FORCEPOINT
POWERED BY Raytheon

V-Series Dual Mode Appliance Upgrade Guide

Forcepoint Web Security, Forcepoint Email Security, Forcepoint URL Filtering
Models: V10000, V5000

Upgrades to v8.4.x

Published 2017

D120517840

Contents

Preparing and Upgrading Dual-Mode Appliances

Background information

Product renaming

Product names have changed in v8.4.0.

Former Name	New Name
TRITON AP-EMAIL (v8.x) TRITON Email Security Gateway / Anywhere (v7.8.4)	Forcepoint Email Security
TRITON AP-WEB (v8.x) TRITON Web Security Gateway / Anywhere (v7.8.4)	Forcepoint Web Security
Forcepoint Web Filter & Security (v8.x) Websense Web Security (v8.x)	Forcepoint URL Filtering
V-Series X-Series TRITON Appliances	V Series X Series Forcepoint Appliances

For a complete list of name changes, see the v8.4.0 Forcepoint Appliances Release Notes.

Overview

Forcepoint Appliance version 8.4 does not support dual-mode appliances. Dual-mode appliances host both Forcepoint Email Security and Forcepoint Web Security (V10000 only), or Forcepoint Email Security and Forcepoint URL Filtering (V5000, V10000).

Before you upgrade a dual-mode appliance to v8.4, either Forcepoint Email Security or Forcepoint URL Filtering must be moved to a new Forcepoint appliance. If Forcepoint Web Security is the web protection module, Forcepoint Email Security must move to a new appliance.

- In most cases, moving Forcepoint Email Security (or Email Security Gateway v7.8.4) is the best or only option. If Forcepoint Web Security is the web protection module, moving Forcepoint Email Security is the only option.

  To make the move easier, special migration tools have been developed and a special procedure is detailed in this guide.
- When the web module is Forcepoint URL Filtering on a V5000, if necessary, it can be moved off of the dual-mode appliance.
- When Forcepoint URL Filtering is located on a V10000 with Forcepoint Email Security, it must be moved because Forcepoint URL Filtering is not supported by itself on a V10000 appliance.

Before you begin, please contact your Forcepoint account representative to learn about special promotions for dual-mode deployments planning a v8.4 upgrade.

This guide applies only to appliances in Web and Email (dual) mode:

- Forcepoint Web Security and Forcepoint Email Security
- Forcepoint URL Filtering and Forcepoint Email Security
- Web Security Gateway (Anywhere) and Email Security Gateway (Anywhere)
- Web Security and Email Security Gateway (Anywhere)

Use the information in this guide to:

1. Migrate Forcepoint Email Security or Forcepoint URL Filtering to a new Forcepoint appliance.
2. Upgrade the original appliance to v8.4.

Warning

If you or Forcepoint personnel have customized any Email Security Gateway or Forcepoint Email Security back-end configuration settings, please contact Technical Support before you begin the upgrade process.

Some customizations may be lost during the upgrade process.

Appliances running these versions of Forcepoint software can be upgraded to v8.3:

Current Version V-Series Dual-Mode	End Version V-Series Single-Mode
7.8.4, 8.0.0, 8.0.1, 8.1.0, 8.2.0	8.3.x

Forcepoint appliances can be upgraded directly to v8.4.0 from v8.1.x, v8.2.x, and v8.3.x.

Forcepoint appliances cannot be upgraded directly from v8.0.x to v8.4.0. To upgrade from v8.0.x to v8.4.0, use the v8.3 upgrade guide to upgrade from v8.0.x to v8.3.0,

and then use the V Series, X Series, and Virtual Appliance Upgrade Guide to upgrade from v8.3.0 to v8.4.0.

Important

In addition to upgrading your appliances, you must also upgrade Forcepoint components installed on other servers. The correct sequence of the upgrade steps is critical to a successful upgrade.

Important

Some older V10000 and V5000 appliances are not supported with versions of 8.0 and higher. See V-Series appliances supported with v8.x.

Important

Forcepoint V5000 G2R2 Appliance customers may encounter a memory shortage after upgrading to version 8.2 or later. This issue is the result of newer versions of software requiring additional memory, and was only captured under a very heavy load. A DIMM Kit (2 x 8GB) is certified to expand the physical memory of the V5000 G2R2 Appliance. It is now generally available and recommended for V5000 G2R2 deployment moving to versions 8.2 and later. Please contact your sales representatives for purchase information. For more details, see the related Knowledge Base article and the DIMM Kit installation instructions.

Overview of the dual-mode upgrade process

Because dual-mode appliances are not supported in v8.4, you need to move either Forcepoint Email Security or Forcepoint URL Filtering to a new Forcepoint appliance. If Forcepoint Web Security is the web protection module, Forcepoint Email Security must move to a new appliance. Moving Forcepoint Web Security is not an option.

Option 1: Move Forcepoint Email Security to a new appliance and upgrade the web protection module on the original, dual-mode appliance.

Option 2: Move Forcepoint URL Filtering to a new appliance and upgrade Forcepoint Email Security on the original, dual-mode appliance. This is the only option when Forcepoint URL Filtering is located on a V10000 appliance.

Moving Forcepoint Web Security is not an option.

Summary of the upgrade process

- Read *Forcepoint Appliances v8.4.0 release notes*, page 5.
- *Choose the product module to move*, page 6.
- Perform the procedure below that matches the module you are moving.

If Forcepoint Email Security will move to a new appliance (recommended)

> **Important**
> This is not an option when the appliance is a V10000 and the web protection module is Forcepoint URL Filtering. In that case, Forcepoint URL Filtering must move. See *Move Forcepoint URL Filtering and upgrade the appliance*.

- Set up a new v8.4.0 Forcepoint Email Security appliance (V-Series or VMware virtual appliance), including firstboot and post-firstboot configuration.
- Perform Forcepoint Email Security pre-upgrade activities.
- On the new appliance, use the Email migration tool to copy email data from the dual-mode appliance to the new appliance.
- Remove Forcepoint Email Security from the dual-mode appliance.
- Perform Forcepoint Web Security or Forcepoint URL Filtering pre-upgrade preparation.
- On the original, now single-mode appliance, upgrade Forcepoint Web Security or Forcepoint URL Filtering.
  1. Upgrade the policy source machine. This may be located on the appliance, or on the Forcepoint Management Server, or on a separate server.
  2. Upgrade the appliance, if not already done.
  3. Upgrade the Forcepoint Management Server, if not already done.
- Upgrade the remaining off-appliance components.
- Perform post-migration/post-upgrade activities.

See *Move Forcepoint Email Security and upgrade the appliance*, page 7.

If Forcepoint URL Filtering will move to a new appliance

- Set up a new V-Series appliance with the same version of Forcepoint URL Filtering that is currently running on the dual-mode appliance.
- Perform a **Web Configuration** backup on the dual-mode appliance. This backs up only the Forcepoint URL Filtering module.
- Restore the backup on the new appliance.
- Upgrade Forcepoint URL Filtering on the new appliance.
  1. Perform Forcepoint URL Filtering pre-upgrade preparation.

2. Upgrade the policy source machine. This may be located on the new appliance or on the Forcepoint Management Server, or a separate server.
3. Upgrade the appliance, if not already done.
4. Upgrade the Forcepoint Management Server, if not already done.

- On the dual-mode appliance, install a hotfix to remove Forcepoint URL Filtering, creating a single-mode Forcepoint Email Security appliance.
- Perform Forcepoint Email Security pre-upgrade preparation.
- Upgrade Forcepoint Email Security on the now single-mode appliance.
- Upgrade remaining off-appliance components.
- Perform post-migration/post-upgrade activities.

See *Move Forcepoint URL Filtering and upgrade the appliance*, page 27.

Forcepoint Appliances v8.4.0 release notes

Before you upgrade, read the v8.4.0 release notes.

- Forcepoint Web Security Release Notes
- Forcepoint Email Security Release Notes
- Forcepoint Appliances Release Notes
- Forcepoint Security Manager Release Notes

See, also, these links to *Release Notes for 8.x releases*, page 44.

Choose the product module to move

Important

Dual-mode upgrade assumes that both the web and email modules are functional and in production (in active use).

If only one mode is in production, remove the unused module and upgrade as a single-mode appliance. See *Removing an unused module*, page 42.

When both modules are in production:

Option 1 (recommended): Migrate Forcepoint Email Security to a new appliance. This is not an option when the appliance is a V10000 and the web protection module is Forcepoint URL Filtering. In that case, Forcepoint URL Filtering must be moved.

Option 2: Migrate Forcepoint URL Filtering to a new appliance. This procedure is more involved and there are no special migration tools.

Forcepoint Web Security cannot be relocated unless a fresh install is performed. Move Forcepoint Email Security, instead.

Forcepoint Email Security migration summary

The following describes only the *email module migration steps*. For a summary of the complete upgrade procedure, see *Summary of the upgrade process*, page 3.

1. Procure and set up a new v8.4.0 Forcepoint Email Security appliance. The appliance can be either a V-Series appliance or VMware virtual appliance.
2. On the dual-mode appliance, apply a hotfix to open a secure channel to the new appliance.
3. On the new appliance, in the CLI use the email **migrate** command to move the email data files from the dual-mode appliance to the new appliance.

