Upgrading Email Security Gateway v7.7.x to v7.8.x

These instructions cover the upgrade of a Websense Email Security Gateway solution from version 7.7.x to version 7.8.x.

If you are currently running a version 7.6.x deployment, and you want to upgrade to version 7.7.3 or 7.8.x, 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, and you want to upgrade to version 7.8.4, you must upgrade to version 7.8.0 first, and then upgrade to version 7.8.4. You cannot upgrade from version 7.7.x directly to version 7.8.4.

See Upgrading Email Security Gateway Solutions for specific upgrade paths.

> **Note**
> Unless noted otherwise, upgrade steps described here apply to both version 7.7.x to 7.8.0 upgrades and version 7.8.0 to 7.8.4 upgrades.

The upgrade process includes Websense V-Series appliance or virtual appliance components, along with TRITON Unified Security Center and Email Security Log Server Windows components. A virtual appliance upgrade applies only to version 7.8.0 and later.

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. See the virtual appliance Quick Start Guide for instructions on backing up a virtual appliance.

Contents:

Upgrade preparation

Several issues should be considered before you begin an Email Security Gateway product upgrade. Unless otherwise noted, these issues apply to both hardware and virtual appliance 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**)

    This step applies only to a hardware appliance upgrade.
  - If you know your version 7.8.0 Email Security Gateway system is at maximum capacity for the total number of message queues, you should remove at least 2 custom queues before performing the upgrade.
    - Message queues: maximum is 32 (**Main > Message Management > Message Queues**)
    - Ensure that you do not have custom queues named either “secure-encryption” or “data-security.” Default queues with those names are created during the upgrade process.
- **Perform database partition inventory (hardware upgrade only).** 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.

Upgrade instructions

Once you have completed the preparations 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

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. Upgrade 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.
   - The installer does not allow you to change existing configuration settings. Changes must be made after the upgrade.
   - The upgrade installer stops the Email Security Gateway Log Server service, updates the Email Security Gateway Log Server, and then restarts the Email Security Gateway Log Server service.

   

   Note

   The Email Security manager is not available until after the TRITON console upgrade completes.

2. Upgrade the TRITON console machine. Use the TRITON Enterprise upgrade installer 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.

> **Note**
>
> 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 current 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 midnight 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 version 7.8.2, 7.8.3, or 7.8.4. If the task is not complete before the subsequent upgrade, IP address information in the Message Log will be blank for messages stored in the partitions that have not yet been converted.

- 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.

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

   Hardware appliance upgrade

   The following methods are available for a hardware appliance upgrade:

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

     This option is available only for an upgrade from version 7.7.x to 7.8.0.

     No pre-upgrade hotfix download and installation is required.
   - Direct download to the V-Series appliance.
     - 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.
     - Upgrade from version 7.8.0, 7.8.2, or 7.8.3 to version 7.8.4 requires no pre-upgrade hotfix installation.

   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)
   - The existence of message queues named “secure-encryption” and “data-security.”

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.

See the appliance upgrade guide for the appliance upgrade procedure.

> **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.

Virtual appliance upgrade (version 7.8.1 and later)

Use the following steps to upgrade a virtual appliance:

a. Download the virtual appliance upgrade package from the MyWebsense Downloads page to a local directory (**WebsenseESGA78xUpgrade_VA.tgz**).
b. Upload the upgrade package to a local FTP server.
c. Log on to the Email Security Gateway virtual appliance.
d. Perform the **esgconfig.py** command to open the Email Security Gateway Virtual Appliance Configuration screen.
e. Select **Upgrade Email Security Gateway** and click **Configure**.
f. On the Upgrade Email Security Gateway page, enter the complete FTP server path for the virtual appliance upgrade package in the **Upgrade URL** field.
g. Click **Upgrade** to initiate the upgrade process. This process can take several minutes.
h. After the upgrade process is complete, check the following log file for any upgrade alerts or messages: **/var/log/upgrade.log**.

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:

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**.

Repair Email Security Gateway registration with Data Security (not required for upgrade to version 7.8.4)

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 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 (hardware appliance only)

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.