FORCEPOINT
POWERED BY Raytheon

V Series, X Series, and Virtual Appliance Upgrade Guide

Forcepoint Web Security, Forcepoint Email Security

Upgrades from 8.3.x to 8.4.x

Published 2017

D120517840

Contents

Upgrading V Series, X Series, and Virtual Appliances to version 8.4.0

V Series, X Series, and Virtual Appliances can be upgraded directly to v8.4.0 from v8.3.x.

Important

When performing the upgrade, always start with the Forcepoint solution upgrade guide.

- Upgrading web protection solutions
- Upgrading email protection solutions

The v8.4 upgrade package is a now a single file that upgrades all installed modules at the same time. Modules cannot be upgraded individually. Modules include:

- **App** — Base appliance infrastructure and appliance controller

TRITON AP-WEB:

- **Web** — TRITON AP-WEB core components
- **Proxy** — Content Gateway web proxy

TRITON AP-EMAIL:

- **Email** — TRITON AP-EMAIL core components

Important

The upgrade process is designed for appliances running in a functional deployment. Required network interfaces must have reliable connections to Forcepoint components and the Internet.

Upgrading does not repair a non-functional system.

Important

Service disruption during upgrade

Appliance services are not available while the upgrade is applied, continuing until the appliance completes its final restart.

Service is not disrupted while the off-box components are upgraded

Important

If you are currently using **link aggregation** and plan to enable VLAN support after upgrade, disable link aggregation before enabling VLAN support on the blade or chassis.
Note: VLAN is only available on X-series appliances

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.

Important

Forcepoint V5000 G2R2 customers must uninstall 8.3 Appliance Hotfix 12 (APP-8.3.0-012) if it is installed. The v8.4 upgrade will automatically include the necessary resolution, so no other hotfix is needed.

Important

Any appliance with Hotfix 200 (Spectre/Meltdown Hotfix) installed must uninstall the hotfix before upgrading to v8.4. After upgrading, Hotfix 200 must be reinstalled on the new version.

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.

Summary of upgrade procedure

1. Perform *Pre-upgrade activities*, page 5.

If you are upgrading a deployment that includes Forcepoint Web Security, upgrade the *Full policy source* machine (Policy Broker/Policy Database). If the *Full policy source*

is located on an off-appliance server, follow the instructions in Upgrade Instructions for Forcepoint Web Security. If the *Full policy source* machine is an X10G, upgrade that blade first.

> **Important**
>
> All Forcepoint components on the *Full policy source* machine are upgraded when Policy Broker and Policy Database are upgraded.
>
> The upgraded Policy Broker and Policy Database services must be running and available for appliance upgrades to succeed.

1. Download the upgrade package and install it.
2. Perform *Post-upgrade activities*, page 9.
3. Upgrade the Forcepoint management server (if not upgraded when Policy Broker/ Policy Database were upgraded), and other servers that host Forcepoint components.

For detailed, step-by-step instructions, see *Upgrade procedure*, page 7.

Rollback

When the upgrade is applied, the original file system is preserved. Should the upgrade procedure experience a fatal error, the original file system is restored. Note that off-appliance components may need to be restarted.

Pre-upgrade activities

Before applying the v8.4.x upgrade, perform the following tasks and be aware of the following issues.

Important

When upgrading from v7.8.3, v8.0.0, or v8.0.1 (or any version that first requires an upgrade to v8.3.0) to v8.4.x, in order to retain SNMP configuration, you must install two hotfixes while the appliance is still running version 8.3. Hotfix files are available in the Appliance v8.3.0 section of the Forcepoint Downloads page.

Before upgrading from v8.3.0 to v8.4.0:

1. Install Appliance Hotfix 01 (APP-8.3.0-001)
2. Restart the appliance
3. Install Appliance Hotfix 90 (APP-8.3.0-090)

If you're not already familiar with the preparation required for upgrade of off-appliance components, review those requirements before upgrading your appliances.

- For web protection solutions, see Before upgrading v8.4.x web protection solutions and v8.4.0 Web Protection Release Notes.
- For Forcepoint Email Security, see Upgrading email protection solutions and v8.4.0 Forcepoint Email Security Release Notes.