The migration step is complete.

Forcepoint URL Filtering migration summary

The following describes only the *web module migration steps*. For a summary of the complete upgrade procedure, see *Summary of the upgrade process*, page 3.

1. Procure and set up a new V-Series appliance with the same version of Forcepoint URL Filtering that is currently running on the dual-mode appliance.
2. Perform a **Web Configuration** backup on the dual-mode appliance. This backs up only the Forcepoint URL Filtering module. Save the backup file to an off-appliance location.
3. Restore the backup on the new appliance.
4. On the new appliance, upgrade Forcepoint URL Filtering to v8.4.0.

The migration step is complete.

Move Forcepoint Email Security and upgrade the appliance

Use this procedure if you are moving Forcepoint Email Security to a new Forcepoint appliance.

1. *Set up the new Forcepoint Email Security appliance*, page 7
2. *Prepare Forcepoint Email Security for migration*, page 7
3. *Move email data*, page 9
4. *Remove the email module from the dual-mode appliance*, page 12
5. *Prepare web protection for upgrade*, page 13
6. *Upgrade Forcepoint Web Security or Forcepoint URL Filtering*, page 18
7. *Perform post-upgrade activities*, page 19

Set up the new Forcepoint Email Security appliance

Procure and set up a new v8.4.0 Forcepoint Email Security appliance.

Important

Contact your Forcepoint account representative to learn about special promotions for dual-mode upgrades to v8.4.

Perform appliance setup, including firstboot, and post-firstboot activities.

See Forcepoint Appliances Getting Started.

Prepare Forcepoint Email Security for migration

Address these details before starting your Forcepoint Email Security migration.

- **Verify the 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 upgrade to version 8.4.0 to ensure that 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 and web protection systems.

  > **Important**
  > You must use your existing Forcepoint Manager Windows machine. Use of a newly installed Forcepoint Security Manager for an upgrade is not currently supported.

- **Ensure that your firewall is configured correctly** so that the ports needed for proper email protection operation are open. See Forcepoint Email Security ports for information about all email protection system default ports, including appliance interface designations and communication direction.
- **Back up and remove tomcat log files and remove temporary manager files (optional; recommended to facilitate timely console upgrade).** Use the following steps:
  1. Log onto the Windows server where the Forcepoint Security 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 of the downloadFile* files.

Appliance-specific details

- If the appliance is registered in Security Manager, unregister the appliance.
- Ensure that the dual-mode and new v8.4 appliance are in the same subnet. If they are not, the migration process may complete, but the version 8.4 appliance Ethernet interfaces are not correctly updated.
- You must release your dual-mode appliances from a cluster before performing the migration. Migrate each appliance, and then rebuild your cluster after the migration process is complete.
- If you are migrating email to a virtual appliance, you may need to reconfigure some network settings. The version 8.4 virtual appliance supports 3 network interfaces: C, P1, and P2. In the migration, the C interface retains the setting you assigned it during firstboot. The P1 and P2 interfaces inherit the settings of P1 and P2 when migrating from a V5000, or the E1 and E2 settings when migrating from a V10000. On the V10000, the P1 and P2 settings are left behind.

- Calculate the disk space used on your existing appliance and ensure that the new appliance has adequate disk space for all data you want to migrate.
- If you or Forcepoint personnel have customized your appliance iptables settings, please contact Technical Support. These customizations are not preserved by the migration process.

Move email data

Summary:

- On the dual-mode appliance, apply Hotfix 300. Hotfix 300 opens a secure channel from your dual-mode appliance to the new appliance.
- On the new appliance, in the CLI migrate your email files using the **migrate** command.

Install Hotfix 300

1. Log on to the Appliance Manager for the dual-mode appliance.
2. Go to the **Administration > Patches / Hotfixes > Hotfixes** page.
3. Enter the name of hotfix 300 in the search box at the top of the screen:

   ESG-*x.x.x*-300

   Where *x.x.x* is the version of Forcepoint Email Security currently running on the dual-mode appliance.
4. Click **Find**. If the hotfix is not found, ensure that the name is entered correctly.
5. In the pop-up display, click **Download** to download the hotfix.

   If you downloaded the hotfix package to a local directory, you can use the **Upload Hotfix Manually** button to upload the hotfix.
6. Click **Install** to install the hotfix. Installation opens a secure channel from the dual-mode appliance to the new appliance.

Migrate the data

All migration steps are performed in the CLI of the new, v8.4 appliance.

The following commands may be used.

Action and Syntax	Details

Log on to the email-specific CLI.
`login email`
	You must be in the config mode to log on to the email-specific CLI.
	Example:
	`(config)# login email`
	`(config)(Email)#`

Migrate interactive mode Move email configuration data and messages (optional) to a new appliance. The CLI prompts for needed information. `migrate interactive`	Example: `(config) (Email) # migrate interactive`
Migrate silent mode Move email configuration data and messages to a new appliance without prompting for input. `migrate silent --host <host_name>`	**Host:** Host name or E1/P1 interface IP address Example: `(config)(Email)# migrate silent --host 10.206.143.3`

1. Log on to the new v8.4 appliance CLI and enter **config** mode.

> **Note**
> If you use a client interface like PuTTY to access the CLI, you will want to configure a longer connection session to accommodate a somewhat lengthy migration process.
>
> For example, in the PuTTY configuration interface, select the **Connection** category. Enter **30** in the **Seconds between keepalives (0 to turn off)** entry field.

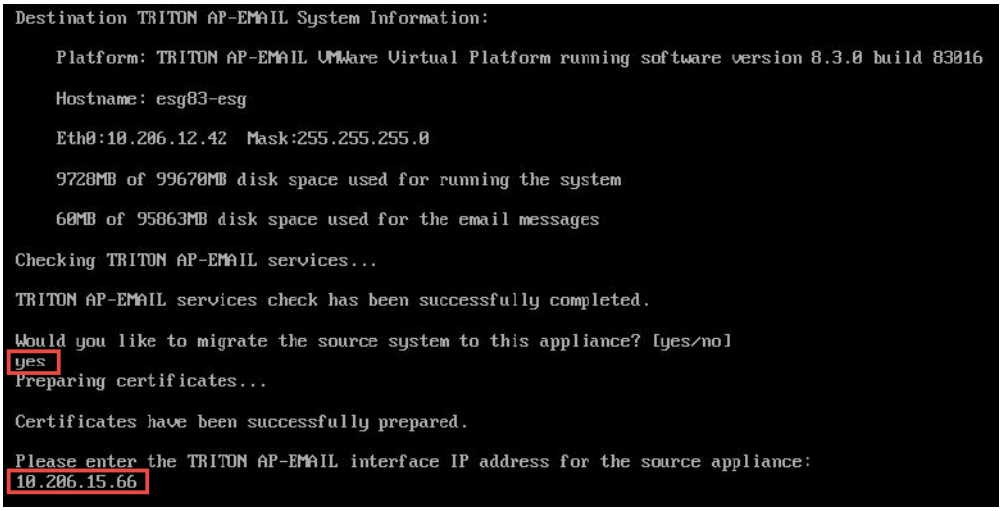
2. In **config** mode, log in to the email module CLI:

   `login email`

3. Perform the migration using the **migrate** command with 1 of 2 options: **interactive** or **silent**.

   Interactive mode is a step-by-step process that requires input during the process.

An example of the interactive mode command is:



You enter the following information:

- Dual-mode appliance E1/P1 interface IP address
- Confirmation for the start of the migration
- Selection of a transfer option:

  Example CLI for this section of the migration looks like:

  ```
  Would you like to start the migration process from the
  source appliance: 10.206.15.66 to this appliance
  (services on both appliances will stop)? [yes/no]
  ```

  yes

  ```
  Please select a transfer option: [1/2/3]

  1. Transfer only configuration files, defer logs, and
  policy incidents.

  2. Transfer configuration files, defer logs, policy
  incidents, and email messages.

  3. Quit
  ```

  2

  ```
  Are you sure you want to transfer all configuration
  files, defer logs, policy incidents, and email messages?
  [yes/no]
  ```

  yes

  :If you migrate email message queues in addition to configuration settings, be aware that the transfer of large-volume queues may take a few hours to complete.

Silent mode requires the user to enter only the dual-mode appliance E1/P1 interface IP address. For example:

```
migrate silent --host 10.206.15.66
```

The second transfer option (all files and all messages) is automatically selected for silent mode, and the migration runs without the need for subsequent user input.

It is helpful to know:

- The migration log accumulates warning messages from any previous unsuccessful migration. Each time you attempt (or complete) a subsequent migration, error messages from your previous migration attempts still appear.
- If you have an email DLP policy configured to use a Forcepoint DLP quarantine action, and the **Settings > General > Remediation** page Release Gateway is set to **Use the gateway that detected the incident**, you should change the Release Gateway to the IP address of your new appliance. Otherwise, when a Data module administrator releases a pre-migration quarantined message, an "Unable to release incident" error is generated.
- Virtual IP address settings in filter actions are not retained after an appliance migration. You need to reconfigure virtual IP address settings manually.

