Upgrading Email Security Gateway v7.7.x to v7.8.0

These instructions cover the upgrade of a Websense Email Security Gateway solution from version 7.7.x to version 7.8.0.

If you are currently running a version 7.6.x deployment, and you want to upgrade to version 7.7.3 or 7.8.0, you must upgrade to version 7.7.0 first, and then upgrade to version 7.7.3 or 7.8.0. See Upgrading Email Security Gateway v7.6.x to v7.7.0 for procedures.

If you are currently running a version 7.7.x deployment, you can upgrade directly to version 7.8.0. If you want to upgrade to version 7.8.2, 7.8.3, or 7.8.4, you must upgrade to version 7.8.0 first, and then upgrade directly to those versions. See Upgrading Email Security Gateway v7.8.0 to v7.8.x for those instructions.

See Upgrading Email Security Gateway Solutions for specific upgrade paths.

> **Important**
>
> This upgrade includes the following Email Security and Data Security issues:
>
> ◆ Email Security database format conversion task is performed on database partitions. The majority of the conversion is performed after the upgrade is complete and must be completed before any subsequent product upgrades.
>
> ◆ Data Security policy and content classifier update may not complete.
>
> **Please read and follow all upgrade preparation and instruction steps carefully, and perform all post-upgrade tasks to mitigate these issues.**

The upgrade process includes a Websense V-Series appliance component, along with TRITON Unified Security Center and Email Security Log Server Windows components.

You should ensure that third-party components are upgraded as well, if necessary, to work with the new Email Security Gateway version.

See Upgrading Email Security Gateway Solutions for important information about backing up your system before you upgrade.

> ⚠️ **Warning**
> If any Websense personnel have performed nonstandard customizations to any Email Security Gateway configuration setting, please contact Websense Technical Support before you begin the upgrade process. Some customizations may be lost during the upgrade process.

Contents:

◆ *Upgrade preparation*
◆ *Upgrade instructions*
◆ *Post-upgrade activities*

Upgrade preparation

Several issues should be considered before you begin an Email Security Gateway product upgrade.

◆ **Verify current deployment.** Ensure that your current deployment is functioning properly, including any third-party integration components, before you begin the upgrade. The upgrade process does not repair a non-functioning system.

◆ **Verify the system requirements** for the version to which you are upgrading to ensure your network can accommodate the new features and functions. See System requirements for this version for a detailed description.

◆ **Prepare Windows components.** See All Websense TRITON solutions for an explanation of general preparations for upgrading Email Security Gateway Windows components.

◆ **Ensure that your firewall is configured correctly** so that the ports needed for proper Email Security Gateway operation are open. See Email Security Gateway ports for information about all Email Security Gateway default ports, including appliance interface designations and communication direction.

◆ **Check configuration settings for maximum capacity.** If Websense Technical Support has modified any configuration setting to exceed its default maximum capacity, please contact Technical Support for assistance before you begin the upgrade process.

The upgrade from version 7.7.x to 7.8.0 adds some default components. If you know your version 7.7.x Email Security Gateway system is at maximum capacity for the following components, you should remove at least 1 item before performing the upgrade to version 7.8.0:

- Filters: maximum is 32 (**Main > Policy Management > Filters**)
- Filter actions: maximum is 32 (**Main > Policy Management > Actions**)
- IP groups: maximum is 128 (**Settings > Inbound/Outbound > IP Groups**)

◆ **Perform database partition inventory.** The upgrade from version 7.7.x to 7.8.0 includes a data conversion task. All version 7.7.x data will be converted during scheduled tasks after the upgrade. These tasks may take a few hours, depending on the number and size of partitions. Consider whether you can remove any partitions to mitigate the impact of the data conversion process.

◆ **Backup and remove tomcat log files and remove temporary manager files (recommended to facilitate timely TRITON console upgrade).** Use the following steps:

1. Log onto the TRITON management server.

2. Navigate to the following directory:

   C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\logs

3. Copy the logs folder to another location (for example, C:\WebsenseBackup\Email), and then delete it in the directory mentioned in step 2.

