FORCEPOINT
POWERED BY Raytheon

X Series Appliance Upgrade Guide

Forcepoint Web Security, Forcepoint Email Security
Model: X10G

Upgrades from 7.8.2 & higher to 8.5.x

Published 2018

Last modified 30-Nov-2018

Contents

Upgrading X Series Appliances to version 8.5.3

Overview

Forcepoint X10G appliances can be upgraded directly to v8.5.3 from v8.1.x, v8.2.x, v8.3.x and v8.4.x.

Note

Beginning with version 8.3, the Forcepoint appliance platform moved to a new architecture. Before upgrading your Forcepoint appliances, it is very important that you read the v8.3.0 TRITON Appliances Release Notes.

Recommended upgrade paths:

From	To	Step One	Step Two	Step Three
v8.0.x,	v8.5.3	Install X10G C Port Hotfix. See the *Summary of upgrade procedure* section.	Upgrade to v8.3.0. Follow the instruction in Upgrading X-Series Appliances to v8.3.0.	Upgrade to v8.5.38.5.3. Follow the instructions in this guide.
v8.1.x, v8.2.x, v8.3.x, v8.4.x	v8.5.3	Upgrade to v8.5.3. Follow the instructions in Upgrading Forcepoint Appliances from v8.4 to v8.5.		

From	To	Step One	Step Two	Step Three
v7.8.2, v7.8.3, v7.8.4 (option 1)	v8.5.3	Upgrade to v8.3.0. Follow the instruction in Upgrading X-Series Appliances to v8.3.0.	Upgrade to v8.5.x. Follow the instructions in Upgrading Forcepoint Appliances from v8.4 to v8.5.	
v7.8.4 (option 2)	v8.5.3	Upgrade appliance module (APP) to v8.0.0 but leave all other software modules at v7.8.4. Follow the instructions in Upgrading X-Series Appliances to v8.0.x.	Upgrade appliance module (APP) to v8.1.0 or v8.2.0 but leave all other software modules at v7.8.4 Prepare a local filestore with the upgrade patch and use the CLI command `load patch --location` for express upgrade. Follow the instructions in Upgrading X-Series Appliances to version 8.2.0.	Use the upgrade patch to upgrade all on-blade modules to v8.4.0. Follow the instructions in this guide.

Starting with v8.3.0, a single ISO image (v8.x.x Unified Appliance Installer) is offered to restore an appliance back to the factory settings as well as to upgrade all installed modules in the target appliance to the corresponding version.

Modules include:

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

Forcepoint Web Security:

- **Web** — Forcepoint Web Security core components
- **Proxy** — Content Gateway web proxy

Forcepoint Email Security:

- **Email** — Forcepoint Email Security 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.

Summary of upgrade procedure

The upgrade procedure uses a filestore. By using a filestore, the *X10G C Port Hotfix* (required for deployments prior to 8.3) and the upgrade package can be uploaded to X10G blade servers from a location in the local network, rather than having to download the files repeatedly from the Forcepoint download server.

1. Identify or define a filestore to use to hold the hotfix and upgrade files.
2. Download the X10G C Port Hotfix and the v8.5.3 upgrade package from the Forcepoint Downloads page to the filestore.
3. Perform *Pre-upgrade activities*, page 5.

4. 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 TRITON 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.

5. Upload the X10G C Port Hotfix from the filestore and install it.
6. Upload the upgrade package and install it.
7. Perform *Post-upgrade activities*, page 9.
8. Upgrade the TRITON management server (if not upgraded when Policy Broker/ Policy Database were upgraded), and other servers that host TRITON components.

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

X10G C Port Hotfix

A dedicated X10G management communication network interface (C) has been added since 8.3. In v8.2 and earlier, management traffic was handled on interface P1. Adding the C interface places management traffic on a dedicated channel and makes X Series platforms consistent with other Forcepoint appliance platforms.