Remove the email module from the dual-mode appliance

After email data migration is complete, a hotfix removes the email module from the dual-mode appliance, converting the appliance to a single-mode web protection appliance that can be upgraded to v8.4 with the standard upgrade procedure.

When the hotfix is installed it immediately removes the email module and reboots the appliance. The action cannot be undone.

The hotfix is specific to the V-Series model (V5000 or V10000) and current Forcepoint software version (7.8.4, 8.0.0, 8.0.1, 8.1.0, 8.2.0, 8.3.0). Be sure to download the correct hotfix for your dual-mode appliance and software version.

- Hotfix 333 is for V10000 dual-mode only. It removes Forcepoint Email Security and its related files. This cannot be undone.
- Hotfix 777 is for V5000 dual-mode only. It removes Forcepoint Email Security and its related files. This cannot be undone.

To install the hotfix:

1. Log on to the dual-mode Appliance Manager.
2. Go to the **Administration > Patches / Hotfixes > Hotfixes** page.
3. Enter the hotfix name in the search box at the top of the screen:

   APP-*x.x.x-yyy*

   Where *x.x.x* is the version of Forcepoint Email Security currently running on the dual-mode appliance, and *yyy* is:

   333 for V10000

   777 for V5000

   For example: APP-8.1.0-333 for a V10000 dual-mode appliance running TRITON AP-EMAIL v8.1.0.
4. Click **Find**. If the hotfix is not found, ensure that the name is entered correctly.
5. In the pop-up display, click **Download** to download the hotfix.

If you downloaded the hotfix package to a local directory, you can use the **Upload Hotfix Manually** button to upload the hotfix.

6. Click **Install** to install the hotfix. Installation removes the email module and all associated files. This action cannot be undone. When installation is complete, the appliance restarts automatically to complete the action. The appliance may restart before the Appliance Manager confirms that installation is complete.

After the appliance completes its restart, the web protection module can be prepared for upgrade.

Prepare web protection for upgrade

Off-appliance components, page 13

Appliance components, page 16

Off-appliance components

1. Verify that third-party components, including your database engine and directory service, are supported with your web protection solutions. See Requirements for web protection solutions.
2. Back up **all of your web protection components** before starting the upgrade. See the **Backup and Restore FAQ** for your version for instructions on backing up both software-based and appliance-based components. (Go to support.forcepoint.com, search for "Backup and Restore FAQ", and use the Product and Versions filters. For Product, filter on the web or email protection product, and then add V10000 or V5000.)

   On appliances, in the Appliance Manager perform a **Web Configuration** backup and save it to an off-appliance location.

   a. Go to the **Administration > Backup Utility > Backup** page.

   b. In the Perform Backup section, for Backup Type select **Web Configuration**, and then click **Run Backup Now**.

   c. To download the file, in the Local Backup Files area, select **Web Configuration** and click on the backup file name (shown as a link).
3. Before upgrading Filtering Service, make sure that the Filtering Service machine and the TRITON management server have the same locale settings (language and character set).

   After the upgrade is complete, Filtering Service can be restarted with any locale settings.
4. If your product includes Web DLP features, before upgrading the management server, make sure your Web DLP components are ready for upgrade:

   a. Stop all discovery and fingerprinting tasks.

   b. Route all traffic away from the system.

   c. Ensure that your supplemental fingerprint repositories are fully synchronized with the primary repository.

d. Make sure all settings are deployed successfully. Log onto the Data Security manager. If the **Deploy** button is highlighted, click it.

e. If your organization was supplied with custom file types, change the name of the following files in the **policies_store\custom_policies\config_files** folder on the management server; otherwise they will be overwritten during upgrade.

- Change **extractor.config.xml** to **custom_extractor.config.xml**.
- Change **extractorlinux.config.xml** to **custom_extractorlinux.config.xml**.

The filenames are case-sensitive.

f. If custom policies were provided, submit a request for updated versions before proceeding.

5. When upgrading to v8.3, a new logging partition is added to your Log Database. Please make sure you do not have 70 active partitions (the limit) prior to upgrading. Use the **Web > Settings > Reporting > Log Database** page of the TRITON Manager to disable at least one active partition prior to upgrading.

6. Back up your current Log Database and stop Log Server.

Warning

If database operations are active during upgrade, the Log Database may be rendered unusable.

When this occurs, it can be difficult to fix.

Make **sure** to stop Log Server and the database jobs, as described below, before upgrading the database.

a. Back up your reporting databases.

Refer to Microsoft documentation for instructions. The databases are named wslogdb70 (the catalog database), wslogdb70_*n* (standard logging partition databases), and wslogdb70_amt_1 (threats partition database).

b. On the Log Server machine, use the Windows Services tool to stop **Websense Log Server**.

7. It is best to **stop all Log Database jobs** prior to starting the upgrade, but, before it upgrades the Log Database, the upgrade process will attempt to stop any Log Database jobs not already stopped. If the jobs cannot be stopped, you will need to stop them manually. However, you do not need to exit the installer to do that.

Stop the Log Database jobs using these steps:

a. If you have a **full version of Microsoft SQL Server** (not Express), stop **all database jobs** as follows. (See below for steps to stop SQL Express jobs.)

- Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).
- To disable all currently active SQL Server Agent jobs, right-click each of the following jobs and select **Disable**:

  Websense_ETL_Job_wslogdb70

  Websense_AMT_ETL_wslogdb70

Websense_IBT_DRIVER_wslogdb70

Websense_Trend_DRIVER_wslogdb70

Websense_Maintenance_Job_wslogdb70

Disabling the jobs prevents them from executing at the next scheduled time, but does not stop them if a job is in process.

Make sure all jobs have completed any current operation before proceeding with upgrade.

- After upgrade, verify that the jobs have been enabled.

  Enable any that were not automatically enabled by the upgrade process. Normal database operations will then resume.

b. If you have **SQL Server Express, stop all database jobs** as follows:

- Log in to the Microsoft SQL Server Management Studio.
- Expand the **Databases** tree to locate the catalog database (wslogdb70, by default), then expand the catalog database node.
- Expand **Service Broker > Queues**.
- Right click **dbo.wse_scheduled_job_queue** and select **Disable Queue**.
- The upgrade process will re-enable the job queue. After upgrade, verify that the Queue has been enabled.

  Enable it, if necessary, by repeating the process, this time ultimately selecting **Enable Queue** to resume normal database operations.

When Log Server is upgraded, the upgrade process first checks the Log Database version and updates the database, if necessary. If you have multiple Log Servers, the database update occurs with the first Log Server upgrade. The database update, including the need to stop the database jobs, is not repeated when additional Log Server instances are upgraded.

8. If Log Server uses a Windows trusted connection to access the Log Database, be sure to log on to the Log Server machine using the trusted account to perform the upgrade. To find out which account is used by Log Server:

   a. Launch the Windows Services tool.

   b. Scroll down to find **Websense Log Server**, then check the **Log On As** column to find the account to use.

Important

As a result of a change made to avoid a potential vulnerability when a presentation report is included as a link in an email, report links in emails that exist prior to upgrading to v8.3 will no longer work.

Content Gateway (Forcepoint Web Security only)

Before upgrading Content Gateway, be aware of the following:

- Most SSL configuration settings are saved and applied to the upgraded Content Gateway, except for dynamic certificates. Note that:
  - The Incident list is retained. Before upgrading, consider performing maintenance on the Incident list; remove unwanted entries.
  - SSLv2 is not enabled by default. If it is enabled prior to upgrade, the setting is retained.
- For user authentication, there is one credential cache for both explicit and transparent proxy mode, and one Global Authentication Options page for setting the caching method and Time-To-Live.

  During upgrade, the Cache TTL value is retained from the Transparent Proxy Authentication tab **unless** the value on the Global Authentication Options tab is not the default. In this case, the customized value is used.
- If you use Integrated Windows Authentication (IWA), be aware that IWA domain joins should be preserved through the upgrade process. However, in case the joins are dropped, make a record of the settings before starting the upgrade. Log on to the Content Gateway manager and record the IWA settings, including the names of domains to which IWA is joined. Keep this record where it is easily retrieved after the upgrade.

Appliance components

Configure and test access to the appliance command-line interface (CLI)

At the end of the upgrade procedure you will need to log on to the upgraded, v8.4 appliance CLI and perform a small number of tasks.

The v8.4 appliance CLI is accessed in the same way as the existing V-Series CLI. If you haven't used the V-Series CLI, or haven't accessed it recently, test your access now and perform any necessary configuration.

SSH access

All V-Series appliances can connect to the CLI with a terminal emulator and SSH. The client machine must be in a network that has a route to the appliance and SSH access must be enabled on the dual-mode appliance in the Appliance Manager.

In the Appliance Manager, check the SSH access setting and, if necessary, enable SSH access.

1. Log on to the Appliance Manager and go to the **Administration > Toolbox** page.
2. In the **Appliance Command Line** section, enable SSH remote access.