Inventory 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
- 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.

Content Gateway Integrated Windows Authentication (IWA) settings

Forcepoint Web Security only: If you use IWA, make a record of the current settings before starting the upgrade.

IWA domain joins should be preserved through the upgrade process. However, in case there is a connectivity problem and IWA domain joins are dropped, it is prudent to document the current settings. Keep the record where you can easily retrieve it after the upgrade.

Back up appliance configuration and settings

It's very important to perform a full appliance configuration backup and save it to a filestore.

1. Log on to the CLI and elevate to **config** mode.
2. To perform an immediate full backup use:

   ```
   create backup now --location filestore_alias
     [--desc "<description>"]
   ```

   Including a unique description makes it easier to identify backup files that may have very similar names and dates.

Unified Appliance Installer for v8.4.0

Starting with v8.4.0, the appliance recovery and upgrade logic has been merged within a unified appliance installer file.

Forcepoint Appliance upgrades to version 8.4.0 and later require different file types (ISO or RPM) depending on the Appliance version from which you are upgrading.

Upgrades from Appliance versions 8.2.x and previous require the RPM file type to upgrade to Appliance version 8.4.0 and later releases. This RPM file ("v8.4.0 Universal upgrade patch for V/X Series Appliances") is available on the Forcepoint Downloads page.

Upgrades from Appliance version 8.3.x require the ISO file type to upgrade to Appliance version 8.4.0 and later. This ISO file ("v8.4.0 Unified Appliance Installer") is available on the Forcepoint Downloads page.

Upgrade procedure

Important

Appliance services are not available while the upgrade is being applied. Disruption continues until the appliance completes its final restart.

It is a best practice to perform the upgrade at a time when service demand is low.

Note

OVA images downloaded before June 2, 2017 should use the migration process described in the KBA titled "Migrating from a v8.3 Email Virtual Appliance (initial image) to v8.4".

OVA images downloaded June 2, 2017 or later can upgrade to 8.4 through the appliance upgrade file.

1. Download the v8.4.x Forcepoint Security Installer to a location where it is easy to copy it to Windows servers hosting Forcepoint web, email, and data components, such as TRITON Manager (renamed Forcepoint Security Manager in v8.4) and Log Server.
2. Perform *Pre-upgrade activities*, page 5.

3. If your deployment includes Forcepoint Web Security, you must upgrade the policy source machine (Policy Broker/Policy Database) before upgrading web protection components on your security blades. If the *Full policy source* machine is an X10G, upgrade that blade first. After upgrading the policy source machine, confirm that Policy Broker and Policy Database services are running.

   Important
   All Forcepoint components on the Full policy source machine are upgraded when Policy Broker/Policy Database are upgraded.

   In all instances, you must upgrade Forcepoint Web Security components in the following order:

   a. *Full policy source*

      Upon completion, confirm that Policy Broker and Policy Database services are running. See Upgrading Web Protection Solutions.

   b. *User directory and filtering* (sometimes called *policy lite*) blades and non-appliance servers that host Policy Server

   c. *Filtering only* blades, and non-appliance servers that host Filtering Service

   d. Off-appliance servers hosting other web protection components (like Log Server or Logon Agent)

   Important
   Successful upgrade of *User directory and filtering* and *Filtering only* appliances require connectivity with the Policy Broker and Policy Database services.

4. If the appliance is registered in Forcepoint Security Manager, in Forcepoint Security Manager go to **Appliances > Manage Appliance** and unregister the appliance. Re-registration is a post-upgrade activity.

   If the appliance is a *User directory and filtering* appliance, unregister the appliance. In the Web module of Forcepoint Security Manager, go to the **Settings > General > Policy Servers** page and unregister the appliance.

5. Download and apply the v8.4 upgrade.

   a. Download the upgrade file.

      ```
      load upgrade
      ```

   b. Install the upgrade.

      ```
      install upgrade
      ```

      Select the v8.4.0 upgrade file from the list.