Download the version of the hotfix that matches the version of the software currently running in your deployment. The file names are similar to:

Websense-App-8.1.0-830.rpm

Websense-App-8.2.0-830.rpm

Download and installation instruction are included in *Upgrade procedure*, page 7.

Rollback

When the upgrade patch 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 v8.5.3 upgrade patch, perform the following tasks and be aware of the following issues.

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 v8.5.3 web protection solutions and v8.5.3 Web Protection Release Notes.
- For Forcepoint Email Security, see Upgrading email protection solutions and v8.5.3 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.

Upgrade procedure

Important

Appliance services are not available while the patch 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.

1. Identify or define a filestore for staging X10G C Port Hotfix and the upgrade patch, and as an off-appliance location for keeping backup files.
2. Download the v8.5.3 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.
3. Download X10G C Port Hotfix and the v8.5.3 upgrade package and place them in the filestore.
   a. Log on to My Account, go to the **Downloads** page.
   b. In the **Forcepoint Appliances > Forcepoint X10G Appliance** section, click the version number that your blades are currently running. To see all versions, you may need to click the **All Downloads** button at the top of the page.
   c. In the **Installer** section, select **8.5.3 Unified Appliance Installer** (8.3 and 8.4 customers) or **v8.5.3 Universal upgrade patch for V / X Series appliances**.

      The rpm name is **Websense-Appliance-Patch-853.rpm**.
   d. On the resulting **Product Installer** page, look at the **Release Date** and **Details** to confirm that you selected the v8.5.3 upgrade rmp, and then click **Download**. You may also want to save the MD5 to perform a checksum on the downloaded file.
   e. Next, go back a page to the **Forcepoint X10G Appliance Version 8.x.x** page, and in the **Hotfix** section select **v8.x.x X10G HF840**.
   f. On the resulting **Hotfix & Patch** page, look at the **Release Date** and **Description** to confirm that you selected the correct hotfix, and then click **Download**. You may also want to save the MD5 to perform a checksum on the downloaded file.
   g. Perform checksums. Or, if needed, move the files to the filestore and then perform checksums.

   You now have the files you need to upgrade all of your X10G blades.
4. Verify that the hotfix and upgrade files are accessible from the blades.

   Log on to the CLI of a blade to be upgraded, elevate to **config** mode and use:

   ```
   load patch --location <filestore_alias>
   load hotfix --location <filestore_alias>
   ```

In each list, confirm that the hotfix and upgrade files are present.

5. Perform *Pre-upgrade activities*, page 5.
6. If your deployment includes TRITON AP-WEB, 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 TRITON components on the Full policy source machine are upgraded when Policy Broker/Policy Database are upgraded.

   In all instances, you must upgrade TRITON AP-WEB 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.

7. If the appliance is registered in TRITON Manager, in TRITON 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 TRITON Manager, go to the **Settings > General > Policy Servers** page and unregister the appliance.
8. Upload and apply the v8.5.3 upgrade patch.

   a. Upload the upgrade patch.

      ```
      load patch --location <filestore_alias>
         --file <upgrade_patch_filename>
      ```

   b. Install the upgrade patch.

      ```
      install patch
      ```

      Select the v8.5.3 upgrade patch from the list.

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

The patch 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 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.

9. Perform *Post-upgrade activities*, page 9.
10. Return to Step 5 and upgrade remaining X10G blade servers.
11. Upgrade the TRITON 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

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 from v8.2 and earlier to v8.5.3.

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 v8.3, v8.4, v8.5, or v8.5.3
X Series appliances sourced from the factory or that have been re-imaged with version 8.3, 8.4, 8.5, or 8.5.3.

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   : 8.5.3
    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, 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 8.5.3

  - v8.5.3 Forcepoint Web Protection Release Notes
  - v8.5.3 Forcepoint Email Security Release Notes

  Version 8.5.0

  - v8.5.0 Forcepoint Web Protection Release Notes
  - v8.5.0 Forcepoint Email Security Release Notes

  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