4. Navigate to the following directory:

   C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\tempEsgUploadFileTemp

5. Delete all the downloadFile* files.

Upgrade instructions

Once you have completed the activities outlined in *Upgrade preparation*, you can perform the product upgrade. This section provides instructions for performing an upgrade of an Email Security Gateway only deployment.

> ![Important]
> **Important**
> If your network includes Websense Web Security, you must upgrade the Policy Broker/Policy Server machine first, whether or not these components reside on an appliance. Other Websense services located on the Policy Broker/Policy Server machine should be upgraded at the same time. See Upgrade procedure for solutions that include Web, Email, and Data Security for more information.

Use the following procedure to perform the upgrade of Email Security Gateway:

1. Log on to the Email Security Gateway Log Server machine and navigate to the Service Control Manager (**Start > Control Panel > Administrative Tools > Services**).

2. Locate the Websense Email Security Log Server property **Startup type**, and change the setting from **Automatic** to **Disabled**.

3. In the Windows Service Control Manager, stop the Email Security Gateway Log Server service. Reboot the Log Server Windows server if possible to release any locked files.

4. Run the script **upgrade_pre_check_for_v7.8.0.sql** in the Email Security Gateway database file **esglogdb76**. See this [Websense Knowledge Base article](#) for the script file and instructions for running it.

5. Use the TRITON Enterprise upgrade installer (version 7.8.1) from the [MyWebsense](#) downloads page to upgrade the Email Security Gateway Log Server if it is installed on a machine other than the one on which the TRITON console is installed. Follow the installation wizard instructions for Log Server.

6. The installer does not allow you to change existing configuration settings. Changes must be made after the upgrade.

> **Important**
>
> If you are upgrading multiple Log Servers, you should perform the upgrades one at a time to avoid possible upgrade process errors.

7. Upgrade the TRITON console machine. Use the TRITON Enterprise upgrade installer (version 7.8.1) from the [MyWebsense](#) downloads page. Ensure that Email Security Gateway is selected for upgrade. The upgrade process includes Data Security and the Email Security Log Server if it is installed on the TRITON console machine.

Follow the installation wizard instructions. The Data Security module upgrade occurs after the TRITON infrastructure upgrade. Email Security Gateway upgrade follows Data Security.

> ⚠ **Important**
>
> The upgrade process from version 7.7.x to 7.8.0 includes a conversion task for existing database files. Any version 7.7.x data in the currently active database partition will be converted after the upgrade operation is complete. Data in other partitions will be converted during a database maintenance job scheduled for several hours after the upgrade.
>
> This job may take a few hours, depending on the number and size of the partitions.
>
> Ensure that you allow the conversion job to complete before beginning an upgrade to a later version. If the task is not complete before a subsequent upgrade, IP address information in the Message Log will be blank for messages stored in the partitions that have not yet been converted.
>
> If you do not want to wait for the later scheduled file conversion, see *Perform database conversion (optional)* for information on how to perform the conversion manually via a script file.

- The upgrade installer Configuration page shows the IP address of the database engine that manages the Email Security Log Database and logon type. If you have changed the database since your previous installation or upgrade, use this page to change these settings.

The upgrade script stops the Email Security Gateway manager service, updates the Email Security Gateway SQL Server databases (and Log Server if found), and then restarts the Email Security Gateway manager service.

> ✔ **Note**
>
> The Email Security manager is not available until after the TRITON console upgrade completes.

8. Upgrade all your V-Series appliances. Email should not be directed through these machines during the upgrade process.

    The following methods are available for an appliance upgrade:

    - USB drive recovery image (USB drive must be larger than 6 GB).

        No pre-upgrade hotfix download and installation is required.

    - Direct download to the V-Series appliance.

Appliance upgrade is performed using the Appliance Manager patch facility to download the appropriate version patch and apply it to the appliance. See the appliance upgrade guide for the appliance patch upgrade procedure.

