FORCEPOINT
POWERED BY Raytheon

X-Series Appliance Upgrade Guide

TRITON AP-WEB, TRITON AP-EMAIL
Models: X10G

Upgrades from 8.0.0 & higher to 8.3.x

R030217830

Published 2017
Printed in the United States of America and Ireland

Trademarks

WinPcap

Contents

1 Upgrading X-Series Appliances to version 8.3.0

Version 8.3 of the TRITON appliance platform introduces a new architecture. Before upgrading your TRITON appliances, it is very important that you read the v8.3.0 TRITON Appliances Release Notes.

X10G appliances can be upgraded directly to 8.3.0 from 8.0.x, 8.1.x, 8.2.x.

Recommended upgrade paths:

From	To	Step One	Step Two
v8.0.x, v8.1.x, v8.2.x	v8.3.0	Follow the instructions in this guide.	
v7.8.2, v7.8.3, v7.8.4	v8.3.0	Upgrade to 8.0.0. See Upgrading X-Series Appliances to v8.0.x.	Follow the instructions in this guide.

Important

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

- Upgrade Instructions for TRITON AP-WEB
- Upgrading email protection solutions

The v8.3 upgrade package is a single rpm that upgrades all installed modules at the same time. 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 functional appliances running in a functional deployment. Required network interfaces must have reliable connections to TRITON 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, *Hotfix 830* (required) 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 hotfix 830 and the v8.3.0 upgrade package from the Forcepoint Downloads page to the filestore.
3. Perform *Pre-upgrade activities*, page 4.

4. If you are upgrading a deployment that includes TRITON AP-WEB, 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 TRITON AP-WEB. 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 hotfix 830 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 6.

Hotfix 830

Version 8.3 adds a dedicated TRITON management communication network interface (C). In v8.2 and earlier, TRITON 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 TRITON appliance platforms.

Prior to applying the v8.3 upgrade patch, administrators must apply hotfix 830, restart the appliance, and then configure the C interface in the CLI.

To configure interface C, be prepared with:

- Unique C interface IPv4 address (required)

  Choose an IP address that is unlikely to change in the future. Changing the C interface IP address significantly impacts the deployment and requires the assistance of Forcepoint Technical Support.
- Subnet mask (required)
- Default gateway IP address (required)
- VLAN ID, if needed

If interface C is on a new subnet and/or VLAN, also update the chassis switch configuration. See the Forcepoint knowledge base article Configuring the C interface VLAN in the X10G switches.

After the C interface is configured, the configuration data is stored until the upgrade patch is applied, at which time the interface is added.

You need to download the version of the hotfix that matches the version of the software currently running in your deployment. The file names are:

Websense-App-8.0.0-830.rpm

Websense-App-8.0.1-830.rpm

Websense-App-8.1.0-830.rpm

Websense-App-8.2.0-830.rpm

Download and installation instruction are included in *Upgrade procedure*, page 6.

Rollback

When the upgrade patch is applied, a copy of 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 v8.3.x 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 v8.3.x web protection solutions and v8.3.0 Web Protection Release Notes.
- For TRITON AP-EMAIL, see Upgrading email protection solutions and v8.3.0 TRITON AP-EMAIL 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.

SNMP settings

The upgrade to v8.3.0 does not preserve SNMP settings. If SNMP is enabled, you should document your existing settings and be prepared to reconfigure SNMP after upgrade.

Content Gateway Integrated Windows Authentication (IWA) settings

TRITON AP-WEB 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, continuing 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 hotfix 830 and the upgrade patch, and as an off-appliance location for keeping backup files.
2. Download the v8.3.x TRITON Unified Installer to a location in which it is easy to copy it to Windows servers hosting TRITON components, such as TRITON Manager and Log Server. See Upgrading Web Protection Solutions.
3. Download hotfix 830 and the v8.3.0 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 **v8.3.0 universal upgrade patch for V / X series appliances**.

      The rpm name is **Websense-Appliance-Patch-830.rpm**.
   d. On the resulting **Product Installer** page, look at the **Release Date** and **Details** to confirm that you selected the v8.3.0 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 HF830**.

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 4.

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. On the security blade to be upgraded, upload and install hotfix 830, and then, in the CLI, configure interface C.

   

   Important

   You must restart the appliance after the hotfix is installed and before you configure interface C.

   a. In the CLI, elevate to **config** mode and upload hotfix 830 from the filestore.

      ```
      load hotfix --location <filestore_alias>
         --file <App-8.X.X-830>
      ```

      For "8.x.x", substitute the version that is currently running on the appliance.

   b. Install the hotfix with:

      ```
      install hotfix
      ```

      Select hotfix 830 from the list.

      When installation is complete, restart the appliance.

   c. After restart, log on to the CLI, elevate to **config** mode, and configure interface C.

      ```
      set interface ipv4 --interface c --ip <ipv4_address>
         --mask <ipv4_netmask> --gateway <ipv4_address>
      ```

      If on a VLAN, set the VLAN ID.

      ```
      set interface vlan --interface c --vid <integer>
      ```

      If interface C is on a new subnet and/or VLAN, you may need to update the chassis switch configuration.

      The configuration information is stored for use by the upgrade patch.

9. Upload and apply the v8.3 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 v8.3.0 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 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 be hung, allow the process to run for at least 90 minutes. If installation has not completed in that time, contact Forcepoint Technical Support.

10. Perform *Post-upgrade activities*, page 9.
11. Return to Step 5 and upgrade remaining X10G blade servers.
12. Upgrade the TRITON management server (if not upgraded when Policy Broker/ Policy Database were upgraded), and other servers that host TRITON components. See Upgrading Web Protection Solutions and Upgrading Email Protection Solutions for instructions.

Post-upgrade activities

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

Important

(TRITON AP-WEB only)

Changing the policy mode is not supported on X-Series appliances that have been upgraded to v8.3. 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 v8.3 X-Series appliances sourced from the factory or that have been re-imaged with version 8.3.

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   : 8.3.0
    Mode                : TRITON AP-WEB
    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.

  - If the appliance hosts TRITON AP-WEB, add a component route.

    Add a component route to route Content Gateway (proxy) traffic to the web protection components through the appliance management interface (C).

    In **config** mode, enter:

    ```
    set component_route -dest <C_interface_IP_address>
        --mask 255.255.255.255 --module proxy
    ```

  - 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 TRITON servers** in TRITON Appliances Getting Started.

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

Additional tasks

- If your appliance includes TRITON AP-EMAIL, perform the TRITON AP-EMAIL Post-upgrade activities.
- In TRITON Manager, go to the **Appliances** tab and register your appliances.
- If you have *User directory and filtering* appliances, in TRITON Manager go to the Web module **Settings > General > Policy Servers** page, and add the Policy Server instances.
- If your appliance includes TRITON AP-WEB, perform the Content Gateway Post-upgrade activities.
- Review the Release Notes for the TRITON solutions on your appliances. New features may require configuration to be put into effect.

  Version 8.3.0

  - v8.3.0 Web Protection 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 Web Protection 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 Web Protection Release Notes
  - v8.1.0 TRITON AP-EMAIL Release Notes
  - v8.1.0 TRITON AP-DATA Release Notes

  Version 8.0.1

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