FORCEPOINT
POWERED BY Raytheon

V Series Appliance Upgrade Guide

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

Upgrades from 7.6.x through 8.5.x

Published 2018

Last modified 30-Nov-2018

Contents

Upgrading V Series Appliances

Chapter 1 **Upgrading V Series Appliances. 1**

Upgrading V Series appliances from v7.6.x to 7.7.x 4
- Versions supported for upgrade 4
- Estimates of time to complete upgrade 5
- Preparing for the appliance upgrade 6
- Upgrade instructions 10
- Upgrading multiple V-Series appliances. 11
- Post-upgrade activities 13

Upgrading V Series appliances from v7.7.x to 7.8.1 15
- Versions supported for upgrade 15
- Estimates of time to complete upgrade 16
- Preparing for the appliance upgrade 17
- Upgrade instructions 20
- Upgrading multiple V-Series appliances. 23
- Post-upgrade activities 25

Upgrading V Series appliances from v7.8.1 to 7.8.2 and from v7.8.1, v7.8.2 or 7.8.3 to 7.8.4. 27
- Estimates of time to complete upgrade 29
- Preparing for the appliance upgrade 30
- Upgrade instructions 32
- Upgrading multiple V-Series appliances. 34
- Post-upgrade activities 36

Upgrading V Series appliances from v7.8.x to 8.0.x 38
- Estimates of time to complete upgrade 40
- Preparing for the appliance upgrade 42
- Upgrade instructions 44
- Upgrading multiple V-Series appliances. 46
- Post-upgrade activities 47

Upgrading V Series appliances from v7.8.x or 8.0.x to 8.1.x 51
- Estimates of time to complete upgrade 54
- Preparing for the appliance upgrade 55
- Upgrade instructions 56
- Upgrading multiple V-Series appliances. 58

Post-upgrade activities 60
Upgrading V Series appliances from v7.8.x, 8.0.x, or 8.1.x to v8.2.x 62
Estimates of time to complete upgrade 64
Pre-upgrade activities 65
Upgrade instructions 66
Upgrading multiple V-Series appliances. 68
Post-upgrade activities 70
Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.3.x 72
Estimates of time to completion 74
Rollback 75
Summary of upgrade procedure 76
Pre-upgrade activities 76
Upgrade procedure 78
Upgrading multiple V-Series appliances. 81
Post-upgrade activities 82
Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.4.x 86
Product renaming 89
Estimates of time to completion 89
Rollback 90
Summary of upgrade procedure 90
Pre-upgrade activities 91
Upgrade procedure 93
Upgrading multiple V Series appliances. 95
Post-upgrade activities 97
Upgrading V Series appliances from 8.1.x, v8.2.x, 8.3.0, or 8.4.0 to 8.5.3 100
Estimates of time to completion 102
Rollback 103
Summary of upgrade procedure 103
Pre-upgrade activities 104
Upgrade procedure 106
Upgrading multiple V Series appliances. 108
Post-upgrade activities 110

Upgrading V Series Appliances

In this guide:

- *Upgrading V Series appliances from 8.1.x, v8.2.x, 8.3.0, or 8.4.0 to 8.5.3*, page 100
- *Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.4.x*, page 86
- *Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.3.x*, page 72
- *Upgrading V Series appliances from v7.8.x, 8.0.x, or 8.1.x to v8.2.x*, page 62
- *Upgrading V Series appliances from v7.8.x or 8.0.x to 8.1.x*, page 51
- *Upgrading V Series appliances from v7.8.x to 8.0.x*, page 38
- *Upgrading V Series appliances from v7.8.1 to 7.8.2 and from v7.8.1, v7.8.2 or 7.8.3 to 7.8.4*, page 27
- *Upgrading V Series appliances from v7.7.x to 7.8.1*, page 15
- *Upgrading V Series appliances from v7.6.x to 7.7.x*, page 4

Use the information in this guide to perform the following upgrades to your V Series™ appliances:

Current Version	End Version (direct upgrade supported)
8.1.0, 8.2.0, 8.3.0, 8.4.0	8.5.3
7.8.4, 8.0.0, 8.0.1, 8.1.0, 8.2.0, 8.3.0	8.4.0
7.8.4, 8.0.0, 8.0.1, 8.1.0, 8.2.0	8.3.0
7.8.4, 8.0.0, 8.0.1, 8.1.0	8.2.0
7.8.1, 7.8.2, 7.8.3, 7.8.4, 8.0.0, 8.0.1	8.1.0
7.8.1, 7.8.2, 7.8.3, 7.8.4	8.0.0, 8.0.1
7.8.1, 7.8.2, 7.8.3	7.8.4
7.8.1	7.8.2
7.7.3	7.8.1
7.7.0	7.8.1

Current Version	End Version (direct upgrade supported)
7.7.0	7.7.3
7.6.0, 7.6.1, 7.6.2, 7.6.5, 7.6.7	7.7.0

Note

If your current appliance version is 8.3.0 or later, use the V Series, X Series, and Virtual Appliance Upgrade Guide.

Getting started

Your appliances must be in one of these modes:

- Web only mode
  - Forcepoint URL Filtering
  - Forcepoint Web Security
- Email only mode
  - Forcepoint Email Security
- Web and Email mode
  - Forcepoint Web Security and Forcepoint Email Security

- Forcepoint URL Filtering and Forcepoint Email Security

Important

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

Note

v8.5.0 was the last supported software release for the V5K G2R2 appliance and the V10K G3R1 appliance. These appliances are no longer supported in the software.

Hardware support will continue to be available throughout End-of-Life for these appliance models. Please refer to related Tech Alert and official product life-cycle matrix for details.

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.

Upgrading V Series appliances from v7.6.x to 7.7.x

Important
The upgrade process is designed for functional appliances 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.

V Series Appliance Upgrade Guide | Upgrades to v7.7.x

Related topics:

- *Versions supported for upgrade*, page 4
- *Estimates of time to complete upgrade*, page 5
- *Preparing for the appliance upgrade*, page 6
- *Upgrade instructions*, page 10
- *Upgrading multiple V-Series appliances*, page 11
- *Post-upgrade activities*, page 13

This upgrade process applies to version 7.6.x for the following solutions and platforms:

- Web Security, Web Security Gateway, and Web Security Gateway Anywhere
- Email Security Gateway and Email Security Gateway Anywhere
- V10000 G1*, V10000 G2, and V5000 G2, V10000 G3

*The latest version available for the V10000 G1 appliance is 7.7.3. No later versions are planned for the V10000 G1 appliance.

Versions supported for upgrade

V Series Appliance Upgrade Guide | Upgrades to v7.7.x

You must upgrade to version 7.7.0 before upgrading to 7.7.3. At version 7.7.0 or 7.7.3, you can upgrade to 7.8.1 (See *Upgrading V Series appliances from v7.7.x to 7.8.1*, page 15).

Direct upgrade to version 7.7.0 is supported from these versions:

- 7.6.0
- 7.6.1
- 7.6.2
- 7.6.5
- 7.6.7

Appliances running versions earlier than v7.6.0 must be upgraded to 7.6.0. Once upgraded to 7.6.0, they can be upgraded directly to 7.7.0.

To upgrade from version 7.6.0 to 7.7.0, follow the same steps shown in this guide for upgrading to version 7.7.x, except use a 7.6.x patch wherever a 7.7.x patch is mentioned.

At sites wishing to stay on the 7.7 series, we recommend upgrading to the latest version of 7.7.x, which is 7.7.3, so that you have the latest fixes and features.

Note

The upgrades to version 7.7.3 are applied to V Series appliances via a software patch. Patches are installed via the Appliance Manager under the **Administration > Patches/Hotfixes > Patches** page. You must be running version 7.7.0 to use the version 7.7.3 patch.

Estimates of time to complete upgrade

V Series Appliance Upgrade Guide | Upgrades to v7.7.x

The table below provides estimates of the time needed for the 7.7.x patch to be installed on an appliance. The amount of time varies, as indicated. Not all V Series configurations are shown.

System	Configuration	Elapsed time
V10000 G2 V10000 G3	Web Security Gateway and Email Security Gateway User directory and filtering	70 - 90 minutes
V10000 G2	Web security only: Web Security Gateway Full policy source	70 - 90 minutes
V10000 G2 V10000 G3	Web Security and Email Security Gateway Full policy source	70-90 minutes
V10000 G2 V5000 G2	Web security only: Web Security Gateway User directory and filtering	90 - 110 minutes
V10000 G2	Dual mode: Web Security Gateway and Email Security Gateway	70 - 90 minutes
V10000 G2 V5000 G2	Email security only	20 - 30 minutes
V5000 G2	Web Security Gateway filtering only	30 minutes

The following provides a basic sample scenario:

Approximate total upgrade time, beginning to end, for all upgrade tasks:

- 1 Dual mode V10000 G2 appliance
- 2 Windows R2 2008 servers: 1 for the TRITON console, 1 for Web and Email Log Server

Approximately 3 to 4 hours

The download speed for each patch that you're going to apply depends on your network environment and can vary significantly.

Activity breakout:

- 1 hour to download the version 7.7.x appliance upgrade (patch) file (if the download speed is 512 kilobytes per second). This is the estimated time per patch. Depending on the upgrade path you take, your upgrade may involve more than one patch.
- 10 minutes to back up the V Series appliance
- 70 to 90 minutes for the patch to perform the upgrade
- 10 minutes to restart the V Series and verify that the upgrade was successful
- 20 minutes to download the version 7.7.x TRITON Unified Installer
- 40 to 60 minutes to run the installer to upgrade the TRITON management server and the Log Server host
- 5 minutes to restart the Windows servers and verify that the upgrade was successful

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied and until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 5.

Note

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

Preparing for the appliance upgrade

V Series Appliance Upgrade Guide | Upgrades to v7.7.x

Before applying the 7.7.x patch, perform these tasks and be aware of the following issues.

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

- For Web Security solutions, see Before upgrading Web Security to v7.7.

- For Email Security Gateway (Anywhere), see Preparing for the upgrade.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to **Administration > Backup Utility**.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, save the backup file in another location off the appliance.

Content Gateway logs

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

To ensure that all Content Gateway logs are retained, you can download the Content Gateway logging directory.

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.

Policy databases and databases are not affected by the upgrade.

Content Gateway Integrated Windows Authentication (IWA) settings

IWA settings are not preserved in the upgrade.

If your deployment uses Content Gateway IWA user authentication, log onto Content Gateway and record the IWA settings, including the name of the domain to which IWA is joined. Keep this record where you can easily retrieve it after upgrade is complete.

Network Agent settings

In the majority of deployments, upgrade preserves all Network Agent settings.

