# Upgrading Email Security Gateway v7.8.4 to TRITON AP-EMAIL v8.2

These instructions cover the upgrade of a Websense Email Security Gateway solution from version 7.8.4 to Forcepoint TRITON AP-EMAIL version 8.2.

If you are currently running a version 7.6.x deployment, and you want to upgrade to version 8.2, you must upgrade to version 7.7.0 first, then upgrade to version 7.8.0, and then to version 7.8.4. See Upgrading Email Security Gateway v7.6.x to v7.7.0, Upgrading Email Security Gateway v7.7.x to v7.8.0, and Upgrading Email Security Gateway v7.8.0 to v7.8.x for procedures.

If you are currently running a version 7.7.x deployment, and you want to upgrade to version 8.2, you must upgrade to version 7.8.0 first, and then upgrade to version 7.8.4 before you upgrade to version 8.2. See Upgrading Email Security Gateway v7.7.x to v7.8.0 and Upgrading Email Security Gateway v7.8.0 to v7.8.x for procedures.

If you are currently running a version 8.0.x or 8.1.x deployment, you can upgrade directly to version 8.2.

See Upgrading Email Protection Solutions for:

- Specific product upgrade paths
- Links to all intermediate upgrade instructions
- Important information about backing up your system before you upgrade. Having backup files is an important safeguard in the event of a power outage or other interruption during the upgrade process.

**Important**

Some older V10000 and V5000 appliances are not supported with version 8.0.0 and later. See V-Series appliances supported with version 8.0.

The upgrade process includes Forcepoint appliance components (V-Series appliance, virtual appliance, or X-Series chassis security blade), along with TRITON Manager and Email Log Server Windows components. Ensure that your deployment also includes TRITON AP-DATA for data loss prevention capabilities. The upgrade process detects and upgrades this module during the TRITON Manager upgrade.

**Warning**

Please contact Technical Support before you begin the upgrade process if:

- Forcepoint personnel have customized any Email Security Gateway or TRITON AP-EMAIL back-end configuration setting
- You have customized your Secure Messaging notification template

Some customizations may be lost during the upgrade process.

**Contents:**



# Upgrade preparation

Several issues should be considered before you begin an email protection solution upgrade.

- **Verify current deployment.** Ensure that your current deployment is functioning properly 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 Forcepoint TRITON solutions for an explanation of general preparations for upgrading the Windows components in your email protection system.
- **Ensure that your firewall is configured correctly** so that the ports needed for proper email protection operation are open. See TRITON AP-EMAIL ports for information about all email protection system default ports, including appliance interface designations and communication direction.
- The upgrade to version 8.x renames 2 default policy rules:
  - ThreatScope is renamed File Sandbox.
  - URL Scanning is renamed URL Analysis.

  If you currently have custom rules with these new names, you should change them before the upgrade process begins, to avoid having duplicate rule names after the upgrade.

- **Back up and remove tomcat log files and remove temporary manager files (optional; recommended to facilitate timely TRITON console upgrade).** Use the following steps:
  1. Log onto the Windows server where the TRITON manager resides.
  2. Navigate to the following directory:

     **C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\logs**
  3. Copy **C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\logs** to another location (for example, to **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 protection system deployment.

**Important**

If your network includes a Forcepoint web protection solution, you must upgrade the Policy Broker/Policy Server machine first, whether or not these components reside on an appliance. Other Forcepoint 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 protection for more information.

Use the following procedure to perform an email system upgrade:

1. Use the TRITON Enterprise upgrade installer from the Forcepoint My Account downloads page to upgrade Email Log Server if it is installed on a machine other than the one on which the TRITON Manager is installed. Follow the installation wizard instructions for Log Server.

   

   **Important**

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

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

2. Upgrade the TRITON Manager machine. Use the TRITON Enterprise upgrade installer from the Forcepoint My Account downloads page. Ensure that TRITON AP-EMAIL and TRITON AP-DATA are selected for upgrade. The upgrade process includes TRITON AP-DATA and the Email Log Server if it is installed on the TRITON Manager machine.

   

   **Warning**

   On the Select Components screen in the upgrade installer, ensure that the **TRITON AP-EMAIL** option is selected. This option is required if you are running your email protection system on a V- or X-Series appliance or an on-premises (ESXi server) virtual appliance.

   The **TRITON AP-DATA Email Gateway** option applies to a cloud-hosted virtual appliance running with TRITON AP-DATA. See the topic titled "Email Gateway for Microsoft Office 365" in the TRITON AP-DATA Installation Guide for details about this product feature.

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

   - The upgrade installer Configuration page shows the IP address of the database engine that manages the Email 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 module service, updates the Email SQL Server databases (and Log Server if found), and then restarts the Email module service.

     

     **Note**

     The TRITON Manager Email module is not available until after the TRITON console upgrade completes.

3. Upgrade all your appliances. Email should not be directed through appliances during the upgrade process.

   **X-Series hardware appliance upgrade**

   See the X-Series appliance Using the X-Series Command Line Interface (CLI) guide for upgrade command options on this platform.

**Important**

You must upgrade your X10G security blade to version 8.0.0 before performing an upgrade to version 8.0.x, 8.1, or 8.2.

**V-Series hardware appliance upgrade**

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.

The appliance upgrade process includes a check for

- Adequate disk space for TRITON AP-EMAIL (at least 8 GB required)
- Cached message log file size (cannot exceed 10 MB)

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

**Note**

Appliance services are not available while the patch is being applied and until the appliance completes its restart.

If your email 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**

Use the following steps to upgrade a virtual appliance:

a. Download the appropriate virtual appliance upgrade package from the Forcepoint My Account downloads page to a local directory.

b. Upload the upgrade package to a local FTP server.

c. Use an SSH client like PuTTY or the virtual appliance console to log on to the email virtual appliance.

d. If you are upgrading from version 7.8.4, perform the **esgconfig.py** command to open the TRITON AP-EMAIL Virtual Appliance Configuration screen.

   If you are currently running virtual appliance version 8.0.x or 8.1, the command to perform for this step is **email_va_config.py**.

e. Select **Upgrade Email Appliance** and click **Configure**.

f. On the Upgrade Email Appliance 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**.

**Note**
You may need to restart the appliance if you cannot establish an **ssh** connection after the upgrade is complete.

Continue with *Post-upgrade activities* to complete the email protection system 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 Manager:

- *Update data loss prevention policies and classifiers*
- *Update Forcepoint databases*
- *Update Email module backup file*

## Update data loss prevention policies and classifiers

1. Select the Data module.
2. Follow the prompts that appear for updating data loss prevention 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**.

## Update Forcepoint databases

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

## Update Email module backup file

Due to a change in implementation at version 8.1, the TRITON Manager Email module backup file format is not compatible with versions earlier than 8.1. You must remove any pre-version 8.1 backup log file before you create a new backup file for

either version 8.1 or 8.2. If you don't remove the old log file before you create the new file, the backup/restore function can become inaccessible.

Use the following steps:

1. Navigate to the following directory on the TRITON management server machine:

   C:\Program Files (x86)\Websense\Email Security\ESG Manager
2. Locate and remove the following file:

   `ESGBackupRestore`

   Copy this file to another location if you want to save it.
3. Create a new backup file for version 8.2 on the **Settings > General > Backup/Restore** page.