Security.

Complete the following steps to upgrade a Data Security Protector from version 7.5 to version 7.6.

Important

Upgrade the Data Security Management Server **before** upgrading Protectors.

1. Obtain the protector update file (protector-update-7.6.0) from www.mywebsense.com and place it in a temporary directory (for example, in /tmp/).Allow read/write/execute by all on the update file, for example:

   ```
   chmod 777 /tmp/protector-update-7.6.0
   ```

2. Start the upgrade, for example:

   ```
   /tmp/protector-update-7.6.0
   ```

3. When the upgrade script is finished, reboot the machine.
4. If, when upgrading Data Security Management Server, you moved management functions to a different machine (i.e., created a TRITON management server on a different machine), reregister Protector with the new TRITON management server:

   ```
   wizard securecomm
   ```

   Note

   Even if you did not move management functions to a different machine, reregister Protector if you changed the domain membership or IP address of the Data Security Management Server machine.

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

   When you upgrade a Data Security server or 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:

- Potential false positives and negatives
- Endpoints not receiving updated profiles
- File-system discovery starts but immediately indicates "completed with errors"
- Endpoints not receiving updated profiles
- File-system discovery starts but immediately indicates “completed with errors”

Upgrade Content Gateway

If you are a Web Security Gateway customer, be sure to upgrade Content Gateway v7.5 to v7.6, and then re-register it with the Data Security Management Server. Refer to the Content Gateway documentation.

Upgrade endpoints

First upgrade the Data Security Management Server and any supplemental Data Security servers. Then upgrade Data Security endpoints. Upgrade endpoints by deploying the 7.6 version of them to their current locations. See Deploying Websense Endpoints.

Important

At the completion of any endpoint update, you must restart the endpoint for the updates to take effect.

It is possible that some endpoints are not connected to the network or are unavailable for upgrade for some other reason. These endpoints will continue to function and be able to identify breaches and create incidents. They will operate according to the last policy applied to it.

In version 7.6, you can configure prior-version endpoints to operate in monitoring mode until they are updated. In this mode, the endpoints only audit actions and do not block.

Note

A prior-version endpoint configured to block printscreen actions will continue to block that action even if you set it to monitoring mode in version 7.6.

Incidents from prior-version endpoints will continue to be accepted by upgraded Data Security Management and supplemental servers.

Data Security Management Server is upgraded to be part of the version 7.6 TRITON Unified Security Center. Note that during upgrade, if there are multiple network interfaces on the machine, you can choose a different IP address than that currently used. If you do so, endpoint clients configured to connect to endpoint servers on this machine will no longer be using the correct IP address. A solution to this situation is create a version 7.6 Data Security supplemental server using the old IP address so endpoint clients can still connect to it and (optionally) remove it after the endpoints have been updated to version 7.6 (connecting to the new IP address).

Notes and Exceptions

Applies to:	In this topic:
◆ Data Security, v7.5.x, 7.6.x	◆ *Estimating export data size*, page 19 ◆ *Traffic Log screen*, page 20 ◆ *SQL Server 2008 R2 Express*, page 20 ◆ *Roles*, page 20 ◆ *New security certificate*, page 21 ◆ *Excel Fingerprints*, page 21 ◆ *SMTP Agent not supported on Windows 2008 R2*, page 21 ◆ *SMTP Agent not supported on Windows 2008 R2*, page 21 ◆ *Exchange Agent deprecated*, page 21

Estimating export data size

Use the following guidelines to estimate the amount of data that will be generated by the upgrade export tool (i.e., export.py script).

Incident metadata

Data in Motion: 1 GB exported data per 350,000 incidents.

Data at Rest: 1 GB exported data per 100,000 incidents.

Incident forensics

Exported data for forensics is equal to the size of the forensics data itself.

Important
If current forensics data is more than 3 GB, it should be located outside the Websense folder as directed in the upgrade instructions. Otherwise the upgrade export process can take a very long time.