However, when the following conditions are both true, the upgrade process does not preserve several Network Agent settings:

- There is a Filtering only appliance that is configured to get policy information from the Policy Broker machine (either the Full policy source appliance or an off-appliance software installation).
- There is an off-appliance Network Agent installation that uses the Filtering Service on the Filtering only appliance, and uses the Policy Server on the Policy Broker machine.

When the above conditions are both true and the upgrade is performed, the settings for the off-appliance Network Agent installation are not retained.

In this case, record your Network Agent settings (configured in TRITON - Web Security) before performing the upgrade. Go to the Local Settings page for each Network Agent instance (**Settings > Network Agent** > *agent_IP_address*) and record **all** of its settings.

The following local settings are not preserved.

- Filtering Service IP address
- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring
- Ignore Port
- Debug Setting

NIC Configuration settings (from the **Settings > Network Agent > NIC Configuration** page for each NIC) are also not preserved:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

Save your record where you can easily access it when the upgrade is complete.

Administrator accounts

Make sure administrator accounts authenticated by a directory service have an email address specified in the directory service. In version 7.7, an email address is required for each administrator account (except group accounts).

Content Gateway changes

See the Content Gateway Release Notes for information about enhancements and changes in version 7.7.0.

If you are upgrading to version 7.7.3, see the Content Gateway Release Notes for information about enhancements and changes in version 7.7.3.

SSL Manager

SSL Manager has been enhanced in several ways. See the release notes for more information.

Of particular note, a few Certificate validation options have changed. Users of Certificate validation should review the changes and adjust their settings.

IPv6

Incremental support is added in version 7.7.0. See the release notes for more information.

Upgrade instructions

V Series Appliance Upgrade Guide | Upgrades to v7.7.x

Important

V Series appliance services are not available while the patch is being applied and until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 5.

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

1. If you have multiple V Series appliances, read *Upgrading multiple V-Series appliances*, page 11, **before** following this procedure.
2. Take all precautions to ensure that power to the V Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.
3. Back up appliance configuration and settings. See *Back up appliance configuration and settings*, page 8.
4. Restart the appliance (in Appliance Manager: **Status** > **General** > **Restart Appliance**).
5. If Policy Broker and Policy Database are installed on an off-appliance server, make sure they're upgraded to version 7.7.x and are running. You should simultaneously upgrade all TRITON services that are installed on the off-box server with Policy Broker and Policy Database.
6. To download the upgrade patch, in the Appliance Manager, go to the **Administration > Patches/Hotfixes > Patches** tab. The 7.7.x upgrade patch should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The 7.7.x patch should be listed as available.

   Alternatively, the patch can be downloaded from www.forcepoint.com and uploaded to the appliance.

   a. Go to My Account (formerly MyWebsense) and select the **Downloads** tab. Click **Get Hotfixes & Patches**. Select your appliance model and version.

   b. Download the upgrade patch.

   c. Log on to the Appliance Manager, and navigate to **Administration > Patches /Hotfixes**.

   d. Click **Browse**, and select the v7.7.x upgrade file.

   e. Click **Upload**. After a few seconds, the upgrade is listed in the **Available patches** list.

   This is an efficient method when your deployment has many appliances because the download from Forcepoint occurs only once. Other appliances can upload the patch from the local location.

7. Click **Install** to apply the upgrade.

   Important

   When patch installation begins, a dialog box indicates that the patch will take 5 to 10 minutes to apply. This is incorrect. The time is significantly longer. See *Estimates of time to complete upgrade*, page 5.

   While the upgrade is being applied, services are **unavailable** to users.

8. When patch installation is complete, the appliance restarts automatically.
9. When the appliance has restarted, log on to the Appliance Manager and verify on the **Configuration > System** page that the V Series version is 7.7.x.

   On the **Configuration > System** page, you can also confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.

   In rare cases, when logging onto the Appliance Manager for the first time after upgrade, your browser may show an **HTTP Status - Internal Error** page. If this occurs, cycle the power to the appliance. Once the appliance has restarted, you should be able to log in.

10. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and then the next one, and so forth. See *Upgrading multiple V-Series appliances*, page 11.
11. Upgrade all TRITON components that run off the appliance. These may include Web and Email Security Log Server, transparent identification agents, and the TRITON manager. If Policy Broker and Policy Database are on the same off-box server as the TRITON manager, you should have already upgraded all components on that box earlier.

    See Upgrading Websense Web Security Solutions and Upgrading Email Security Gateway to v7.7 for instructions.

If the upgrade fails, contact Technical Support.

Upgrading multiple V-Series appliances

V Series Appliance Upgrade Guide | Upgrades to v7.7.x

When multiple V Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is an Email mode (only) appliance

Apply the 7.7.x upgrade patch before upgrading the off-appliance components.

If the appliance includes Web Security mode

It is a best practice to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

Best practice for upgrade sequence if Full policy source is on V-Series appliance

Follow this sequence whether the Full policy source is a Web mode (only) or Web and Email mode appliance.

Upgrade the **Full policy source** V Series appliance. Each time the upgrade completes, the appliance automatically restarts.

1. Sequentially apply the upgrade to all **User directory and filtering** appliances.
2. Sequentially apply the upgrade to all **Filtering only** appliances.
3. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on V-Series appliance

If you have multiple V Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure Policy Broker and Policy Server are upgraded to version 7.7.x and are running. You should simultaneously upgrade all TRITON services that are installed on the off-appliance server with Policy Broker and Policy Server. Use the version 7.7.x TRITON Unified Installer to upgrade the Policy Broker system. See Upgrading Websense Web Security Solutions for instructions.
2. Sequentially apply the upgrade to all **User directory and filtering** appliances. Each time the upgrade completes on an appliance, the appliance automatically restarts.
3. Sequentially apply the upgrade to all **Filtering only** appliances.
4. Use the version 7.7.x TRITON installer to upgrade remaining off-appliance components. See Upgrading Websense Web Security Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source* appliance is unavailable, is being replaced, or is being re-imaged, then set a *User directory and filtering* or *Filtering only* appliance (temporarily) to be the Full policy source. To do this:

1. Back up the Full backup file of the User directory and filtering or Filtering only appliance in case changing the policy source fails.

2. On that secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **Full policy source**. Save the setting.
4. Upgrade this appliance to version 7.7.x. The appliance automatically restarts when the upgrade finishes.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance. When the upgrade is done, the appliance automatically restarts.
2. On the previously upgraded secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **User directory and filtering** or **Filtering only** and enter the IP address of the primary appliance. Save the setting.
4. Use the version 7.7.x TRITON installer to upgrade remaining off-appliance components. See Upgrading Websense Web Security Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.6.x to 7.7.x*, page 4.

Post-upgrade activities

V Series Appliance Upgrade Guide | Upgrades to v7.7.x

- If your appliance includes Email Security Gateway (Anywhere), perform the Email Security Gateway Post-upgrade activities.
- If your appliance hosts a Web Security Policy Server (is a user directory and filtering appliance), log onto the TRITON console, go to the Web Security manager **Settings > General > Policy Servers** page, and add the Policy Server instance. Next, go to the TRITON console **Appliances** tab and register the appliance.
- If your appliance includes Web Security Gateway (Anywhere), perform the Content Gateway Post-upgrade activities.
- If your appliance uses the Network Agent module, *Verify Network Agent settings*, page 14.
- Review the Release Notes for the TRITON solutions on your appliances (links provided below). There are several new features that may require some configuration to put into effect.

  Web Security users will be especially interested in the Threats dashboard (no configuration needed). Web Security Gateway (Anywhere) users will be interested in the enhanced outbound scanning options. It is recommended that all of the Scanning Options be reviewed.

  - Web Security Release Notes
  - Content Gateway Release Notes
  - Email Security Gateway Release Notes

If you are upgrading to version 7.7.3, see the Content Gateway Release Notes for information about enhancements and changes in version 7.7.3.

Verify Network Agent settings

If you had to record your Network Agent settings prior to upgrade (*Network Agent settings*, page 8), restore them after the TRITON console has been upgraded.

Log on to TRITON - Web Security and go to **Settings > Network Agent > Local Settings**.

Select the IP address of the affected Network Agent installations and check and restore all values, paying particular attention to:

- Filtering Service IP address
- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring
- Ignore Port
- Debug Setting

Also, check the **Settings > Network Agent > NIC Configuration** page for each NIC:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

When your changes are complete, click **OK** and then **Save and Deploy**.

Upgrading V Series appliances from v7.7.x to 7.8.1

V Series Appliance Upgrade Guide | Upgrades to v7.8.1

Related topics:

- *Versions supported for upgrade*, page 15
- *Estimates of time to complete upgrade*, page 16
- *Preparing for the appliance upgrade*, page 17
- *Upgrade instructions*, page 20
- *Upgrading multiple V-Series appliances*, page 23
- *Post-upgrade activities*, page 25

This upgrade process applies to version 7.7.x for the following TRITON components and platforms:

- Web Security, Web Security Gateway, and Web Security Gateway Anywhere
- Email Security Gateway and Email Security Gateway Anywhere
- V10000 G2 and G3 and V5000 G2 appliances

Note

For an overview of this upgrade process, see the support video, Upgrading a Websense V-Series appliance to v7.8.1.

For high-level flow diagrams for upgrading from v7.7.x, see:

Web Security Gateway and Email Security Gateway on V-Series: Upgrade to 7.8.1

Web Security and Web Security Gateway on V-Series Upgrade to 7.8.1

Email Security Gateway on V-Series: Upgrade to 7.8.1

Versions supported for upgrade

V Series Appliance Upgrade Guide | Upgrades to v7.8.1

You can upgrade directly to version 7.8.1 from these versions of 7.7.x:

- 7.7.0, 7.7.3

Appliances running earlier versions must be upgraded to version 7.7.0 first before upgrading to version 7.8.1.

Estimates of time to complete upgrade

V Series Appliance Upgrade Guide | Upgrades to v7.8.1

The table below provides estimates of the time needed for the 7.8.1 patch to be installed on an appliance. The amount of time varies, as indicated. Not all V Series configurations are shown.

System	Configuration	Elapsed time
V10000 G2/G3	Web security only: Web Security Gateway Full policy source	40-50 minutes
V10000 G2/G3 V5000 G2	Web security only: Web Security Gateway User directory and filtering	40-50 minutes
V10000 G2/G3	Dual mode: Web Security Gateway and Email Security Gateway	40-50 minutes
V10000 G2/G3 V5000 G2	Email security only	40-50 minutes

The following provides a basic sample scenario:

Approximate total upgrade time, beginning to end, for all upgrade tasks:

- 1 Dual mode V10000 G2 appliance
- 2 Windows R2 2008 servers: 1 for the TRITON console, 1 for Web and Email Log Server

Approximately 5.5 to 6 hours

The download speed for the patch depends on your network environment and can vary significantly.