Test SSH access

1. On a Windows system connect with **PuTTY,** or similar. On a Mac system connect with **Terminal**.
2. Connect to the appliance management interface (C) IP address on port 22.
3. Log on with the **admin** credentials.

iDRAC access

Most V-Series models supported by v8.3 have an integrated DELL Remote Access Controller (iDRAC). If you have never worked with the iDRAC, see **Using the iDRAC** Forcepoint Appliances Getting Started.

To access the CLI, log on to the iDRAC and go to **Overview > Server**. In the upper right **Virtual Console Preview** area, click **Launch**.

VGA and USB direct connect

Connect a monitor and keyboard directly to the appliance.

Serial port direct connect

Configure a serial connection to a monitor and keyboard. The connection should be set to:

- 9600 baud rate
- 8 data bits
- no parity

Appliance customizations

Important

Customizations are not retained through the upgrade process.

Before upgrading, inventory all customizations and make a plan for restoring any that are required.

Customizations can include:

- Custom patches
- Hand updated files
- Extra packages added by hand
- Extra files added, binary or configuration

Post-upgrade, Forcepoint Technical Support may be able to help restore some files from your pre-upgrade file system.

SNMP settings

Warning

Upgrade to v8.4.0 does not preserve SNMP settings.

A fix is in development. Please check the Forcepoint Knowledge Base or contact Technical Support to see if a hotfix is available.

Before upgrading, document your existing SNMP settings for reapplication after upgrade.

Content Gateway logs

If the appliance hosts Forcepoint Web Security (Web Security Gateway / Anywhere), during the upgrade, depending on their size, older Content Gateway logs may be automatically removed to make room for the new version.

To ensure that the current Content Gateway log is retained (content_gateway.out), download it to a location off of the appliance.

1. In the Appliance Manager, go to **Administration >Logs**.
2. Select the **Content Gateway** module and then **Download entire log file**.
3. Click **Submit** and specify a location to save the file.

Content Gateway Integrated Windows Authentication (IWA) settings

IWA domain joins should be preserved through the upgrade process. However, in case there is an error and IWA domain joins are dropped, make a record of the settings before starting the upgrade. Log on to Content Gateway and record the IWA settings.

Upgrade Forcepoint Web Security or Forcepoint URL Filtering

With the email module removed, the web protection module is now on a single-mode appliance that can be upgraded to v8.3 using the standard upgrade procedure.

For Forcepoint Web Security, see Upgrade Instructions for Forcepoint Web Security (also applies to v7.8.4 Web Security Gateway/Anywhere).

For Forcepoint URL Filtering, see Upgrade Instructions for Forcepoint URL Filtering (also applies to v7.8.4 Web Security).

Components must be upgraded in the following order:

- Policy Broker machine
- Policy Server machines
- Filtering Service, Network Agent, and User Service machines
- Log Server
- TRITON management server (already upgraded if it hosts Policy Broker)

- Software instances of Content Gateway (Forcepoint Web Security only)
- Any additional components

Important

After upgrading all Web components, return to this guide for a complete list of post-upgrade activities.

Perform post-upgrade activities

Appliance post-upgrade activities

Depending on the Web or Email module installed on your appliance, after upgrade perform the following:

In the CLI

Elevate to **config** mode and perform system checks and verify some configuration settings.

- System information

  ```
  show appliance info
  ```

  Results may be similar to:

  ```
  Uptime              : 0 days, 2 hours, 13 minutes
  Hostname            : webapp.example.com
  Hardware_platform   : V10000 G4
  Appliance_version   : 8.3.0
  Mode                : Forcepoint Web Security
  Policy_mode         : Filtering only
  Policy_source_ip    : 10.222.21.10
  ```

- Upgrade history

  ```
  show upgrade --history
  ```

- Appliance status

  ```
  show appliance status
  ```

  ```
  show <module>
  ```

  If expected system services are not running, restart the module that hosts the service

  ```
  restart <module>
  ```

- Network interface settings

  ```
  show interface info
  ```

  If you have bonded interfaces, note that the names used to indicate the type of bond have changed. For example, load-balancing is now “balance-rr”.

- Check and synchronize the system time

  ```
  show system ntp
  show system clock
  show system timezone
  ```

  If the clock is off and NTP is configured, sync with:

  ```
  sync system ntp
  ```

  Otherwise, to sync when the time is set manually, see **System time and time synchronization with TRITON servers** in Forcepoint Appliances Getting Started.

- Configure a **filestore**. A **filestore** is an off-appliance location for storing appliance-related files, including backup, log, and configuration files.

  Establishing a filestore is essential for saving and loading files.

  A filestore definition includes:

  - A unique name, known as the filestore alias.
  - The IP address of the filestore host and the port on which to connect.
  - The directory location (path or share) on the host.
  - The protocol to use to connect and move files to and from the filestore. Supported protocols include **ftp**, **tftp**, and **samba**.
  - Optionally, the name of a user (account) with permissions on the filestore.

  To define a filestore:

  ```
  set filestore --alias <filestore_alias>
     --type <ftp|tftp|samba> --host <ip_address>
     --path <share_directory>
     [--user <user_name>] [--port <port>]
  ```

  Example:

  ```
  set filestore --alias fstore --type samba
     --host 10.123.48.70 --path myfiles/myfolder
     --user jdoe
  ```

- If you integrate with a SIEM, configure SNMP polling and alerting. Use the documentation created in the pre-upgrade activity. See, also, **SNMP polling and alerting** in Forcepoint Appliances Getting Started.

In Forcepoint Security Manager

- Register your appliances. Log on to Forcepoint Security Manager and go to the **Appliances** tab to register your appliances.
- If you have *User directory and filtering* appliances, in Forcepoint Security Manager go to the Web module **Settings > General > Policy Servers** page, and add the Policy Server instances.

Forcepoint Email Security post-upgrade activities

Your system should have the same configuration after the migration as it did before the migration.

Perform the following tasks in the Forcepoint Security Manager:

- Redirect email traffic through your system to ensure that it performs as expected.
- *Update data loss prevention policies and classifiers*
- *Update Forcepoint databases*
- *Update Email module backup file*
- *Update appliance management interface configuration settings*
- *Configure email DNS lookup*
- *Update Log Database*

Update data loss prevention policies and classifiers

1. In TRITON Manager, select the Data module.
2. Follow the prompts 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. When finished, 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 v8.1, 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 v8.x. 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 v8.3 on the **Settings > General > Backup/Restore** page.

Update appliance management interface configuration settings

If your upgrade to v8.3 included a data migration, you need to re-configure some functions that use the appliance management (C) interface after the migration and upgrade are complete. The management (C) interface is new for virtual appliance users at v8.3.

Appliance registration

In the EMAIL module of TRITON Manager, go to **Settings > General > Email Appliances** and click on the host name link to delete the appliance. Log off and then back on to TRITON Manager and add the appliance's new C interface IP address.

Data loss prevention

Re-register the Forcepoint Email Security appliance with the Data module as follows:

1. Select the TRITON Email module and navigate to the **Settings > General > Data Loss Prevention** page.
2. Click **Unregister** to remove the DLP registration.
3. In the TRITON Data module, navigate to the **Settings > Deployment > System Modules** page. Select the Forcepoint Email Security module.
4. In the upper left corner, click **Delete**.
5. In the TRITON Email module **Settings > General > Data Loss Prevention** page, ensure the appliance management (C) interface IP address appears in the **Communication IP address** field.
6. Click **Register** to register the appliance with the Data module.
7. Select the Data module and click **Deploy**.

Email hybrid service

Re-register the Forcepoint Email Security appliance with the email hybrid service as follows:

1. Select the TRITON Email module and navigate to the **Settings > Hybrid Service > Hybrid Configuration** page.
2. Click **Edit** at the bottom of the page.
3. Replace the SMTP server IP address with the new C interface IP address.
4. Click **OK**.

Personal Email Manager notification message

You may need to enter your destination appliance management interface IP address for the proper distribution of Personal Email Manager notification messages.

1. Select the TRITON Email module and navigate to the **Settings > Personal Email > Notification Message** page.
2. Enter the new appliance management (or C) interface in the **IP address or hostname** entry field.
3. Click **OK**.

Configure email DNS lookup

The appliance firstboot process includes the entry of DNS server settings. You can enhance DNS lookup query performance by configuring a second set of DNS server entries specifically for the Email module. Use the following CLI commands, as needed:

```
set interface dns --module email --dns1  <DNS_IP>
set interface dns --module email --dns2  <DNS_IP>
set interface dns --module email --dns3  <DNS_IP>
```

Update Log Database

If you encounter the following warnings after your upgrade, you may need to update the Email Log Database with new values for appliance hostname, management interface IP address, C interface IP address, and device ID:

1. Open SQL Server Management Studio.
2. Click **New Query**.
3. In the query window, enter the following command:

   ```
   USE [esglogdb76]
   ```

   Select the **esg_device_id**, **admin_manage_ip**, and **device_c_port_ip** from the dbo.esg_device_list.
4. Enter **GO**.
5. Locate the **esg_device_id** associated with either the admin_manage_ip or the device_c_port_ip of the source appliance.
6. Execute the following command using the values you obtained in the previous steps:

   ```
   UPDATE dbo.esg_device_list SET esg_name = '<host name>',
   admin_manage_ip = '<appliance management IP address>',
   device_c_port_ip = '<C IP address>' WHERE esg_device_id =
   '<device id>'
   ```
7. Enter **GO**.
8. Run the query.