> **!** **Important**
> Upgrade from version 7.7.x to 7.8.0 involves installing a version 7.7.x pre-upgrade hotfix and then a patch. You install the hotfix associated with your appliance version, to lay down the appropriate image for the patch to perform the upgrade.

The appliance upgrade process includes a check for

- Adequate disk space for Email Security Gateway (at least 8 GB required)
- Cached message log file size (cannot exceed 10 MB)

A backup and restore function to save existing Email Security Gateway configuration settings is also included. You are prompted to contact Websense Technical Support if any configuration file is missing.

> **✔** **Note**
> V-Series appliance services are not available while the patch is being applied and until the appliance completes its restart.

If your Email Security appliances are configured in a cluster, the primary box should be upgraded first, followed by all its secondary machines, 1 at a time. You do not need to release the appliances from the cluster in order to perform the upgrade.

Continue with *Post-upgrade activities* to deploy the Email Security Gateway upgrade.

Post-upgrade activities

Your system should have the same configuration after the upgrade process as it did before the upgrade. Any configuration changes can be made after the upgrade process is finished.

After your upgrade is completed, redirect email traffic through your system to ensure that it performs as expected.

Email hybrid service registration information is retained during the upgrade process, so you do not need to complete the registration again.

You should perform the following tasks in the TRITON console:

- *Restart Email Security Log Server service*

- *Modify Email Security Log Server Startup type property*
- *Repair Email Security Gateway registration with Data Security*
- *Update Data Security policies and classifiers*
- *Update Websense databases*
- *Review mail routing settings*
- *Enable email hybrid service commercial bulk message analysis*
- *Perform database conversion (optional)*

Restart Email Security Log Server service

Restart the Email Security Gateway Log Server service in the Windows Control Panel.

Modify Email Security Log Server Startup type property

1. Log on to the Email Security Gateway Log Server machine and navigate to the Service Control Manager (**Start > Control Panel > Administrative Tools > Services**).
2. Locate and modify the Websense Email Security Log Server property **Startup type** from **Disabled** to **Automatic**.

Repair Email Security Gateway registration with Data Security

1. In the Email Security Gateway module, navigate to **Settings > General > Data Security** and click **Unregister**.
2. Click **Register** to re-register the Email Security Gateway appliance with Data Security.
3. In the Data Security module, click **Deploy** in the upper right area of the screen.

Update Data Security policies and classifiers

1. Select the Data Security module.
2. Follow the prompts that appear for updating Data Security policies and classifiers.

   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.
3. Click **Deploy**.

If you receive an error message while attempting to perform this task, you should perform the procedure outlined in the article [Problem upgrading Data Security from v7.8.1](#).

Update Websense databases

Click **Update Now** in the **Settings > General > Database Downloads** page. This action performs an immediate database download update.

Review mail routing settings

Review the routing preferences in the **Settings > Inbound/Outbound > Mail Routing > Add** (or **Edit**) **Route** page, in the Delivery Method section. If multiple servers are configured for a single route, each server is assigned a preference of 5 after the upgrade. Adjust these preferences to meet your requirements. A lower preference has a higher priority. If multiple servers share the same preference, round robin load balancing is used.

Enable email hybrid service commercial bulk message analysis

If you want to use the email hybrid service commercial bulk email analysis feature, you must enable it after the upgrade.

Version 7.8.x includes commercial bulk email analysis as part of the hybrid service prefiltering capability. The results of this analysis are added in the message header passed to Email Security Gateway, which uses the hybrid service score to determine how a message is processed.

Enable this feature on the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page for the Commercial Bulk Email filter. This functionality is available only if your subscription is for Email Security Gateway Anywhere.

Perform database conversion (optional)

If you do not want to wait for the file conversion task scheduled after the upgrade process, because you want to upgrade immediately to a later version of Email Security Gateway, you can perform the conversion manually via a SQL script file. See this Websense Knowledge Base article for the script file and instructions for running it.