Activity breakout:

- 90 seconds to download the pre-upgrade hotfix
- 10 minutes to apply the hotfix and restart the appliance. After the hotfix is applied, you must manually restart it.
- 3.5 hours to download the version 7.8.1 appliance upgrade (patch) file (if the download speed is 512 kilobytes per second)(the patch size is 6 gigabytes)
- 10 minutes to back up the V Series appliance
- 50 minutes for the patch to perform the upgrade, which includes automatically restarting the appliance twice
- 5 minutes to log onto the Appliance manager to verify that the upgrade was successful
- 20 minutes to download the version 7.8.1 TRITON Unified Installer

- 40 to 60 minutes to run the installer to upgrade on the TRITON management server and the Log Server host
- 5 minutes to restart the Windows servers and verify that the upgrade was successful

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied and until the appliance finishes automatically restarting twice. See *Estimates of time to complete upgrade*, page 16.

Preparing for the appliance upgrade

V Series Appliance Upgrade Guide | Upgrades to v7.8.1

Before applying the 7.8.1 patch, perform the following tasks and be aware of the following issues.

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

- For Web Security solutions, see Before upgrading Web Security to v7.8.
- For Email Security Gateway (Anywhere), see Preparing for the upgrade.

Back up appliance configuration and settings

Note that at the start of the upgrade process, you are given the chance to run the backup and save the backup file to a remote machine. But if you wish to perform a **full appliance configuration** backup in advance:

1. Log on to Appliance Manager and go to the **Administration > Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, save the backup file in another location off the appliance.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.7.x to 7.8.1*, page 15.

Content Gateway logs

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

To ensure that all Content Gateway logs are retained, you can download the Content Gateway logging directory.

1. In the Appliance Manager, go to **Administration >Logs**.

2. Select the **Websense Content Gateway** module and then **Download entire log file**.
3. Click **Submit** and specify a location to save the file.

Policy databases and TRITON databases are not affected by the upgrade.

Content Gateway Integrated Windows Authentication (IWA) settings

The upgrade process backs up and restores the IWA configuration, preserving the pre-existing domain memberships (joins).

Network Agent settings

Important

If your appliance has a Network Agent module that is temporarily disabled, enable or permanently disable it. If you do nothing, the module is permanently disabled.

In the majority of deployments, upgrade preserves all Network Agent settings.

However, when the following conditions are both true, the upgrade process does not preserve several Network Agent settings:

- There is a Filtering only appliance that is configured to get policy information from the Policy Broker machine (either the Full policy source appliance or an off-appliance software installation).
- There is an off-appliance Network Agent installation that uses the Filtering Service on the Filtering only appliance, and uses the Policy Server on the Policy Broker machine.

When the above conditions are both true and the upgrade is performed, the settings for the off-appliance Network Agent installation are not retained.

In this case, record your Network Agent settings (configured in the Web Security manager) before performing the upgrade. Go to the Local Settings page for each Network Agent instance (**Settings > Network Agent** > *agent_IP_address*) and record **all** of its settings.

The following local settings are not preserved.

- Filtering Service IP address
- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring
- Ignore Port
- Debug Setting

NIC Configuration settings (from the **Settings > Network Agent > NIC Configuration** page for each NIC) are also not preserved:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

Save your record where you can easily access it when the upgrade is complete

Administrator accounts

Make sure the administrator accounts authenticated by a directory service have an email address specified in the directory service. In version 7.8.1, an email address is required for each administrator account (except group accounts).

Content Gateway changes

See the Content Gateway Release Notes for information about enhancements and changes in version 7.8.1.

Disable on-appliance TRITON console

In version 7.8.1, the Web Security manager cannot reside on an appliance. If your deployment uses an on-appliance TRITON console, disable it and create a Windows-based TRITON management server before upgrading.

To disable the on-appliance TRITON console:

1. Log on to the Appliance Manager (https://<*C interface IP address*>:9447/appmng)
2. Under **Configuration**, select **Web Security Components**.
3. Under **TRITON - Web Security**, select **Disabled**.
4. Click **Save**.

   The disabling process may take several minutes. Wait for it to complete.
5. When the process completes successfully, a **TRITON Configuration** link appears below the **Disabled** option. Use this link to create a backup of TRITON settings that can be restored to the off-appliance TRITON Unified Security Center:
   a. Click the backup file link that is displayed below the Disabled button.
   b. If a certificate error is displayed, click the continue or accept option to start the download.
   c. Save the TRITON backup file (**EIP_bak.tgz**) in a convenient location.
   d. Create a TRITON management server on Windows Server 2008 R2 or Windows Server 2012.

If Full policy source is not on V Series appliance

If Policy Broker and Policy Server are installed on an off-appliance server, make sure they're upgraded to version 7.8.1 and are running. You should simultaneously upgrade all TRITON services that are installed on the off-appliance server with Policy Broker and Policy Server.

Integration mode

If you are using Web Security (no Gateway) appliances, make sure your integration mode is one of these supported modes:

- Stand-alone (Network Agent only)
- Microsoft TMG
- Citrix
- Cisco ASA

Upgrade instructions

V Series Appliance Upgrade Guide | Upgrades to v7.8.1

> **Important**
>
> V Series appliance services are not available while the patch is being applied and until the appliance finishes automatically restarting twice. See *Estimates of time to complete upgrade*, page 16.
>
> It is best to perform the upgrade at a time when service demand is low.

1. If you have multiple V Series appliances, read *Upgrading multiple V-Series appliances*, page 23, **before** following this procedure.
2. Take all precautions to ensure that power to the V Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.
3. Back up appliance configuration and settings. See *Back up appliance configuration and settings*, page 17. You can also do a backup at the start of the upgrade process.
4. If Policy Broker and Policy Database are installed on an off-appliance server, make sure they're upgraded to version 7.8.1 and are running. You should simultaneously upgrade all TRITON services that are installed on the off-box server with Policy Broker and Policy Database.
5. The upgrade involves two steps: installing a hotfix that goes with your appliance version, and then installing a patch. The patch consists of an **rpm** file and an **img** file. The hotfix enables you to download and upload these very large patch files.

> **Important**
>
> You **must install the appropriate Hotfix 90** for your version before you upload or download the upgrade patch files to the appliance, or the upgrade will not succeed.

Note that some sites who are storing years of snapshots and backups on their V Series appliances have noticed that the upgrade to v7.8.1 (where the underlying operating system becomes 64-bit) does not have enough space, due to the excess of backup files. If you have a large number of old backups or snapshots that might prevent a successful upgrade, please consider Hotfix 91 for 7.7.0 (or 7.7.3, whichever version you are running). Hotfix 91 enables you to eliminate old files and expands a partition used during the 7.8.1 upgrade. See Knowledge Base article 7158 for additional details.

6. To get the hotfix, in the Appliance manager, go to **Administration** > **Patches/ Hotfixes** > **Hotfixes** tab. Enter the name of the hotfix to download and install it on the appliance.
   - For example, APP-7.7.0-090 if you're upgrading from version 7.7.0 and APP-7.7.3-090 if you're upgrading from version 7.7.3.
     a. Click **Find** to locate the hotfix.
     b. Click **Download**. When the download is done, the hotfix appears in the table of downloaded hotfixes with the status **Ready to install**.

        If you have several appliances and do not want to download the hotfix from www.forcepoint.com multiple times, you can use the **Save to network location** link to copy the downloaded hotfix to a convenient location on your network, and then, on each appliance, use the **Upload Hotfix Manually** button to upload the file to the appliance.

        Note that if you copy the downloaded hotfix from one appliance to a local server, for use with other appliances, you must do this **before** installing the hotfix.
     c. Click **Install** to apply the hotfix. The installation may temporarily interrupt some services.
     d. Click **OK** to continue. It may take more than 5 minutes to install the hotfix.
7. After the hotfix is installed, manually restart the appliance in the Appliance manager by going to **Status** > **General**. Under Appliance Controller, click **Restart Appliance**. Restarting the appliance takes from 5 to 8 minutes. The appliance has successfully restarted when you're returned to the Appliance manager logon page.

Note

There are two ways to get the patch itself. Steps 8, 9, and 10 describe one method. At the end of step 10 is an alternative method.

8. To download the upgrade patch, in the Appliance manager, go to the **Administration > Patches/Hotfixes > Patches** tab. The 7.8.1 upgrade patch should be listed in the table of **Available patches**.
9. If the patch is not listed in the table, click **Check for Patches**.

You may see security warnings as the system tries to run a TRITON application related to uploading the patch. Click **Continue**. Mark the **I accept the risk...** check box, and then click **Run**.

10. Next, click **Download**. The patch size is 6 gigabytes, so this will take some time.

    When the download is done, the patch status becomes **Ready to Install**.

    Once the patch is downloaded, it can be saved to a local network location. You can upload the patch to other appliances from the local location by clicking the **Upload Patch Manually** button. If you copy the patch from one appliance to a local server, for use with other appliances, select **both** the rpm file and the img file **at the same time** in the Upload Patch utility. If you try to upload one file, then the other, a warning message is displayed, and the upload cannot be completed successfully.

    As an **alternative** to steps 8, 9, and 10, the patch can be downloaded from www.forcepoint.com and uploaded to the appliance.

    a. Go to My Account (formerly MyWebsense) and select the **Downloads** tab. Click **Get Hotfixes & Patches**. Select your appliance model and version.

    b. Download the upgrade patch, which consists of a tarball containing two files: an rpm and an img file.

    c. Unpack the patch tarball into the two files.

    d. Log on to the Appliance Manager, and navigate to **Administration > Patches /Hotfixes** > **Patches** tab.

    e. Via the **Upload Patch Manually** button, browse for and select the patch to open. Click **Upload**. Both files in the patch must be uploaded simultaneously. After a few seconds, the patch is listed in the **Available patches** list.

    This is an efficient method when your deployment has many appliances because the download occurs only once. Other appliances can upload the patch from the local location.

11. Click **Install**.

12. A **system check** is launched to make sure you're set up correctly for the upgrade to succeed. This may take several minutes.

    a. If all pre-requisites are met, you can back up your appliance files to a remote machine by clicking **Back Up**. It is a best practice to back up your files at this point if you have not already done so.

    b. If you choose to back up your appliance, provide the connection information for the remote machine. You can click **Test Connection** to test the connection.

    c. To perform the backup, click **Run Backup Now**.

    d. When you see the backup has succeeded, click **Install Patch**.