Content Gateway post-upgrade activities (Forcepoint Web Security only)

After you have finished upgrading components, perform the following.

1. If at the start of the upgrade process you manually moved your existing log files to a temporary location, move them back to **/opt/WCG/logs** and delete the files in the temporary location.
2. Register Content Gateway nodes in the Web module of TRITON Manager on the **Settings > Content Gateway Access** page.

   Registered nodes add a link to the Content Gateway manager logon portal and provide a visual system health indicator: a green check mark or a red X.
3. Configure Content Gateway system alerts on the **Settings > Alerts > System** page in the Web module of the TRITON Manager.

   This subset of Content Gateway system alerts can be configured to be sent to administrators, in addition to being displayed in the Content Gateway manager.
4. If you use SSL support:
   a. If your clients don't yet use a SHA-1 internal Root CA, create and import a SHA-1 Root CA into all affected clients. See Internal Root CA in Content Gateway Help.
   b. Using the notes you compiled prior to upgrade, rebuild your Static Incident list.
5. If you use proxy user authentication, review the settings on the **Global Authentication Options** page (**Configure > Security > Access Control > Global Configuration Options**).
6. If you use IWA user authentication, confirm that the AD domain is still joined. Go to **Monitor > Security > Integrated Windows Authentication**. If it is not joined, rejoin the domain. Go to **Configure > Security > Access Control > Integrated Windows Authentication**.
7. If you use Rule-Based Authentication, review your configuration. Go to **Configure > Security > Access Control**.
   a. Check the **Domains** page.
      - IWA domains that were joined before upgrade should still be joined.
      - LDAP and Legacy NTLM domains should be listed.
   b. Check each rule.
      - Go to the **Authentication Rules** page and enter the editor.
      - Select each rule and check the configuration.
      - For Multiple Realm Authentication rules that used Cookie Mode Caching, check the cookie list on the Global Authentication Option page.
      - Check that the expected domain is in the **Auth Sequence** list.

   Important: The Rule-Based Authentication feature is very rich and can satisfy many user authentication requirements. To make best use of it, please refer to Rule-Based Authentication.

8. If a web protection and data protection solution were deployed together, confirm that Content Gateway has automatically re-registered with the Data module of the TRITON Manager. If it has not, manually re-register.
   a. Ensure that the Content Gateway and the TRITON management server system clocks are synchronized to within a few minutes.
   b. In the Content Gateway manager:
      - Go to **Configure > My Proxy > Basic**, ensure that **Web DLP: Integrated on-box** is enabled, and click **Apply**.
      - Next to **Integrated on-box**, click the **Not registered** link. This opens the **Configure > Security > Web DLP registration** screen.
      - Enter the IP address of the TRITON management server.
      - Enter a user name and password for logging onto the TRITON Manager. The user must be a TRITON AP-DATA (formerly Data Security) administrator with Deploy Settings privileges.
      - Click **Register**. If registration is successful, a message confirms the result and prompts you to restart Content Gateway. If registration fails, an error message indicates the cause of failure. Correct the problem and perform the registration process again.
9. If web and data protection products were deployed together and upgraded, you may need to remove stale entries of Content Gateway instances registered in TRITON AP-DATA system modules:
   a. Log onto the TRITON console.
   b. Select the **Data** tab and navigate to the **Settings > Deployment > Modules** page.
   c. Listed are 2 instances of each Content Gateway module registered with the system. Delete the older instances. You can identify these by looking at the version number.
   d. Click **Deploy**.
10. If web and data protection products were deployed together and configured to use the on-box policy engine, and then reconfigured during upgrade or later to use the ICAP interface, the Content Gateway instance may need to be deleted from the list of TRITON AP-DATA system modules or the deployment will fail. Go to the **Data** > **Settings** > **Deployment** > **System Modules** page, click on the affected Content Gateway instance to open its **Details** page, click **Delete** and then **Deploy**.
11. If your v7.8.4 or higher explicit proxy deployment was customized to support an external load balancer with IWA user authentication, the configuration is preserved during upgrade. You do not need to re-apply the custom configuration. You should, however, test your deployment to verify that the load balancer is performing as expected.
12. With v8.2.x, the basic functionality for 2 features was changed slightly:
    - **Send authentication to parent proxy**, configured on the **Configure > My > Proxy > Basic > General** page
    - **X-Forwarded-For**, enabled on the **Configure > Protocols > HTTP > Privacy**

    In both cases, header values are forwarded only to a configured parent proxy.

If you are upgrading from v7.8.4, v8.0, or v8.1, enabled either of these settings in your previous version, and are expecting header values to be forwarded for all outbound requests, add the appropriate variable to your records.config file (in the **/opt/WCG/config** directory, by default).

- To add the user name to outbound requests, add:

  ```
  CONFIG proxy.config.http.insert_xua_to_external INT
  ```

- To send X-Forwarded-For header values directly to the Internet, add:

  ```
  CONFIG proxy.config.http.insert_xff_to_external INT 1
  ```

13. If you were using v7.8.4, v8.0, or v8.1 with custom cipher list settings using these variables in records.config:

    ```
    proxy.config.ssl.server.cipherlist
    proxy.config.ssl.client.cipherlist
    ```

    you need to reconfigure the custom settings because these variables were replaced in v8.2.

    - proxy.config.ssl.server.cipherlist_suffix replaces proxy.config.ssl.server.cipherlist
    - proxy.config.ssl.client.cipherlist_suffix replaces proxy.config.ssl.client.cipherlist

    The non-default cipher list in use prior to upgrade is saved for reference as a comment in records.config. Default values for the new variables are put place during the upgrade and can be reconfigured after the upgrade is complete.

    See Content Gateway Manager Help for more information on how these new variables now work with proxy.config.ssl.server.cipherlist_option and proxy.config.ssl.client.cipherlist_option to create cipher lists.

14. The **Tunnel Skype** option on the **Configure > Protocols > HTTPS** page of Content Gateway Manager is no longer available in v8.3. Variables stored in the records.config file that apply to Skype are removed during the upgrade process.
15. The settings on the **Configure > Networking > Connection Management > Low Memory Mode** page of Content Gateway manager are no longer available in v8.3. Corresponding variables stored in the records.config file are removed by the upgrade.
16. If **LOW** encryption cipher suites was previously selected on the **Configure > SSL > Decryption/Encryption > Inbound** or **Outbound** pages of Content Gateway manager, the v8.3 upgrade process will change the setting to **MEDIUM**. LOW is no longer a valid option on those pages.

    The corresponding records.config variables are also updated by the upgrade.
17. During upgrade to v8.3, the **Enable the certificate verification engine** on the **Configure > SSL > Validation > General** page of Content Gateway manager will be changed to ON for any customer who does not already have the feature enabled.
18. In v8.3, improvements were made to the Adaptive Redirection Module (ARM). The ARM component now utilizes iptables, policy routing, and transparent sockets which are configured during product installation or upgrade.

    The Content Gateway Manager has been changed to reflect these improvements.

- The **Network Address Translation (NAT)** section of the **Configure > Networking > ARM > General** page has been renamed to **Redirection Rules** to better reflect the contents of the table.
- Text on that page has also been updated.

To facilitate interception and redirection of traffic:

- IPTables rules are configured during upgrade.
  - Forcepoint IPTables chains are inserted.
  - Forcepoint IPTables rules are also inserted into existing chains.
  - Forcepoint chains and rules use “NC_” as a prefix for identification purposes.
- IPTables rules configured outside of Content Gateway Manager must
  - Be inserted *after* Forcepoint rules.
  - Never be added to Forcepoint chains.
- Forcepoint chains and rules should never be edited.
- If customized chains or rules impact the Forcepoint configuration, navigate to /opt/wcg/bin and execute the following to re-establish the Forcepoint IPTables chains and rules:

  ```
  netcontrol.sh -r
  ```

For some customers, the GRE **Packet Return Method** (GRE return) may not be as expected. In all cases, GRE return, as documented by Cisco (see this site), is fully functional. However, tunneling back through a router (enhanced GRE tunnel return) now requires a specific kernel module. This module is only available on a Forcepoint appliance. Contact Forcepoint Technical Support to enable this functionality in a software deployment.

To provide more appropriate statistical data for the new ARM, the **Bypass Statistics** now provide information for:

- Total Packets Bypassed
- Packets Dynamically Bypassed
- DNS Packets Bypassed
- Packets Shed

Move Forcepoint URL Filtering and upgrade the appliance

Use this procedure if you are moving Forcepoint URL Filtering to a new TRITON appliance.