Resources and configuration

Total exported data approximately 0.5 GB, broken down as follows:

- 0.2 GB for Resource Repository
- 0.1 for other management data
- 0.2 for predefined policies

Fingerprint and discovery

Export data is equal to the sum of the following:

- %dss_home%\DiscoveryJobs
- PreciseID database folder (%dss_home%\PreciseID DB by default)
- Sum of *Endpoint package size* of all *PreciseID File* classifiers (typically, under 1 GB)

Traffic Log screen

After upgrading to v7.6.0, the Traffic Log screen may display the following actions incorrectly for version 7.5 traffic:

- Block
- Encrypt
- Endpoint confirm allow
- Endpoint confirm denied

SQL Server 2008 R2 Express

If you choose to use SQL Server 2008 R2 Express to store Data Security data, only the 4 most recent partitions will be online. All other partitions are archived.

Roles

Version 7.6 has a new permission structure. When upgrading, 7roles are reset to support the new structure.

New security certificate

After upgrade, you must install or permanently accept a new security certificate issued by Websense, Inc. to avoid seeing a certificate error when you first launch TRITON Unified Security Center. The prior-version certificate (accepted when accessing TRITON - Web Security or TRITON - Data Security) is no longer valid.

An SSL connection is used for secure, browser-based communication with TRITON Unified Security Center. This connection uses a security certificate issued by Websense, Inc. Because the supported browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch TRITON Unified Security Center from a new browser. To avoid seeing this error, you can install or permanently accept the certificate within the browser. See the *Websense Knowledge Base* for instructions.

Excel Fingerprints

When upgrading from version 7.5, incorrect fingerprints of Excel files remain. Prior versions of Data Security had a issue when extracting text out of numeric cells in Excel documents. Only the first (most significant) 15-digits of any numeric cell would be fingerprinted.

Although this issue has been resolved in version 7.6, Excel files fingerprinted in previous versions may not be caught by version 7.6 if they contain many numeric fields with more than 15 digits.

Re-fingerprint the relevant files (delete the document fingerprints and start another fingerprinting scan). This assumes that the fingerprinted files still exist on the file servers (or SharePoint server) to be re-fingerprinted.

SMTP Agent not supported on Windows 2008 R2

If SMTP agent was installed on the version 7.5 Data Security Management Server, it will no longer be present if you upgrade the Data Security Management Server to a Windows 2008 R2 machine.

Exchange Agent deprecated

Exchange Agent is no longer supported in version 7.6. Upon upgrade, it will not be upgraded, but instead removed.

3 Upgrading Data Security from v7.6.0 to v7.7.2

To upgrade your machine from v7.6.0 to v7.7.2, perform the following steps, in order:

1. *Upgrade the Data Security Management Server*, page 23
2. *Upgrade any supplemental Data Security servers and standalone agents*, page 27
3. *Upgrade protectors and mobile agents*, page 28
4. *Upgrade endpoints*, page 29

Upgrade the Data Security Management Server

You upgrade your management server using the TRITON installation package, **WebsenseTRITON772Setup.exe**. 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 7.6.0 system is functional prior to upgrade.
- Make sure your base version is 7.6.0.
- Perform a full backup of your 7.6.0 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.
- If you use regulatory and compliance attributes in your quick policies, make a note of the laws that you enforce. You will need to re-configure these settings after upgrade.

  a. Select **Main > Policy Management > DLP Policies**.

  b. One by one, open your quick policies—Web DLP, email DLP, and mobile DLP.

  c. Make note of the regulatory and compliance attributes. For Web and mobile DLP, this attribute is on the Attributes tab. For email DLP it is on the Outbound and Inbound tabs.

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 v7.7.2 TRITON unified installer (Windows only): **WebsenseTRITON772Setup.exe**, available from:

www.websense.com/MyWebsense/Downloads/

Select **Data Security**, **version** (7.7.2), and **operating system** (Windows), then click **download** next to the installer description. Do not select version 7.7.3 even though it's newer.