13. Review the subscription agreement that you have with Websense. Check **I accept this agreement** and **Continue**.

14. A confirmation message tells you that during the upgrade, you are logged out of the Appliance manager and the appliance restarts twice. Click **OK** to begin the upgrade.

    While the upgrade is performed, services are **unavailable** to users.

15. After the appliance has automatically restarted twice, log on to the Appliance manager, and go to **Administration** > **Patches/Hotfixes** > **Patches** tab. Under **Patch History**, for version 7.8.1, it should say "Upgrade Succeeded" in the **Comments** section. In the Appliance manager, you can also check the appliance version number by going to the **Configuration > System** page and looking under **System Information**.

    On the **Configuration** > **System** page, you can also confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.

16. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and subsequent appliances. See *Upgrading multiple V-Series appliances*, page 23.

17. Upgrade all components that you haven't already upgraded and which run off the appliance. These may include Web and Email Security Log Server, transparent identification agents, and the TRITON manager. If Policy Broker and Policy Server are on the same off-appliance server as the TRITON manager, you should have already upgraded all components on that box earlier.

    See Upgrading Websense Web Security Solutions and Upgrading Email Security Gateway to v7.8 for instructions.

If the upgrade fails, contact Technical Support.

Occasionally, you may need to upgrade or recover your appliance using a USB image. Complete instructions for downloading and creating the USB image can be found in this Knowledge Base article.

Upgrading multiple V-Series appliances

V Series Appliance Upgrade Guide | Upgrades to v7.8.1

1. For multiple V Series appliances, just like for a single appliance, you need to download the pre-upgrade hotfix from the Appliance manager, install it, and restart each appliance.
2. Then, you must download and install the v7.8.1 upgrade patch. (See *Upgrade instructions*, page 20.)

    Once the patch is downloaded, it can be saved to a local network location. You can upload the patch to other appliances from the local location by clicking the **Upload Patch Manually** button.

    When multiple V Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is an Email mode (only) appliance

Apply the 7.8.1 hotfix and upgrade patch before upgrading the off-appliance components.

If the appliance includes Web Security mode

It is a best practice to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

Best practice for upgrade sequence if Full policy source is on V-Series appliance

Follow this sequence whether the Full policy source is a Web mode (only) or Web and Email mode appliance.

Upgrade the **Full policy source** V Series appliance. The appliance automatically restarts each time the upgrade is completed.

1. Sequentially apply the upgrade to all **User directory and filtering** appliances.
2. Sequentially apply the upgrade to all **Filtering only** appliances.
3. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on V-Series appliance

If you have multiple V Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure Policy Broker and Policy Server are upgraded to version 7.8.1 and are running. You should simultaneously upgrade all TRITON services that are installed on the off-appliance server with Policy Broker and Policy Server. Use the version 7.8.1 TRITON installer to upgrade the Policy Broker system. See Upgrading Websense Web Security Solutions for instructions.
2. Sequentially apply the upgrade to all **User directory and filtering** appliances. When the upgrade completes, the appliance automatically restarts.
3. Sequentially apply the upgrade to all **Filtering only** appliances.
4. Use the version 7.8.1 TRITON installer to upgrade remaining off-appliance components. See Upgrading Websense Web Security Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source* appliance is unavailable, is being replaced, or is being re-imaged, then set a *User directory and filtering* or *Filtering only* appliance (temporarily) to be the Full policy source. To do this:

1. On that secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
2. For **Policy Source**, select **Full policy source**. Save the setting.

3. Upgrade this appliance to version 7.8.1. The appliance automatically restarts when the upgrade is done.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance.The appliance automatically restarts when the upgrade is done.
2. On the previously upgraded secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **User directory and filtering** or **Filtering only** and enter the IP address of the primary appliance. Save the setting.
4. Use the version 7.8.1 TRITON installer to upgrade remaining off-appliance components. See Upgrading Websense Web Security Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.7.x to 7.8.1*, page 15.

Post-upgrade activities

V Series Appliance Upgrade Guide | Upgrades to 7.8.1

- If your appliance includes Email Security Gateway (Anywhere), perform the Email Security Gateway Post-upgrade activities.
- If your appliance hosts a Web Security Policy Server (is a user directory and filtering appliance), log onto the TRITON console, go to the Web Security manager **Settings > General > Policy Servers** page, and add the Policy Server instance. Next, go to the TRITON console **Appliances** tab and register the appliance.
- If your appliance includes Web Security Gateway (Anywhere), perform the Content Gateway Post-upgrade activities.
- If your appliance uses the Network Agent module, *Verify Network Agent settings*, page 26.
- Review the Release Notes for the solutions on your TRITON appliances (links provided below). There are several new features that may require some configuration to put into effect.

  Web Security users will be especially interested in the deployment visualization and management tools offered by the **Status** > **Deployment** page. Web Security Gateway Anywhere users will be interested in the option to enable ThreatScope™ sandboxing of suspicious files.

  Email Security users will be interested in the ThreatScope cloud-based message analysis function, which inspects email attachment file types for security threats.

  - Web Security Release Notes
  - Gateway Release Notes
  - Email Security Gateway Release Notes

Verify Network Agent settings

If you had to record your Network Agent settings prior to upgrade (*Network Agent settings*, page 18), restore them after the TRITON console has been upgraded.

1. Log on to the Web Security manager.
2. On the Settings tab, under Network Agent, place the mouse over **General**, then select the IP address of the Network Agent instance you want to configure.
3. Check and restore all values, paying particular attention to:
   - Filtering Service IP address
   - If Filtering Service is unavailable
   - Proxies and Caches
   - Port Monitoring
   - Ignore Port
   - Debug Setting
4. Check the **Settings > Network Agent > NIC Configuration** page for each NIC, especially the selections for:
   - Use this NIC to monitor traffic
   - Monitor List
   - Monitor List Exceptions
5. When your changes are complete, click **OK**.
6. Repeat steps 2 through 5 for additional Network Agent instances.
7. When you are finished updating your settings, click **Save and Deploy**.

Upgrading V Series appliances from v7.8.1 to 7.8.2 and from v7.8.1, v7.8.2 or 7.8.3 to 7.8.4

Related topics:

- *Estimates of time to complete upgrade*, page 29
- *Preparing for the appliance upgrade*, page 30
- *Upgrade instructions*, page 32
- *Upgrading multiple V-Series appliances*, page 34
- *Post-upgrade activities*, page 36

This upgrade process applies to version 7.8.1, 7.8.2, and 7.8.3 for the following TRITON components and platforms:

- Web Security, Web Security Gateway, and Web Security Gateway Anywhere
- Email Security Gateway and Email Security Gateway Anywhere
- V10000 G2 and G3 and V5000 G2 appliances

Important

V10000 G4 and **V5000 G3** appliances running 7.8.1, 7.8.2, or 7.8.3 cannot be upgraded to a higher version of 7.8.x using an upgrade patch (a patch can be used to upgrade to any version of 8.x). Attempting to upgrade using the 7.8.x upgrade patch that's offered will result in a pre-check verification failure.

With these models, to move to a higher version of 7.8.x, perform a full back of the appliance, re-image the appliance with the desired version of 7.8.x, and restore the backup. See **Restoring to Factory Image** in the V-Series Getting Started guide, and the knowledge base article V-Series USB image for restoring to factory settings.

Here are the various upgrade paths to version 7.8.2, 7.8.3, or 7.8.4. The table also includes the path for upgrading from version 7.7.x to 7.8.1. You must upgrade to version 7.8.1 before you can upgrade to 7.8.2 or later:

To upgrade from	To this version	Step One	Step Two	Step Three
7.7.x	7.8.1	Apply HF 90	Upgrade to 7.8.1	
7.7.x	7.8.2	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.2

To upgrade from	To this version	Step One	Step Two	Step Three
7.7.x	7.8.3	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.3
7.7.x	7.8.4	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.4
7.8.1	7.8.4	Upgrade to 7.8.4		
7.8.2	7.8.4	Upgrade to 7.8.4		
7.8.3	7.8.4	Upgrade to 7.8.4		

For an overview of the upgrade process, see the following flow diagrams:

- Web Security Gateway and Email Security Gateway on V-Series: Upgrade to 7.8.x
- Web Security and Web Security Gateway on V-Series Upgrade to 7.8.x
- Email Security Gateway on V-Series: Upgrade to 7.8.x

The upgrade from v7.8.1 to 7.8.2 is:

- Applied to V Series appliances via a software patch.

  Patches are installed via the Appliance console under the **Administration > Patches/Hotfixes > Patches** page.
- Similar to upgrading from 7.6.x to v7.7.x with the exception that you must use a 7.8.2 patch in place of the 7.7.x patch and a system check is performed during the upgrade.

The upgrade from v7.8.1, 7.8.2, or 7.8.3 to 7.8.4 is:

- Applied to V Series appliances via a software patch.

  Patches are installed via the Appliance console under the **Administration > Patches/Hotfixes > Patches** page.
- Similar to upgrading from 7.6.x to v7.7.x with the exception that you must use a 7.8.3 patch in place of the 7.7.x patch and a system check is performed during the upgrade.

Important

After upgrading a filtering only appliance with an off-appliance policy source, Web Security manager lists two Filtering Service instances with the same IP address in **Settings > Network Agent > Global**.

To avoid this problem, before upgrading a filtering only appliance from v7.8.1 to 7.8.2 or from v7.8.x to 7.8.4:

1. Switch filtering only mode to full policy source mode.
2. Run the upgrade process.
3. Switch back to filtering only mode.

Estimates of time to complete upgrade

V Series Appliance Upgrade Guide | Upgrades to v7.8.x

The table below provides estimates of the time needed for the 7.8.2, 7.8.3, or 7.8.4 patch to be installed on an appliance. The amount of time varies, as indicated. Not all V Series configurations are shown.

System	Configuration	Elapsed time
V10000 G2 V10000 G3	Web Security Gateway and Email Security Gateway User directory and filtering	90 - 110 minutes
V10000 G2	Web security only: Web Security Gateway Full policy source	70 - 90 minutes
V10000 G2 V10000 G3	Web Security and Email Security Gateway Full policy source	70-90 minutes
V10000 G2 V5000 G2	Web security only: Web Security Gateway User directory and filtering	90 - 110 minutes
V10000 G2	Dual mode: Web Security Gateway and Email Security Gateway	70 - 90 minutes
V10000 G2 V5000 G2	Email security only	20 - 30 minutes
V5000 G2	Web Security Gateway filtering only	30 minutes

The following provides a basic sample scenario:

Approximate total upgrade time, beginning to end, for all upgrade tasks:

- 1 Dual mode V10000 G2 appliance
- 2 Windows R2 2008 servers: 1 for the TRITON console, 1 for Web and Email Log Server

Approximately 3 to 4 hours

The download speed for each patch that you're going to apply depends on your network environment and can vary significantly.