1. *Set up the new Forcepoint URL Filtering appliance*, page 28
2. *Back up Forcepoint URL Filtering on the dual-mode appliance*, page 28
3. *Restore the backup on the new appliance*, page 29
4. *Prepare Forcepoint URL Filtering for upgrade*, page 30

5. *Upgrade the new Forcepoint URL Filtering appliance*, page 34
6. *Remove Forcepoint URL Filtering from the dual-mode appliance*, page 34
7. *Prepare Forcepoint Email Security for upgrade*, page 35
8. *Upgrade Forcepoint Email Security*, page 36
9. *Perform post-upgrade activities*, page 37

Set up the new Forcepoint URL Filtering appliance

Procure and set up a new V-Series appliance with the same version of Forcepoint URL Filtering that's running on the dual-mode appliance.

Important

Contact your Forcepoint account representative to learn about special promotions for dual-mode upgrades to v8.4.

1. Install and cable the appliance. Refer to Quick Start poster included in the appliance shipping container. **Do not run firstboot.**
2. Re-image the appliance to the version currently running on the dual-mode appliance. Follow the instructions in this Forcepoint knowledge base article: How to restore a V-Series appliance to a factory image.
3. After the appliance is re-imaged, run **firstboot**. Be sure to configure the appliance for Forcepoint URL Filtering only (Web Security with 7.8.4).

   Specify a unique C interface IP address. The C interface IP address will change to the dual-mode C interface IP address as part of the migration process. This is because changing the C interface IP address in a web protection deployment is complicated, whereas changing it in an email protection deployment is simple.

   There is no need to perform additional configuration on the appliance.

Back up Forcepoint URL Filtering on the dual-mode appliance

1. Log on to the Appliance Manager for the dual-mode appliance.
2. Go to **Administration > Backup Utility**, perform a **Web Configuration** backup, and save the backup file to an off-appliance location. A **Web Configuration** backup saves all client and policy data stored on the appliance, including the Network Agent configuration (if used).
   a. In the Appliance Manager, go to the **Administration > Backup Utility > Backup** page.
   b. In the Perform Backup section, for Backup Type select **Web Configuration**, and then click **Run Backup Now**.
   c. To download the file, in the Local Backup Files area, select **Web Configuration** and click on the backup file name (shown as a link).

3. Go to **Configuration > Network Interfaces** and document the interface settings. The new appliance will use the dual-mode interface settings, and the dual-mode appliance will configure new settings.
4. Shut down the dual mode appliance. Go to **Status > General** and click **Shut Down Appliance**. This is done to facilitate the network interface setting changes.

Restore the backup on the new appliance

The restore procedure includes stopping and starting off-appliance TRITON web protection services.

To restore the Web Configuration backup file created in the previous step:

1. Use the **WebsenseAdmin stop** command to stop all software components running off the appliance.

   For example, stop Log Server, Sync Service, Linking Service, transparent identification agents, and components on the TRITON management server machine.

   - Windows: Navigate to the C:\Program Files *or* Program Files (x86)\Websense\Web Security\ folder.
   - Linux: Navigate to the /opt/Websense/ directory.
2. Open the Appliance Manager for the new appliance and go to **Administration > Backup Utility**.
3. Click the **Restore** tab and select **Web Configuration** from the **Select restore mode** list.

   The current appliance version must match the version associated with the backup file. Thus, a version 8.1 backup can be restored only to an appliance that is at version 8.1.
4. Click **Run Restore Wizard** and select the **Another location** radio button to indicate where the backup file is stored. Then click **Next**.
5. Browse to the location of the backup file on the remote machine, select it, and then click **Next**.
6. Verify the details on the Confirm page, and then click **Restore Now**. When the restore is complete, the new appliance has the same configuration as the instance on the dual-mode appliance. That instance is removed in a later step.
7. When the restore is complete, go to **Configuration > Network Interfaces** and configure the network interfaces with the settings you documented on the dual-mode appliance.
8. Restart the appliance.
9. Use the **WebsenseAdmin start** command to start the components that run off the appliance.
   - Windows: Navigate to the C:\Program Files *or* Program Files (x86)\Websense\Web Security\ folder.
   - Linux: Navigate to the /opt/Websense/ directory.

Prepare Forcepoint URL Filtering for upgrade

Off-appliance components

1. Verify that third-party components, including your database engine and directory service, are supported with Forcepoint URL Filtering. See Requirements for web protection solutions.
2. Back up **all of your web protection components** before starting the upgrade. See the **Backup and Restore FAQ** for your version for instructions for backing up both software-based and appliance-based components.

   On the new appliance, in the Appliance Manager perform a **Full Appliance Configuration** backup and save it to an off-appliance location.
3. Before upgrading Filtering Service, make sure that the Filtering Service machine and the TRITON management server have the same locale settings (language and character set).

   After the upgrade is complete, Filtering Service can be restarted with any locale settings.
4. When upgrading to v8.4, a new logging partition is added to your Log Database. Please make sure you do not have 70 active partitions (the limit) prior to upgrading. Use the **Web > Settings > Reporting > Log Database** page of the TRITON Manager to disable at least one active partition prior to upgrading.
5. Back up your current Log Database and stop Log Server.

   Warning

   If database operations are active during upgrade, the Log Database may be rendered unusable.

   When this occurs, it can be difficult to fix.

   Make **sure** to stop Log Server and the database jobs, as described below, before upgrading the database.

   a. Back up your reporting databases.

      Refer to Microsoft documentation for instructions. The databases are named wslogdb70 (the catalog database), wslogdb70_*n* (standard logging partition databases), and wslogdb70_amt_1 (threats partition database).

   b. On the Log Server machine, use the Windows Services tool to stop **Websense Log Server**.
6. It is best to **stop all Log Database jobs** prior to starting the upgrade, but, before it upgrades the Log Database, the upgrade process will attempt to stop any Log Database jobs not already stopped. If the jobs cannot be stopped, you will need to stop them manually. However, you do not need to exit the installer to do that.

Stop the Log Database jobs using these steps:

a. If you have a **full version of Microsoft SQL Server** (not Express), stop **all database jobs** as follows. (See below for steps to stop SQL Express jobs.)
   - Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).
   - To disable all currently active SQL Server Agent jobs, right-click each of the following jobs and select **Disable**:

     Websense_ETL_Job_wslogdb70

     Websense_AMT_ETL_wslogdb70

     Websense_IBT_DRIVER_wslogdb70

     Websense_Trend_DRIVER_wslogdb70

     Websense_Maintenance_Job_wslogdb70

     Disabling the jobs prevents them from executing at the next scheduled time, but does not stop them if a job is in process.

     Make sure all jobs have completed any current operation before proceeding with upgrade.
   - After upgrade, verify that the jobs have been enabled.

     Enable any that were not automatically enabled by the upgrade process. Normal database operations will then resume.

b. If you have **SQL Server Express, stop all database jobs** as follows:
   - Log in to the Microsoft SQL Server Management Studio.
   - Expand the **Databases** tree to locate the catalog database (wslogdb70, by default), then expand the catalog database node.
   - Expand **Service Broker > Queues**.
   - Right click **dbo.wse_scheduled_job_queue** and select **Disable Queue**.
   - The upgrade process will re-enable the job queue. After upgrade, verify that the Queue has been enabled.

     Enable it, if necessary, by repeating the process, this time ultimately selecting **Enable Queue** to resume normal database operations.

When Log Server is upgraded, the upgrade process first checks the Log Database version and updates the database, if necessary. If you have multiple Log Servers, the database update occurs with the first Log Server upgrade. The database update, including the need to stop the database jobs, is not repeated when additional Log Server instances are upgraded.

7. If Log Server uses a Windows trusted connection to access the Log Database, be sure to log on to the Log Server machine using the trusted account to perform the upgrade. To find out which account is used by Log Server:
   a. Launch the Windows Services tool.
   b. Scroll down to find **Websense Log Server**, then check the **Log On As** column to find the account to use.

Important

As a result of a change made to avoid a potential vulnerability when a presentation report is included as a link in an email, report links in emails that exist prior to upgrading to v8.3 will no longer work.

Appliance components

Configure and test access to the appliance command-line interface (CLI)

At the end of the upgrade procedure you will need to log on to the upgraded, v8.4 appliance CLI and perform a small number of tasks.

The v8.3 appliance CLI is accessed in the same way as the existing V-Series CLI. If you haven't used the V-Series CLI, or haven't accessed it recently, test your access now and perform any necessary configuration.

SSH access

All V-Series appliances can connect to the CLI with a terminal emulator and SSH. The client machine must be in a network that has a route to the appliance and SSH access must be enabled on the dual-mode appliance in the Appliance Manager.

In the Appliance Manager, check the SSH access setting and, if necessary, enable SSH access.

1. Log on to the Appliance Manager and go to the **Administration > Toolbox** page.
2. In the **Appliance Command Line** section, enable SSH remote access.

Test SSH access

1. On a Windows system connect with **PuTTY,** or similar. On a Mac system connect with **Terminal**.
2. Connect to the appliance management interface (C) IP address on port 22.
3. Log on with the **admin** credentials.

iDRAC access

Most V-Series models supported by v8.3 have an integrated DELL Remote Access Controller (iDRAC). If you have never worked with the iDRAC, see **Using the iDRAC** in Forcepoint Appliances Getting Started.

To access the CLI, log on to the iDRAC and go to **Overview > Server**. In the upper right **Virtual Console Preview** area, click **Launch**.