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.

> **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. If you have Web Security as well as Data Security:
   a. Select **Settings > Deployment > System Modules**.
   b. Listed are 2 instances of each Web Content Gateway module that is registered with the system. Delete the older instances. You can identify these by looking at the version number that is displayed.
5. If you use regulatory and compliance attributes in your quick policies, do the following to restore your settings.
   a. Select **Main > Policy Management > DLP Policies**.
   b. One by one, open your quick policies—Web DLP, email DLP, and mobile DLP.
   c. Select the regulatory and compliance attribute. For Web and mobile DLP, this attribute is on the Attributes tab. For email DLP it is on the Outbound and Inbound tabs.
   d. Select the laws to enforce. You wrote these down before starting the upgrade.
6. Click **Deploy**.

Upgrade any supplemental Data Security servers and standalone agents

Complete these steps to upgrade a supplemental Data Security server or stand-alone agent (e.g. SMTP, printer, crawler, or ISA/TMG) from v7.6.0 to v7.7.2.

1. On the machine hosting the server or agent software, launch the installer, **WebsenseTRITON772Setup.exe**. The software is detected, and the upgrade wizard appears.
2. Click **Next** until you complete the wizard.

   Any v7.6.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**.
4. 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 v7.6.0 to v7.7.2.

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 TRITON - Data Security.

1. Download the protector update script from the v7.7.2 product area of www.websense.com/MyWebsense/Downloads/.
2. Copy the update file, protector-update-7.7.0-060, into the directory `/tmp`.
3. Enter the command:

   ```
   chmod +x /tmp/protector-update-7.7.0-060
   ```

4. If you are upgrading from v7.6.8, log on as root and run the following command:

   ```
   rm -r /var/tmp/yum_update_cache
   ```

5. Run the following command:

   ```
   bash /tmp/protector-update-7.7.0-060
   ```

6. Answer **Y** on the "Are you sure?" question, and complete the wizard, accepting the defaults.
7. Restart the protector or mobile agent machine when the wizard completes.
8. 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".
9. 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
   ```

10. If you are upgrading from v7.6.8, run the following command:

    ```
    rm -r /var/tmp/yum_update_cache
    ```

11. In the Data Security manager, click **Deploy**.
12. 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

Before upgrading endpoint clients, do the following:

1. Disable all discovery tasks so that they don't run during the upgrade process.
2. Wait until there are no new endpoint discovery incidents appearing in the Data Security incidents report.

You can install endpoint packages on top of earlier versions without uninstalling and re-installing them.

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 v7.7.2 package to each endpoint using GPO, SMS, or a similar deployment method. You can install v7.7.2 on top of earlier versions without uninstalling and re-installing them.
4. Restart the endpoint after installation is complete.

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_el4** - should be used with Red Hat Enterprise Linux version 4.x.
   - **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 v7.7.2 on top of earlier versions without uninstalling and re-installing them.

4 Upgrading Data Security from v7.7.2 to v7.8.x

To upgrade your machine from v7.7.2 to v7.8.x, perform the following steps, in order:

1. *Upgrade the Data Security Management Server*, page 31
2. *Upgrade any supplemental Data Security servers and standalone agents*, page 35
3. *Upgrade protectors and mobile agents*, page 36
4. *Upgrade endpoints*, page 37

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. As before, perform the upgrade in the order described. The sequence is critical.

Preparing for upgrade

- Unless instructed otherwise by Websense Technical Support, ensure your system is functional prior to upgrade.
- Make sure your base version is 7.7.2.
- Perform a full backup of your 7.7.2 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): **WebsenseTRITON78*x*Setup.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.

Note

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

TRITON Infrastructure

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.
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.

Wizard Screen	Fields
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 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.

Upgrade protectors and mobile agents

Do the following to upgrade your protector or mobile agent from v7.7.2 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 TRITON - Data Security.

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.
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.

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.

See Installing and Deploying the Data Endpoint or more information.