Activity breakout:

- 1 hour to download the version 7.8.x appliance upgrade (patch) file (if the download speed is 512 kilobytes per second). This is the estimated time per patch. Depending on the upgrade path you take, your upgrade may involve more than one patch.

- 10 minutes to back up the V Series appliance
- 70 to 90 minutes for the patch to perform the upgrade
- 10 minutes to restart the V Series and verify that the upgrade was successful
- 20 minutes to download the version 7.8.x TRITON Unified Installer
- 40 to 60 minutes to run the installer to upgrade the TRITON management server and the Log Server host
- 5 minutes to restart the Windows servers and verify that the upgrade was successful

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied and until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 29.

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

Preparing for the appliance upgrade

V Series Appliance Upgrade Guide | Upgrades to v7.8.2 and 7.8.3

Before applying the 7.8.2, 7.8.3, or 7.8.4 patch, perform these tasks and be aware of the following issues.

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

- For Web Security solutions, see Before upgrading Web Security to v7.8.x.
- For Email Security Gateway (Anywhere), see Preparing for the upgrade.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to the **Administration > Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, save the backup file in another location off the appliance.

Content Gateway logs

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

To ensure that all Content Gateway logs are retained, you can download the Content Gateway logging directory.

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

Policy databases and TRITON databases are not affected by the upgrade.

Content Gateway Integrated Windows Authentication (IWA) settings

IWA settings are not preserved in the upgrade.

If your deployment uses Content Gateway IWA user authentication, log onto Content Gateway and record the IWA settings, including the name of the domain to which IWA is joined. Keep this record where you can easily retrieve it after upgrade is complete.

Network Agent settings

In the majority of deployments, upgrade preserves all Network Agent settings.

However, when the following conditions are both true, the upgrade process does not preserve several Network Agent settings:

- There is a Filtering only appliance that is configured to get policy information from the Policy Broker machine (either the Full policy source appliance or an off-appliance software installation).
- There is an off-appliance Network Agent installation that uses the Filtering Service on the Filtering only appliance, and uses the Policy Server on the Policy Broker machine.

When the above conditions are both true and the upgrade is performed, the settings for the off-appliance Network Agent installation are not retained.

In this case, record your Network Agent settings (configured in TRITON - Web Security) before performing the upgrade. Go to the Local Settings page for each Network Agent instance (**Settings > Network Agent** > *agent_IP_address*) and record **all** of its settings.

The following local settings are not preserved.

- Filtering Service IP address
- If Filtering Service is unavailable
- Proxies and Caches

- Port Monitoring
- Ignore Port
- Debug Setting

NIC Configuration settings (from the **Settings > Network Agent > NIC Configuration** page for each NIC) are also not preserved:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

Save your record where you can easily access it when the upgrade is complete.

Administrator accounts

Make sure the administrator accounts authenticated by a directory service have an email address specified in the directory service. In version 7.8.x, an email address is required for each administrator account (except group accounts).

Content Gateway changes

See the Content Gateway Release Notes for information about enhancements and changes in version 7.8.2.

See the Content Gateway Release Notes for information about enhancements and changes in version 7.8.3.

See the Content Gateway Release Notes for information about enhancements and changes in version 7.8.4.

Upgrade instructions

V Series Appliance Upgrade Guide | Upgrades to v7.8.x

Important

V Series appliance services are not available while the patch is being applied and until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 29.

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

1. If you have multiple V Series appliances, read *Upgrading multiple V-Series appliances*, page 34, **before** following this procedure.
2. Take all precautions to ensure that power to the V Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.

3. Back up appliance configuration and settings. See *Back up appliance configuration and settings*, page 30.
4. Restart the appliance (in Appliance Manager: **Status** > **General** > **Restart Appliance**).
5. If Policy Broker and Policy Database are installed on an off-appliance server, make sure they're upgraded to the version you want (either 7.8.2. 7.8.3, or 7.8.4) and are running. You should simultaneously upgrade all TRITON services that are installed on the off-box server with Policy Broker and Policy Database.
6. To download the upgrade patch, in the Appliance Manager, go to the **Administration > Patches/Hotfixes > Patches** tab. The upgrade patch for the version you want (7.8.2, 7.8.3, or 7.8.4) should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The patch should be listed as available.

   Alternatively, the patch can be downloaded from www.forcepoint.com and uploaded to the appliance.

   a. Go to My Account (formerly MyWebsense) and select the **Downloads** tab. Click **Get Hotfixes & Patches**. Select your appliance model and version.
   b. Download the upgrade patch.
   c. Log on to the Appliance Manager, and navigate to **Administration > Patches /Hotfixes**.
   d. Click **Upload Patch Manually**, then **Browse**, and then select the upgrade file for the version you want (7.8.2, 7.8.3, or 7.8.4).
   e. Click **Upload**. After a few seconds, the upgrade is listed in the **Available patches** list.

   This is an efficient method when your deployment has many appliances because the download occurs only once. Other appliances can upload the patch from the local location.
7. Click **Install** to apply the upgrade. Note that in v7.8.x, patch installation takes significantly longer than warned. See *Estimates of time to complete upgrade*, page 29.
8. A **system check** is launched to make sure you're set up correctly for the upgrade to succeed. This may take several minutes.
9. When you see that all patch pre-requisites have been met, you can continue to install the patch by clicking **Install Patch**.
10. Review the subscription agreement that you have with Websense. Check **I accept this agreement** and **Continue**.
11. A confirmation message tells you that during the upgrade, you are logged out of the Appliance manager and the appliance restarts. Click **OK** to begin the upgrade.

    While the upgrade is performed, services are **unavailable** to users.
12. After the appliance has automatically restarted, log on to the Appliance manager, and go to **Administration** > **Patches/Hotfixes** > **Patches** tab. Under **Patch History**, for version 7.8.2, 7.8.3, or 7.8.4, it should say "Patch has been installed

successfully" in the **Comments** section. In the Appliance manager, you can also check the appliance version number by going to the **Configuration > System** page and looking under **System Information**.

On the **Configuration** > **System** page, you can also confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.

13. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and subsequent appliances. See *Upgrading multiple V-Series appliances*, page 34.
14. Upgrade all TRITON components that you haven't already upgraded and which run off the appliance. These may include Web and Email Security Log Server, transparent identification agents, and the TRITON manager. If Policy Broker and Policy Server are on the same off-appliance server as the TRITON manager, you should have already upgraded all components on that box earlier.

    See Upgrading Websense Web Security Solutions and Upgrading Email Security Gateway to v7.8.x for instructions.

If the upgrade fails, contact Technical Support.

Upgrading multiple V-Series appliances

V Series Appliance Upgrade Guide | Upgrades to v7.8.x

When multiple V Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is an Email mode (only) appliance

Apply the upgrade patch for the version you want before upgrading the off-appliance components.

If the appliance includes Web Security mode

It is a best practice to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

Best practice for upgrade sequence if Full policy source is on V-Series appliance

Follow this sequence whether the Full policy source is a Web mode (only) or Web and Email mode appliance.

Upgrade the **Full policy source** V Series appliance. Each time the upgrade completes, the appliance automatically restarts.

1. Sequentially apply the upgrade to all **User directory and filtering** appliances.
2. Sequentially apply the upgrade to all **Filtering only** appliances.

3. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on V-Series appliance

If you have multiple V Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure Policy Broker and Policy Server are upgraded to the version you want and are running. You should simultaneously upgrade all TRITON services that are installed on the off-appliance server with Policy Broker and Policy Server. Use the version 7.8.x TRITON Unified Installer to upgrade the Policy Broker system. See Upgrading Websense Web Security Solutions for instructions.
2. Sequentially apply the upgrade to all **User directory and filtering** appliances. Each time the upgrade completes on an appliance, the appliance automatically restarts.
3. Sequentially apply the upgrade to all **Filtering only** appliances.
4. Use the version 7.8.x TRITON installer to upgrade remaining off-appliance components. See Upgrading Websense Web Security Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source* appliance is unavailable, is being replaced, or is being re-imaged, then set a *User directory and filtering* or *Filtering only* appliance (temporarily) to be the Full policy source. To do this:

1. Back up the Full backup file of the User directory and filtering or Filtering only appliance in case changing the policy source fails.
2. On that secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **Full policy source**. Save the setting.
4. Upgrade this appliance to the version you want. The appliance automatically restarts when the upgrade finishes.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance. When the upgrade is done, the appliance automatically restarts.
2. On the previously upgraded secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **User directory and filtering** or **Filtering only** and enter the IP address of the primary appliance. Save the setting.

4. Use the version 7.8.x installer to upgrade remaining off-appliance components. See Upgrading Websense Web Security Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.8.1 to 7.8.2 and from v7.8.1, v7.8.2 or 7.8.3 to 7.8.4*, page 27.

Post-upgrade activities

V Series Appliance Upgrade Guide | Upgrades to v7.8.x

- If your appliance includes Email Security Gateway (Anywhere), perform the Email Security Gateway Post-upgrade activities.
- If your appliance hosts a Web Security Policy Server (is a user directory and filtering appliance), log onto the TRITON console, go to the Web Security manager **Settings > General > Policy Servers** page, and add the Policy Server instance. Next, go to the TRITON console **Appliances** tab and register the appliance.
- If your appliance includes Web Security Gateway (Anywhere), perform the Content Gateway Post-upgrade activities.
- If your appliance uses the Network Agent module, *Verify Network Agent settings*, page 37.
- Review the Release Notes for the TRITON solutions on your appliances (links provided below). There are several new features that may require some configuration to put into effect.

  For the 7.8.2 release, Web Security users may be especially interested in improvements made to Policy Broker replication, Filtering Service, User Service, Directory Agent, Log Server, LogonApp, the Installer, and the Web Security manager. For Web Security Gateway Anywhere users, emphasis was placed on stability and performance.

  Email Security Gateway users may be interested in the on-premises secure message delivery feature, providing a secure portal in which an organization's customers may view, send, and manage email that contains sensitive information. Email Security Gateway Anywhere users will be interested in the phishing detection and education feature, part of the ThreatScope add-on functionality.

  - Web Security Release Notes
  - Content Gateway Release Notes
  - Email Security Gateway Release Notes

  For the 7.8.3 release, Web Security Gateway Anywhere users can configure a delay for the download of data files used for Content Gateway analysis; use IP spoofing with explicit proxy; and configure rule-based authentication to use a new Captive Portal authentication method. Web Security now offers support for Mac OS X 10.9.2 and Windows 8.1 Update 1 for the logon application, and for Firefox 28 and Chrome 33 and 34.