VGA and USB direct connect

Connect a monitor and keyboard directly to the appliance.

Serial port direct connect

Configure a serial connection to a monitor and keyboard. The connection should be set to:

- 9600 baud rate
- 8 data bits
- no parity

Appliance customizations

Important

Customizations are not retained through the upgrade process.

Before upgrading, inventory all customizations and make a plan for restoring any that are required.

Customizations can include:

- Custom patches
- Hand updated files
- Extra packages added by hand
- Extra files added, binary or configuration

Post-upgrade, Forcepoint Technical Support may be able to help restore some files from your pre-upgrade file system.

SNMP settings

Warning

Upgrade to v8.3.0 does not preserve SNMP settings.

A fix is in development. Please check the Forcepoint Knowledge Base or contact Technical Support to see if a hotfix is available.

Before upgrading, document your existing SNMP settings for reapplication after upgrade.

Upgrade the new Forcepoint URL Filtering appliance

The new Forcepoint URL Filtering appliance can now be upgraded to v8.4 using the standard upgrade procedure. See Upgrade Instructions for Forcepoint URL Filtering (also applies to v7.8.4 Web Security).

Components must be upgraded in the following order:

- Policy Broker machine
- Policy Server machines
- Filtering Service, Network Agent, and User Service machines
- Log Server
- TRITON management server (already upgraded if it hosts Policy Broker)
- Any additional components

Important

When the upgrade is complete, shut down the appliance.

This allows the dual-mode appliance to be booted, converted to a single-mode appliance, and upgraded to v8.4. The network interfaces are also reconfigured as part of the process.

Remove Forcepoint URL Filtering from the dual-mode appliance

After Forcepoint URL Filtering is migrated to the new appliance and upgraded, a hotfix is used to remove the web module from the dual-mode appliance, converting the appliance to a single-mode Forcepoint Email Security appliance that can be upgraded to v8.4 with the standard upgrade procedure.

When the hotfix is installed it immediately removes the web module and reboots the appliance. The action cannot be undone.

To install the hotfix:

1. Confirm that the new Forcepoint URL Filtering appliance is shut down.
2. Boot the dual-mode appliance and log in to its Appliance Manager. (At this point it still has the same C interface IP address as the new appliance.)
3. Go to the **Administration > Patches / Hotfixes > Hotfixes** page.
4. Enter the hotfix name in the search box at the top of the screen:

   APP-*x.x.x*-555

   Where *x.x.x* is the version of Forcepoint URL Filtering currently running on the dual-mode appliance.
5. Click **Find**. If the hotfix is not found, ensure that the name is entered correctly.
6. In the pop-up display, click **Download** to download the hotfix.

If you downloaded the hotfix package to a local directory, you can use the **Upload Hotfix Manually** button to upload the hotfix.

7. Click **Install** to install the hotfix. Installation removes Forcepoint URL Filtering and all associated files. This action cannot be undone. When installation is complete, the appliance restarts automatically to complete the action. The appliance may restart before the Appliance Manager confirms that installation is complete.

After the appliance completes its restart, Forcepoint Email Security can be prepared for upgrade.

Prepare Forcepoint Email Security for upgrade

Several issues should be considered before you begin the Forcepoint Email Security 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 Forcepoint Email Security ports for information about all email protection system default ports, including appliance interface designations and communication direction.
- The upgrade to version 8.4 renames the following 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.
- The upgrade to version 8.4 adds a default Spoofed Email policy filter, a Spoof policy action, and an Antispoof policy rule. If you currently have policy elements with these names, you should change them before the upgrade process begins, to avoid having duplicate names after the upgrade.
- New presentation reports are added in version 8.4 for spoofed email and URL analysis data. Examples include:

  Outbound Spoofed Email Percentage Summary

  Top Inbound Spoofed Email Sender Domains

  Top Inbound Recipients of Spoofed Email

  Top Outbound Embedded URL Categories Detected

Outbound Embedded URL Detection Volume Summary

The upgrade process may not be successfully completed if you have existing custom reports with the same names as the new version 8.4 reports.

- **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 Forcepoint Email Security

With the web module removed, Forcepoint Email Security is now hosted on a single-mode appliance that can be upgraded to v8.3 using the standard upgrade procedure. See Upgrade Instructions for Forcepoint Email Security for complete upgrade instructions.

When the upgrade is complete, reconfigure the network interface settings (C, P1/E1, P2/E2).

1. Log on to the CLI of the upgraded Forcepoint Email Security appliance and elevate to config mode.

   ```
   (view)# config
   ```

   You are prompted for a password. Enter the admin password.
2. Use the **set interface ipv4** command to configure the C, P1/E1, P2/E2 interfaces (P2/E2 optional). E1 and E2 are used on the V10000. P1 and P2 are used on the V5000.

   ```
   set interface ipv4 --interface <c|p1|p2|e1|e2>
    --ip <ipv4_address> --mask <ipv4_netmask>
    [--gateway <ipv4_address>]
   ```

   For example:

   ```
   (config)# set interface ipv4 --interface c
             --ip 10.200.200.10 --mask 255.255.0.0
             --gateway 10.200.0.5
   ```

   To display the interface settings:

   ```
   show interface info
   ```

3. When the interfaces are configured, restart the appliance.
4. Boot the Forcepoint URL Filtering appliance and proceed to the post-upgrade activities.

Perform post-upgrade activities

Appliance activities should be performed on both the Forcepoint Email Security appliance and the Forcepoint URL Filtering appliance.

- *Appliance post-upgrade activities*, page 37
- *Forcepoint Email Security post-upgrade activities*, page 38

Appliance post-upgrade activities

In the CLI

Elevate to **config** mode and perform system checks and verify some configuration settings.

- System information

  ```
  show appliance info
  ```

  Results may be similar to:

  ```
  Uptime              : 0 days, 2 hours, 13 minutes
  Hostname            : webapp.example.com
  Hardware_platform   : V10000 G4
  Appliance_version   : 8.3.0
  Mode                : Forcepoint Web Security
  Policy_mode         : Filtering only
  Policy_source_ip    : 10.222.21.10
  ```

- Upgrade history

  ```
  show upgrade --history
  ```

- Appliance status

  ```
  show appliance status
  ```

  ```
  show <module>
  ```

  If expected system services are not running, restart the module that hosts the service

  ```
  restart <module>
  ```

- Network interface settings

  ```
  show interface info
  ```

- Check and synchronize the system time

  ```
  show system ntp
  ```

  ```
  show system clock
  ```

  ```
  show system timezone
  ```

  If the clock is off and NTP is configured, sync with:

  ```
  sync system ntp
  ```

Otherwise, to sync when the time is set manually, see **System time and time synchronization with TRITON servers** in Forcepoint Appliances Getting Started.

- Configure a **filestore**. A **filestore** is an off-appliance location for storing appliance-related files, including backup, log, and configuration files.

  Establishing a filestore is essential for saving and loading files.

  A filestore definition includes:

  - A unique name, known as the filestore alias.
  - The IP address of the filestore host and the port on which to connect.
  - The directory location (path or share) on the host.
  - The protocol to use to connect and move files to and from the filestore. Supported protocols include **ftp**, **tftp**, and **samba**.
  - Optionally, the name of a user (account) with permissions on the filestore.

  To define a filestore:

  ```
  set filestore --alias <filestore_alias>
     --type <ftp|tftp|samba> --host <ip_address>
     --path <share_directory>
     [--user <user_name>] [--port <port>]
  ```

  Example:

  ```
  set filestore --alias fstore --type samba
     --host 10.123.48.70 --path myfiles/myfolder
     --user jdoe
  ```

- If you integrate with a SIEM, configure SNMP polling and alerting. Use the documentation created in the pre-upgrade activity. See, also, **SNMP polling and alerting** in Forcepoint Appliances Getting Started.

In TRITON Manager

- Register your appliances. Log on to TRITON Manager and go to the **Appliances** tab to register your appliances.
- If you have *User directory and filtering* appliances, go to the Web module **Settings > General > Policy Servers** page, and add the Policy Server instances.
- For Forcepoint Email Security, go to the Email module, go to **Settings > General > Email Appliances** and click on the host name link to delete the appliance. Log off and then back on to TRITON Manager and add the appliance's new C interface IP address.

Forcepoint Email Security post-upgrade activities

Perform the following tasks in the TRITON Manager:

- Redirect email traffic through your system to ensure that it performs as expected.
- *Update data loss prevention policies and classifiers*
- *Update Forcepoint databases*
- *Update Email module backup file*

- *Update appliance management interface configuration settings*
- *Configure email DNS lookup*
- *Update Log Database*

Update data loss prevention policies and classifiers

1. In TRITON Manager, select the Data module.
2. Follow the prompts 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. When finished, 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 v8.1, 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 v8.x. 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 v8.4 on the **Settings > General > Backup/Restore** page.

Update appliance management interface configuration settings

Data loss prevention

Re-register the Forcepoint Email Security appliance with the Data module as follows:

1. In TRITON Manager, select the Email module and navigate to the **Settings > General > Data Loss Prevention** page.
2. Click **Unregister** to remove the DLP registration.
3. In the TRITON Data module, navigate to the **Settings > Deployment > System Modules** page. Select the Forcepoint Email Security module.
4. In the upper left corner, click **Delete**.