      When prompted, confirm to continue, then accept the subscription agreement.

      The upgrade performs several system checks. The checks may take several minutes.

      When installation is complete, the appliance automatically restarts.

If the upgrade fails, the blade server automatically rolls back to the prior version. If the source of the failure is not obvious or cannot be easily addressed, contact Forcepoint Technical Support.

If an error message displays, indicating that ISO verification has failed, repeat the command with the parameter --force <iso_file_name>.

If installation seems to stop, allow the process to run for at least 90 minutes. If installation has not completed in that time, contact Forcepoint Technical Support.

6. Perform *Post-upgrade activities*, page 9.
7. Return to Step 5 and upgrade remaining appliances.
8. Upgrade the management server (if not upgraded when Policy Broker/Policy Database were upgraded), and other servers that host Forcepoint components. See Upgrading Web Protection Solutions and Upgrading Email Protection Solutions for instructions.

Post-upgrade activities

Note

Product names are changed for v8.4.0.

TRITON AP-EMAIL is Forcepoint Email Security
TRITON AP-WEB is Forcepoint Web Security
TRITON AP-DATA is Forcepoint Data Security
TRITON Manager is Forcepoint Security Manager

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

Depending on the Forcepoint solutions installed on your appliances, after upgrade perform the following activities.

Important

(Forcepoint Web Security only)

Changing the policy mode is not supported on X Series appliances that have been upgraded to v8.4. This is consistent with past versions.

When the “set mode” command is used to change the policy mode, an error is returned. The last line of the error output is:

```
ERROR: [the time]:
ApplianceModeChanger::main(): Unable to
switch appliance modes.
```

The policy mode can be changed on v8.4 X Series appliances sourced from the factory or that have been re-imaged with version 8.4.

All appliances can use the **set mode** command to change the policy source *location* (the IP address of the policy source host machine).

In the CLI

- Elevate to **config** mode and perform system and configuration checks.
  - Display system information.

    ```
    show appliance info
    ```

    Results may be similar to:

    ```
    Uptime              : 0 days, 2 hours, 13 minutes
    Hostname            : webapp.example.com
    Hardware_platform   : X10G G2
    Appliance_version   : 8.4.0
    Mode                : Forcepoint Web Security
    Policy_mode         : Filtering only
    Policy_source_ip:   : 10.222.21.10
    ```

  - Display the upgrade history.

    ```
    show upgrade history
    ```

  - Display the appliance and module status.

    ```
    show appliance status
    ```

    ```
    show <module>
    ```

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

    ```
    restart <module>
    ```

  - Display network interface settings.

    ```
    show interface info
    ```

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

  - Check and, if necessary, 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 Forcepoint servers** in Forcepoint Appliances Getting Started.

  - Use the **set log archive** command to establish size and frequency values for archiving log files.
- If you integrate with a SIEM or an SNMP server, check your SNMP polling and alerting settings.

  ```
  show snmp config
  ```

  ```
  show trap config
  ```

  ```
  show trap events
  ```

Additional tasks

- If your appliance includes Forcepoint Email Security, perform email Post-upgrade activities.
- In Forcepoint Security Manager, go to the **Appliances** tab and register your appliances.
- If you have *User directory and filtering* appliances, in Forcepoint Security Manager go to the Web Security module **Settings > General > Policy Servers** page, and add the Policy Server instances.
- If your appliance includes Forcepoint Web Security, perform the Content Gateway Post-upgrade activities.
- Review the Release Notes for the Forcepoint 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

  Version 8.3.0

  - v8.3.0 Web Protection Release Notes
  - v8.3.0 TRITON AP-EMAIL Release Notes

  Version 8.2.0

  - v8.2.0 Web Protection Release Notes
  - v8.2.0 TRITON AP-EMAIL Release Notes

  Version 8.1.0

  - v8.1.0 Web Protection Release Notes
  - v8.1.0 TRITON AP-EMAIL Release Notes

  Version 8.0.1

  - v8.0.1 Web Protection Release Notes
  - v8.0.1 TRITON AP-EMAIL Release Notes