  Email Security Gateway users may be interested in how an email DLP policy action plan in Data Security may now include a filter action created in the Email Security manager. The on-premises secure messaging portal end-user registration process has also been enhanced.

- Web Security Release Notes
- Content Gateway Release Notes
- Email Security Gateway Release Notes

For the 7.8.4 release, please review the release notes below.

- Web Security Release Notes
- Content Gateway Release Notes
- Email Security Gateway Release Notes

Verify Network Agent settings

If you had to record your Network Agent settings prior to upgrade (*Network Agent settings*, page 31), restore them after the TRITON console has been upgraded.

Log on to TRITON - Web Security and go to **Settings > Network Agent > Local Settings**.

Select the IP address of the affected Network Agent installations and check and restore all values, paying particular attention to:

- Filtering Service IP address
- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring
- Ignore Port
- Debug Setting

Also, check the **Settings > Network Agent > NIC Configuration** page for each NIC:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

When your changes are complete, click **OK** and then **Save and Deploy**.

Upgrading V Series appliances from v7.8.x to 8.0.x

V Series Appliance Upgrade Guide | Upgrades to v8.0.x

Related topics:

- *Estimates of time to complete upgrade*, page 29
- *Preparing for the appliance upgrade*, page 30
- *Upgrade instructions*, page 32
- *Upgrading multiple V-Series appliances*, page 34
- *Post-upgrade activities*, page 36

Important

Not all models of V Series appliances support version 8.0.x.

Older V10000 G2 and V5000 G2 appliances, known as revision 1 (or R1) appliances are not supported with version 8.0.0 and higher. Forcepoint stopped shipping these models:

- V10000 G2 R1 Third quarter, 2011
- V5000 G2 R1 First quarter, 2012

If you plan to upgrade to version 8.0.x, you should verify the full model number of the appliances you plan to upgrade. See the knowledge base article titled V-Series appliances supported with version 8.0.

Also see the v8.0.0 V-Series Release Notes.

Important

Product names and bundles have changed in 8.0.0. See the v8.0.0 V-Series Release Notes.

This upgrade process applies to versions 7.8.x for the following TRITON solutions and platforms:

- Web Security, Web Security Gateway, and Web Security Gateway Anywhere
- Email Security Gateway and Email Security Gateway Anywhere
- V10000 and V5000 appliances; see V-Series appliances supported with version 8.0 for a list of supported models

The table lists the various upgrade paths to version 8.0.x. The table also includes the path for upgrading from version 7.7.x to 7.8.1. You must upgrade to version 7.8.1 (or later) before upgrading to version 8.0.x:

To upgrade from	To this version	Step One	Step Two	Step Three
7.7.x	7.8.1	Apply HF 90	Upgrade to 7.8.1	
7.7.x	7.8.2	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.2
7.7.x	7.8.3	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.3
7.7.x	7.8.4	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.4
7.8.1, 7.8.2, 7.8.3, 7.8.4	8.0.x	Upgrade to 8.0.x		

For an overview of the upgrade process, see the following video and flow diagrams:

- Upgrading Websense V-Series appliances to v8.0.x
- Web Security Gateway and Email Security Gateway on V-Series: Upgrade to 8.0.x
- Web Security and Web Security Gateway on V-Series Upgrade to 8.0.x
- Email Security Gateway on V-Series: Upgrade to 8.0.x

The upgrade from v7.8.1, 7.8.2, 7.8.3, or 7.8.4 to 8.0.x is:

- Applied to V Series appliances via a software patch.

  Patches are installed via the Appliance console under the **Administration > Patches/Hotfixes > Patches** page.

Important

If you have multiple appliances, and:

- They are running version 7.8.3 or 7.8.4
- You plan to download the upgrade patch and then upload it to a local host for download to the other appliances

You may run into a Java version error. For a complete description and work around, please see the knowledge base article V-Series patch upload Java version error.

Important

After upgrading a filtering only appliance with an off-appliance policy source, the Web module of TRITON Manager (formerly the Web Security manager) lists two Filtering Service instances with the same IP address in **Settings > Network Agent > Global**.

To avoid this problem, before upgrading a filtering only appliance from v7.8.x to 8.0.x:

1. Switch filtering only mode to full policy source mode.
2. Run the upgrade process.
3. Switch back to filtering only mode.

Estimates of time to complete upgrade

V Series Appliance Upgrade Guide | Upgrades to v8.0.x

The table below provides estimates of the time needed for the 8.0.0 patch to be installed on an appliance. The amount of time varies, as indicated. Not all V Series configurations are shown.

System	Configuration	Elapsed time
V10000	Dual mode: Web Security Gateway (now TRITON AP-WEB) Full policy source and Email Security Gateway (now TRITON AP-EMAIL)	50 - 70 minutes
V10000	Dual mode: Web Security Gateway (now TRITON AP-WEB) User directory and filtering and Email Security Gateway (now TRITON AP-EMAIL)	70 - 90 minutes
V10000	Dual mode: Web Security (now Web Filter & Security) and Email Security Gateway (now TRITON AP-EMAIL)	45-65 minutes

System	Configuration	Elapsed time
V10000	Web security only: Web Security Gateway (now TRITON AP-WEB) Full policy source	40 - 60 minutes
V10000 V5000	Web security only: Web Security Gateway (now TRITON AP-WEB) User directory and filtering	60 - 80 minutes
V10000 V5000	Email Security Gateway (now TRITON AP-EMAIL) only	20 - 30 minutes
V5000	Web Security Gateway (now TRITON AP-WEB) Filtering only	30 minutes

The following provides a basic sample scenario:

Approximate total upgrade time, beginning to end, for all upgrade tasks:

- 1 Dual mode V10000 appliance
- 2 Windows R2 2008 servers: 1 for the TRITON Manager, 1 for Web and Email Log Server

Approximate upgrade time: 3 to 4 hours

The download speed for each patch that you're going to apply depends on your network environment and can vary significantly.

Activity breakout:

- 1 hour to download the version 8.0.x appliance upgrade (patch) file (if the download speed is 512 kilobytes per second). This is the estimated time per patch. Depending on the upgrade path you take, your upgrade may involve more than one patch.
- 10 minutes to back up the V Series appliance
- 70 to 90 minutes for the patch to perform the upgrade
- 10 minutes to restart the V Series and verify that the upgrade was successful
- 20 minutes to download the version 8.0.x TRITON Unified Installer
- 40 to 60 minutes to run the installer to upgrade the TRITON management server and the Log Server host
- 5 minutes to restart the Windows servers and verify that the upgrade was successful

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied and until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 29.

Note

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

Preparing for the appliance upgrade

V Series Appliance Upgrade Guide | Upgrades to v8.0.x

Before applying the 8.0.x patch, perform these tasks and be aware of the following issues.

If you are 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 Web Security to v8.0.x.
- For email protection solutions, see Preparing for the upgrade.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to the **Administration > Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, save the backup file in another location off the appliance.

Content Gateway logs

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

To ensure that all Content Gateway logs are retained, you can download the Content Gateway logging directory.

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

Policy databases and TRITON databases are not affected by the upgrade.

Content Gateway Integrated Windows Authentication (IWA) settings

IWA domain joins should be preserved through the upgrade process. However, in the event that the IWA domain joins are dropped during the upgrade, make a record of the settings in advance. Log on to Content Gateway and record the IWA settings, including the names of domains to which IWA is joined. Keep this record where you can easily retrieve it after the upgrade.

Network Agent settings

In the majority of deployments, upgrade preserves all Network Agent settings.

However, when the following conditions are both true, the upgrade process does not preserve several Network Agent settings:

- There is a Filtering only appliance that is configured to get policy information from the Policy Broker machine (either the Full policy source appliance or an off-appliance software installation).
- There is an off-appliance Network Agent installation that uses the Filtering Service on the Filtering only appliance, and uses the Policy Server on the Policy Broker machine.

When the above conditions are both true and the upgrade is performed, the settings for the off-appliance Network Agent installation are not retained.

In this case, record your Network Agent settings (configured in TRITON - Web Security) before performing the upgrade. Go to the Local Settings page for each Network Agent instance (**Settings > Network Agent** > *agent_IP_address*) and record **all** of its settings.

The following local settings are not preserved.

- Filtering Service IP address
- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring
- Ignore Port
- Debug Setting

NIC Configuration settings (from the **Settings > Network Agent > NIC Configuration** page for each NIC) are also not preserved:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

Save your record where you can easily access it when the upgrade is complete.

Administrator accounts

Make sure that administrator accounts authenticated by a directory service have an email address specified in the directory service. In versions 7.8.1 and later, an email address is required for each administrator account (except group accounts).

Content Gateway changes

See the Websense Web Protection Release Notes for information about enhancements and changes in version 8.0.0.

Upgrade instructions

V Series Appliance Upgrade Guide | Upgrades to v8.0.x

Important

V Series appliance services are not available while the patch is being applied and until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 40.

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

1. If you have multiple V Series appliances, read *Upgrading multiple V-Series appliances*, page 46, **before** following this procedure.
2. Take all precautions to ensure that power to the V Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.
3. Back up appliance configuration and settings. See *Back up appliance configuration and settings*, page 42.
4. Restart the appliance (in Appliance Manager: **Status** > **General** > **Restart Appliance**).
5. If Policy Broker and Policy Database are installed on an off-appliance server, make sure they're upgraded to version 8.0.x and are running. You should simultaneously upgrade all TRITON services that are installed on the off-box server with Policy Broker and Policy Database.
6. To download the upgrade patch, in the Appliance Manager go to the **Administration > Patches/Hotfixes > Patches** tab. The upgrade patch for version 8.0.x should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The patch should be listed as available.

   Alternatively, the patch can be downloaded from www.forcepoint.com and uploaded to the appliance.

   a. Go to My Account (formerly MyWebsense) and select the **Downloads** tab. Click **Get Hotfixes & Patches**. Select your appliance model.

   b. Download the upgrade patch.

c. Log on to the Appliance Manager and navigate to **Administration > Patches /Hotfixes**.

d. Click **Browse** and select the upgrade file for version 8.0.x.

e. Click **Upload**. After a few seconds the upgrade is listed in the **Available patches** list.

This is an efficient method when your deployment has many appliances because the download from Forcepoint occurs only once. Other appliances can upload the patch from the local location.

7. Click **Install** to apply the upgrade. Note that patch installation may take significantly longer than warned. See *Estimates of time to complete upgrade*, page 40.
8. A **system check** is launched to make sure you're set up correctly for the upgrade to succeed. This may take several minutes.
9. When you see that all patch pre-requisites have been met, you can continue to install the patch by clicking **Install Patch**.
10. Review the subscription agreement that you have with Websense. Check **I accept this agreement** and **Continue**.
11. A confirmation message tells you that during the upgrade you are logged out of the Appliance manager and the appliance restarts. Click **OK** to begin the upgrade.