5. In the TRITON Email module **Settings > General > Data Loss Prevention** page, ensure the appliance management (C) interface IP address appears in the **Communication IP address** field.
6. Click **Register** to register the appliance with the Data module.
7. Select the Data module and click **Deploy**.

Email hybrid service

Re-register the Forcepoint Email Security appliance with the email hybrid service as follows:

1. In TRITON Manager, select the Email module and navigate to the **Settings > Hybrid Service > Hybrid Configuration** page.
2. Click **Edit** at the bottom of the page.
3. Replace the SMTP server IP address with the new C interface IP address.
4. Click **OK**.

Personal Email Manager notification message

You may need to enter your destination appliance management interface IP address for the proper distribution of Personal Email Manager notification messages.

1. In TRITON Manager, select the TRITON Email module and navigate to the **Settings > Personal Email > Notification Message** page.
2. Enter the new appliance management (or C) interface in the **IP address or hostname** entry field.
3. Click **OK**.

Configure email DNS lookup

The appliance firstboot process includes the entry of DNS server settings. You can enhance DNS lookup query performance by configuring a second set of DNS server entries specifically for the Email module. In the Forcepoint Email Security appliance CLI, use the following commands, as needed:

```
set interface dns --module email --dns1  <DNS_IP>
set interface dns --module email --dns2  <DNS_IP>
set interface dns --module email --dns3  <DNS_IP>
```

Update Log Database

If you encounter the following warnings after your upgrade, you may need to update the Email Log Database with new values for appliance hostname, management interface IP address, C interface IP address, and device ID:

1. Open SQL Server Management Studio.
2. Click **New Query**.
3. In the query window, enter the following command:

   ```
   USE [esglogdb76]
   ```

   Select the **esg_device_id**, **admin_manage_ip**, and **device_c_port_ip** from the dbo.esg_device_list.
4. Enter **GO**.
5. Locate the **esg_device_id** associated with either the admin_manage_ip or the device_c_port_ip of the source appliance.
6. Execute the following command using the values you obtained in the previous steps:

   ```
   UPDATE dbo.esg_device_list SET esg_name = '<host name>',
   admin_manage_ip = '<appliance management IP address>',
   device_c_port_ip = '<C IP address>' WHERE esg_device_id =
   '<device id>'
   ```
7. Enter **GO**.
8. Run the query.

Removing an unused module

If a module on your dual-mode appliance is not used, in many cases you can remove it and upgrade directly to version 8.4.

Appliance Model	Dual-Mode Configuration: Forcepoint URL Filtering + Email Security	Dual-Mode Configuration: Web Security + Email Security
V5000	URL Filtering can be removed with a hotfix	Not applicable. This combination is not supported on a V5000.
	Email Security can be removed with a hotfix	
V10000	URL Filtering can be removed with a hotfix	Removing Web Security requires re-imaging the appliance
	URL Filtering must be re-hosted; it is not supported standalone on a V10000	Email Security can be removed with a hotfix

See:

- *Removing Forcepoint Email Security*, page 42
- *Removing Forcepoint URL Filtering*, page 43.
- *Removing Forcepoint Web Security*, page 44

Removing Forcepoint Email Security

If you are not using the email module on your

- V5000 Forcepoint URL Filtering dual-mode appliance, or
- V10000 Forcepoint Web Security dual-mode appliance

...you can remove the email module with a hotfix, converting it to a single-mode web protection appliance. You can then upgrade the web protection module to v8.4 using the standard upgrade procedure.

When the hotfix is installed it immediately removes the email module and reboots the appliance. The action cannot be undone.

The hotfix is specific to the V-Series model (V5000 or V10000) and current TRITON software version (7.8.4, 8.0.0, 8.0.1, 8.1.0, 8.2.0, 8.3.0). Be sure to download the correct hotfix for your dual-mode appliance and software version.

- Hotfix 333 is for V10000 dual-mode only. It removes Forcepoint Email Security and its related files. This cannot be undone.
- Hotfix 777 is for V5000 dual-mode only. It removes Forcepoint Email Security and its related files. This cannot be undone.

To install the hotfix:

1. Log on to the dual-mode Appliance Manager, go to **Status > General**, and stop all TRITON-AP EMAIL services.
2. Go to the **Administration > Patches / Hotfixes > Hotfixes** page.
3. Enter the hotfix name in the search box at the top of the screen:

   APP-*x.x.x-yyy*

   Where *x.x.x* is the version of Forcepoint Email Security currently running on the dual-mode appliance, and *yyy* is:

   333 for V10000

   777 for V5000

   For example: APP-8.1.0-333 for a V10000 dual-mode appliance running TRITON AP-EMAIL v8.1.0.
4. Click **Find**. If the hotfix is not found, ensure that the name is entered correctly.
5. In the pop-up display, click **Download** to download the hotfix.
6. Click **Install** to install the hotfix. Installation removes the email module and all associated files. This action cannot be undone. When installation is complete, the appliance restarts automatically to complete the action. The appliance may restart before the Appliance Manager confirms that installation is complete.

After the appliance completes its restart, the web protection module can be upgraded.

For Forcepoint Web Security, see Upgrade Instructions for Forcepoint Web Security (also applies to v7.8.4 Web Security Gateway/Anywhere).

For Forcepoint URL Filtering, see Upgrade Instructions for Forcepoint URL Filtering (also applies to v7.8.4 Web Security).

Removing Forcepoint URL Filtering

If you are not using the Forcepoint URL Filtering module on your V5000 or V10000 dual-mode appliance, you can remove it with a hotfix, converting it to a single-mode Forcepoint Email Security appliance, and upgrade it to v8.4 using the standard upgrade procedure.

When the hotfix is installed it immediately removes Forcepoint URL Filtering and reboots the appliance. The action cannot be undone.

To install the hotfix:

1. Log on to the dual-mode Appliance Manager, go to **Status > General**, and stop all Forcepoint URL Filtering and Network Agent services.
2. Go to the **Administration > Patches / Hotfixes > Hotfixes** page.
3. Enter the hotfix name in the search box at the top of the screen:

   APP-*x.x.x*-555

   Where *x.x.x* is the version of Forcepoint URL Filtering currently running on the dual-mode appliance.

4. Click **Find**. If the hotfix is not found, ensure that the name is entered correctly.
5. In the pop-up display, click **Download** to download the hotfix.

   If you downloaded the hotfix package to a local directory, you can use the **Upload Hotfix Manually** button to upload the hotfix.
6. Click **Install** to install the hotfix. Installation removes Forcepoint URL Filtering and all associated files. This action cannot be undone. When installation is complete, the appliance restarts automatically to complete the action. The appliance may restart before the Appliance Manager confirms that installation is complete.

After the appliance completes its restart, Forcepoint Email Security can be upgraded using the standard procedure. See Upgrade Instructions for Forcepoint Email Security.

Removing Forcepoint Web Security

When Forcepoint Web Security is unused on a V10000 dual-mode appliance, it can only be removed by re-imaging the appliance.

The procedure is:

1. In the Appliance Manager, perform an **Email Configuration** backup and save the backup file to a location off of the appliance.
2. Document all of the current interface settings.
3. Re-image the appliance to the version of Forcepoint Email Security currently running on the appliance. Follow the instructions in this Forcepoint knowledge base article: How to restore a V-Series appliance to a factory image.

   Perform firstboot, select email mode, and configure the C interface with the same values as when in dual-mode.
4. Restore the **Email Configuration** backup and restart the appliance.
5. After the appliance completes its restart, Forcepoint Email Security can be upgraded using the standard v8.4 upgrade procedure. See Upgrade Instructions for TRITON AP-EMAIL.

Release Notes for 8.x releases

Review the Release Notes for the TRITON solutions on your appliances. New features may require configuration to be put into effect.

Version 8.4.0

- v8.4.0 Forcepoint Web Protection Release Notes
- v8.4.0 Forcepoint Email Security Release Notes
- v8.4.0 Forcepoint DLP Release Notes

Version 8.3.0

- v8.3.0 TRITON AP-WEB Release Notes
- v8.3.0 TRITON AP-EMAIL Release Notes
- v8.3.0 TRITON AP-DATA Release Notes

Version 8.2.0

- v8.2.0 TRITON AP-WEB Release Notes
- v8.2.0 TRITON AP-EMAIL Release Notes
- v8.2.0 TRITON AP-DATA Release Notes

Version 8.1.0

- v8.1.0 TRITON AP-WEB Release Notes
- v8.1.0 TRITON AP-EMAIL Release Notes
- v8.1.0 TRITON AP-DATA Release Notes

Version 8.0.x

- v8.0.1 TRITON AP-WEB Release Notes
- v8.0.0 TRITON AP-WEB Release Notes
- v8.0.1 RITON AP-EMAIL Release Notes
- v8.0.0 TRITON AP-EMAIL Release Notes
- v8.0.1 TRITON AP-DATA Release Notes
- v8.0.0 TRITON AP-DATA Release Notes