    While the upgrade is performed, services are **unavailable** to users.
12. After the appliance has automatically restarted, log on to the Appliance manager and go to **Administration** > **Patches/Hotfixes** > **Patches** tab. Under **Patch History**, for version 8.0.0, it should say "Patch has been installed successfully" in the **Comments** section. In the Appliance manager, you can also check the appliance version number by going to the **Configuration > System** page and looking under **System Information**.

    On the **Configuration** > **System** page, you can also confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.
13. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and subsequent appliances. See *Upgrading multiple V-Series appliances*, page 46.
14. Upgrade all TRITON components that you haven't already upgraded and which run off the appliance. These may include Web and Email Log Server, transparent identification agents, and the TRITON Manager. If Policy Broker and Policy Server are on the same off-appliance server as the TRITON Manager, you should have already upgraded all components on that box.

    See Upgrading Websense Web Protection Solutions and Upgrading Email Protection Solutions for instructions.

If the upgrade fails, contact Technical Support.

Upgrading multiple V-Series appliances

V Series Appliance Upgrade Guide | Upgrades to v8.0.x

When multiple V Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is an Email mode (only) appliance

Apply the upgrade patch for the version you want before upgrading the off-appliance components.

If the appliance includes Web Security mode

It is a best practice to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

Best practice for upgrade sequence if Full policy source is on V-Series appliance

Follow this sequence whether the Full policy source is a Web mode (only) or Web and Email mode appliance.

Upgrade the **Full policy source** V Series appliance. Each time the upgrade completes, the appliance automatically restarts.

1. Sequentially apply the upgrade to all **User directory and filtering** appliances.
2. Sequentially apply the upgrade to all **Filtering only** appliances.
3. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on V-Series appliance

If you have multiple V Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure Policy Broker and Policy Server are upgraded to the version you want and are running. You should simultaneously upgrade all TRITON services that are installed on the off-appliance server with Policy Broker and Policy Server. Use the version 8.0.x TRITON Unified Installer to upgrade the Policy Broker system. See Upgrading Websense Web Protection Solutions for instructions.
2. Sequentially apply the upgrade to all **User directory and filtering** appliances. Each time the upgrade completes on an appliance, the appliance automatically restarts.
3. Sequentially apply the upgrade to all **Filtering only** appliances.
4. Use the version 8.0.x TRITON installer to upgrade remaining off-appliance components. See Upgrading Websense Web Protection Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source* appliance is unavailable, is being replaced, or is being re-imaged, then set a *User directory and filtering* or *Filtering only* appliance (temporarily) to be the Full policy source. To do this:

1. Back up the Full backup file of the User directory and filtering or Filtering only appliance in case changing the policy source fails.
2. On that secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **Full policy source**. Save the setting.
4. Upgrade this appliance to the version you want. The appliance automatically restarts when the upgrade finishes.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance. When the upgrade is done, the appliance automatically restarts.
2. On the previously upgraded secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **User directory and filtering** or **Filtering only** and enter the IP address of the primary appliance. Save the setting.
4. Use the version 8.0.x TRITON installer to upgrade remaining off-appliance components. See Upgrading Websense Web Protection Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.8.x to 8.0.x*, page 38.

Post-upgrade activities

V Series Appliance Upgrade Guide | Upgrades to v8.0.x

Version 8.0.0 is the first product release to use a new, simplified product naming and grouping of the familiar Websense TRITON product line.

Original Name	New Name
Websense Web Filter	Websense Web Filter & Security
Websense Web Security	Websense Web Filter & Security

Original Name	New Name
Websense TRITON Web Security Gateway	Websense TRITON AP-WEB
Websense TRITON Web Security Gateway Anywhere	Websense TRITON AP-WEB with: ● Web Hybrid Module ● Web DLP Module ● Web Sandbox Module
Websense TRITON Data Security	Websense TRITON AP-DATA
Websense TRITON Email Security Gateway	Websense TRITON AP-EMAIL with ● Email DLP Module ● Email Encryption Module ● Email Sandbox Module
Websense TRITON Email Security Gateway Anywhere	Websense TRITON AP-EMAIL with ● Email DLP Module ● Email Sandbox Module ● Email Hybrid Module ● Image Analysis Module

The TRITON Unified Security Center is now known as TRITON Manager.

For more information about how these changes may affect you, or to change the add-on modules activated by your subscription, contact your sales partner or Forcepoint Sales representative.

Depending on the solutions installed on your appliances, after upgrade perform the following:

- If your appliance includes TRITON AP-EMAIL, perform the TRITON AP-EMAIL Post-upgrade activities.
- If your appliance hosts a Web Protection Policy Server (is a *User directory and filtering* appliance), log onto the TRITON Manager, go to the Web module **Settings > General > Policy Servers** page, and add the Policy Server instance. Next, go to the TRITON Manager **Appliances** tab and register the appliance.
- If your appliance includes TRITON AP-WEB, perform the Content Gateway Post-upgrade activities.
- If your appliance uses the Network Agent module, *Verify Network Agent settings*, page 49.
- Review the Release Notes for the TRITON solutions on your appliances (links provided below). There are several new features that may require some configuration to put into effect.

  For the 7.8.2 release, web protection users may be especially interested in improvements made to Policy Broker replication, Filtering Service, User Service, Directory Agent, Log Server, LogonApp, the Installer, and the Web component manager. For Web Security Gateway Anywhere (TRITON AP-WEB) users, emphasis was placed on stability and performance.

Email Security Gateway (TRITON AP-EMAIL) users may be interested in the on-premises secure message delivery feature, providing a secure portal in which an organization's customers may view, send, and manage email that contains sensitive information. Email Security Gateway Anywhere users will be interested in the phishing detection and education feature, part of the TRITON File Sandbox (formerly ThreatScope) add-on functionality.

- v7.8.2 Web Security Release Notes
- v7.8.2 Content Gateway Release Notes
- v7.8.2 Email Security Gateway Release Notes

For the 7.8.3 release, Web Security Gateway Anywhere users can configure a delay for the download of data files used for Content Gateway analysis; use IP spoofing with explicit proxy; and configure rule-based authentication to use a new Captive Portal authentication method. Web Security now offers support for Mac OS X 10.9.2 and Windows 8.1 Update 1 for the logon application, and for Firefox 28 and Chrome 33 and 34.

Email Security Gateway users may be interested in how an email DLP policy action plan in Data Security may now include a filter action created in the Email Security manager. The on-premises secure messaging portal end-user registration process has also been enhanced.

- v7.8.3 Web Security Release Notes
- v7.8.3 Content Gateway Release Notes
- v7.8.3 Email Security Gateway Release Notes

For the 7.8.4 release, please review the release notes below.

- v7.8.4 Web Security Release Notes
- v7.8.4 Content Gateway Release Notes
- v7.8.4 Email Security Gateway Release Notes

For the 8.0.0 release, please review the release notes below.

- v8.0.0 Web Protection Release Notes
- v8.0.0 TRITON AP-EMAIL Release Notes

For the 8.0.1 release, please review the release notes below.

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

Verify Network Agent settings

If you had to record your Network Agent settings prior to upgrade (*Network Agent settings*, page 31), restore them after the TRITON console has been upgraded.

Log on to TRITON Manager. In the Web module, go to **Settings > Network Agent > Local Settings**.

Select the IP address of the affected Network Agent installations and check and restore all values, paying particular attention to:

- Filtering Service IP address

- If Filtering Service is unavailable
- Proxies and Caches
- Port Monitoring
- Ignore Port
- Debug Setting

Also, check the **Settings > Network Agent > NIC Configuration** page for each NIC:

- Use this NIC to monitor traffic
- Monitor List
- Monitor List Exceptions

When your changes are complete, click **OK** and then **Save and Deploy**.

Upgrading V Series appliances from v7.8.x or 8.0.x to 8.1.x

Related topics:

- *Estimates of time to complete upgrade*, page 54
- *Preparing for the appliance upgrade*, page 55
- *Upgrade instructions*, page 56
- *Upgrading multiple V-Series appliances*, page 58
- *Post-upgrade activities*, page 60

Important

Not all V Series models support versions 8.x.

Older V10000 G2 and V5000 G2 appliances, known as revision 1 (or R1) appliances are not supported with version 8.0.0 and higher. Websense stopped shipping these models:

- V10000 G2 R1 Third quarter, 2011
- V5000 G2 R1 First quarter, 2012

If you plan to upgrade to version 8.x, you should verify the full model number of the appliances you plan to upgrade. See the knowledge base article titled V-Series appliances supported with version 8.0.

Important

Product names and bundles changed in version 8.0.0. The changes are summarized in the *Post-upgrade activities*, page 60.

This upgrade process applies to the following TRITON solutions and platforms:

- V10000 and V5000 appliances; see V-Series appliances supported with v8.x for a list of supported models
- TRITON AP-WEB and Web Filter & Security
- Web Security, Web Security Gateway, and Web Security Gateway Anywhere
- TRITON AP-EMAIL, Email Security Gateway, and Email Security Gateway Anywhere

The table lists the upgrade paths to version 8.1.x. The table also includes the path for upgrading from version 7.7.x to 7.8.1. You must upgrade to version 7.8.1 (or later) before upgrading to version 8.1.x:

To upgrade from	To this version	Step One	Step Two	Step Three
7.7.x	7.8.1	Apply HF 90	Upgrade to 7.8.1	
7.7.x	7.8.2	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.2
7.7.x	7.8.3	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.3
7.7.x	7.8.4	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.4
7.8.x *See **Important**, below.	8.1.x	Upgrade to 8.1.x		
8.0.x	8.1.x	Upgrade to 8.1.x		

The upgrade from 7.8.x or 8.0.x to 8.1.x is applied to V Series appliances with a software patch. Patches are installed via the Appliance console under the **Administration > Patches/Hotfixes > Patches** page.

Important

If you have multiple appliances, and:

- They are running version 7.8.3, 7.8.4, 8.0.0, or 8.0.1
- You plan to download the upgrade patch and then upload it to a local host for download to the other appliances

You may run into a Java version error. For a complete description and work around, please see the knowledge base article V-Series patch upload Java version error.

Important

If you have multiple appliances, and:

- They are running version 7.8.1 or 7.8.2
- And, you plan to download the upgrade patch and then upload it to other appliances

You need to apply hotfix 10 before you upload the upgrade patch. Hotfix 10 removes a file size limit that otherwise prevents the patch file from successfully uploading from the local storage location. This problem does not exist in v7.8.3; no hotfix is available or needed for that version.

To apply hotfix 10:

1. In the Appliance manager, go to **Administration > Patches / Hotfixes > Hotfixes**.
2. Locate and download the hotfix 10 rpm package.
   - If the appliance is running 7.8.1, enter **APP-7.8.1-010** and click **Find**.
   - If the appliance is running 7.8.2, enter **APP-7.8.2-010** and click **Find**.
3. After locating the correct hotfix, click **Download**.
4. Click **Install** to install the hotfix.
5. After installation is complete, restart the appliance.

After hotfix 10 is installed, to upload a patch on the appliance you must use Internet Explorer 11 or higher, or Chrome 11 or higher, or Firefox 4 or higher.

For an overview of the upgrade process, see the following upgrade flow diagrams:

- Web Security Gateway and Email Security Gateway on V-Series: Upgrade to 8.1.x
- Web Security and Web Security Gateway on V-Series Upgrade to 8.1.x
- Email Security Gateway on V-Series: Upgrade to 8.1.x

Estimates of time to complete upgrade

V Series Appliance Upgrade Guide | Upgrades to v8.1.x

The table below provides estimates of the time needed for the 8.1.0 patch to be installed on an appliance. The amount of time varies, as indicated. Not all V Series configurations are shown.

System	Configuration	Elapsed time
V10000	Dual mode: **TRITON AP-WEB** (formerly Web Security Gateway) Full policy source or, User directory and filtering or, Filtering only and **TRITON AP-EMAIL** (formerly Email Security Gateway)	40 - 60 minutes
V10000	Web security only: TRITON AP-WEB (formerly Web Security Gateway) Full policy source	35 - 45 minutes
V10000 V5000	Web security only: TRITON AP-WEB (formerly Web Security Gateway) User directory and filtering	35 - 45 minutes
V10000 V5000	TRITON AP-EMAIL (formerly Email Security Gateway) only	20 - 30 minutes
V5000	TRITON AP-WEB (formerly Web Security Gateway) Filtering only	30 minutes

The following provides a basic sample scenario:

Approximate total upgrade time, beginning to end, for all upgrade tasks:

- 1 Dual mode V10000 appliance
- 2 Windows 2012 servers: 1 for the TRITON Manager, 1 for Web and Email Log Server

Approximate upgrade time: 3 to 4 hours

The download speed for each patch depends on your network environment and can vary significantly.

Activity breakout:

- 1 hour to download the 8.1.x upgrade (patch) file (assuming the download speed is 512 kilobytes per second). This is the estimated time per patch. Depending on the upgrade path you take, your upgrade may involve more than one patch.

- 10 minutes to back up the V Series appliance
- 60 to 70 minutes for the patch to perform the upgrade and to verify that the upgrade was successful
- 20 minutes to download the version 8.1.x TRITON Unified Installer
- 40 to 60 minutes to run the installer to upgrade the TRITON management server and the Log Server host
- 5 minutes to restart the Windows servers and verify that the upgrade was successful

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied to the appliance, continuing until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 54.

Note

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

Preparing for the appliance upgrade

V Series Appliance Upgrade Guide | Upgrades to v8.1.x

Before applying the 8.1.x patch, perform these tasks and be aware of the following issues.

If you are 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 Web Security to v8.1.x.
- For email protection solutions, see Preparing for the upgrade.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to the **Administration > Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, save the backup file to an off-appliance location.

Content Gateway logs

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

To ensure that all Content Gateway logs are retained, you can download the Content Gateway logging directory.

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

Policy databases and TRITON databases are not affected by the upgrade.

Content Gateway Integrated Windows Authentication (IWA) settings

IWA domain joins should be preserved through the upgrade process. However, in case the 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, including the names of domains to which IWA is joined. Keep this record where you can easily retrieve it after the upgrade.

Administrator accounts

Make sure administrator accounts authenticated by a directory service have an email address specified in the directory service. In versions 7.8.1 and later, an email address is required for each administrator account (except group accounts).

Content Gateway changes

See the Websense Web Protection Release Notes for information about enhancements and changes in version 8.1.0.

Upgrade instructions

V Series Appliance Upgrade Guide | Upgrades to v8.1.x

Important

V Series appliance services are not available while the patch is being applied and until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 54.

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

1. If you have multiple V Series appliances, read *Upgrading multiple V-Series appliances*, page 58, **before** following this procedure.
2. Take all precautions to ensure that power to the V Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.
3. Back up appliance configuration and settings. See *Back up appliance configuration and settings*, page 55.
4. Restart the appliance (in Appliance Manager: **Status** > **General** > **Restart Appliance**). This ensures that the appliance is in a clean state for the upgrade.
5. If Policy Broker and Policy Database are installed on an off-appliance server, make sure they're upgraded to version 8.1.x and are running. You should simultaneously upgrade all TRITON services that are installed on the off-box server with Policy Broker and Policy Database.
6. To download the upgrade patch, in the Appliance Manager go to the **Administration > Patches/Hotfixes > Patches** tab. The upgrade patch for version 8.1.x should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The patch should be listed as available.

   Alternatively, the patch can be downloaded from www.forcepoint.com and uploaded to the appliance.

   

   Important

   If you are upgrading from 7.8.1 or 7.8.2, you need to apply hotfix 10. Hotfix 10 removes a file size limit that otherwise prevents the patch file from successfully uploading from the local storage location. See the **Important** note near to beginning of *Upgrading V Series appliances from v7.8.x or 8.0.x to 8.1.x*.

   a. Go to My Account (formerly MyWebsense) and select the **Downloads** tab. Click **Hotfixes & Patches**. In the **Product** drop down, select your appliance model. In the **Version** drop down, select 8.1.x.

   b. Download the upgrade patch.

   c. Log on to the Appliance manager and navigate to **Administration > Patches /Hotfixes**.

   d. Click **Upload Patch Manually,** then **Browse,** and then select the upgrade file for version 8.1.x.

   e. Click **Upload** to initiate upload of the patch to the appliance. Depending on the speed of the network, upload can take as long as 20 minutes. When the upload is complete the upgrade is listed in the **Available patches** list.

   Because local network speeds are usually faster than the Internet gateway, this is an efficient method when your deployment has many appliances. The upgrade patch is downloaded only once from patch download server. Other appliances upload the patch from the local location.
7. Click **Install** to apply the upgrade.

If the subscription agreement is not displayed within 60 seconds, close and re-open the browser, return to the **Patches / Hotfixes > Patches** page, and initiate the patch installation again.

Note that patch installation may take significantly longer than warned. See *Estimates of time to complete upgrade*, page 54.

8. The patch first performs a **system check** to make sure the appliance is set up correctly for the upgrade to succeed. This may take several minutes.
9. When you see that all patch pre-requisites have been met, you can continue to install the patch by clicking **Install Patch**.
10. Review the subscription agreement. Check **I accept this agreement** and **Continue**.
11. A confirmation message tells you that during the upgrade you are logged out of the Appliance manager and the appliance restarts. Click **OK** to begin the upgrade.

    While the upgrade is performed, services are **unavailable** to users.
12. After the appliance has automatically restarted, log on to the Appliance manager and go to **Administration** > **Patches/Hotfixes** > **Patches** tab. Under **Patch History**, for version 8.1.x, it should say "Patch has been installed successfully" in the **Comments** section. In the Appliance manager, you can also check the appliance version number by going to the **Configuration > System** page and looking under **System Information**.

    On the **Configuration** > **System** page, you can also confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.
13. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and subsequent appliances. See *Upgrading multiple V-Series appliances*, page 58.
14. Upgrade all TRITON components that you haven't already upgraded and which run off the appliance. These may include Web and Email Log Server, transparent identification agents, and the TRITON Manager. If Policy Broker and Policy Server are on the same off-appliance server as the TRITON Manager, you should have already upgraded all components on that box.

    See Upgrading Websense Web Protection Solutions and Upgrading Email Protection Solutions for instructions.

If the upgrade fails, contact Technical Support.

Upgrading multiple V-Series appliances

V Series Appliance Upgrade Guide | Upgrades to v8.1.x

When multiple V Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is an Email mode (only) appliance

Apply the upgrade patch for the version you want before upgrading the off-appliance components.

If the appliance includes a Web protection mode

It is a best practice to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

Best practice for upgrade sequence if Full policy source is on V-Series appliance

Follow this sequence whether the Full policy source is a Web mode (only) or Web and Email mode appliance.

Upgrade the **Full policy source** V Series appliance. Each time the upgrade completes, the appliance automatically restarts.

1. Sequentially apply the upgrade to all **User directory and filtering** appliances.
2. Sequentially apply the upgrade to all **Filtering only** appliances.
3. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on V-Series appliance

If you have multiple V Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure Policy Broker and Policy Server are upgraded to the version you want and are running. You should simultaneously upgrade all TRITON services that are installed on the off-appliance server with Policy Broker and Policy Server. Use the version 8.1.x TRITON Unified Installer to upgrade the Policy Broker system. See Upgrading Websense Web Protection Solutions for instructions.
2. Sequentially apply the upgrade to all **User directory and filtering** appliances. Each time the upgrade completes on an appliance, the appliance automatically restarts.
3. Sequentially apply the upgrade to all **Filtering only** appliances.
4. Use the version 8.1.x Websense installer to upgrade remaining off-appliance components. See Upgrading Websense Web Protection Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source*

appliance is unavailable, is being replaced, or is being re-imaged, then set a *User directory and filtering* or *Filtering only* appliance (temporarily) to be the Full policy source. To do this:

1. Back up the Full backup file of the User directory and filtering or Filtering only appliance in case changing the policy source fails.
2. On the secondary appliance, in the V Series manager, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **Full policy source**. Save the setting.
4. Upgrade this appliance to the version you want. The appliance automatically restarts when the upgrade finishes.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance. When the upgrade is done, the appliance automatically restarts.
2. On the previously upgraded secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **User directory and filtering** or **Filtering only** and enter the IP address of the primary appliance. Save the setting.
4. Use the version 8.1.x TRITON installer to upgrade remaining off-appliance components. See Upgrading Websense Web Protection Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.8.x or 8.0.x to 8.1.x*, page 51.

Post-upgrade activities

V Series Appliance Upgrade Guide | Upgrades to v8.1.x

Version 8.0.0 was the first product release to use a new, simplified product naming and grouping of the familiar TRITON product line.

Original Name	New Name
Websense Web Filter	Websense Web Filter & Security
Websense Web Security	Websense Web Filter & Security
Websense TRITON Web Security Gateway	Websense TRITON AP-WEB
Websense TRITON Web Security Gateway Anywhere	Websense TRITON AP-WEB with: ● Web Hybrid Module ● Web DLP Module ● Web Sandbox Module
Websense TRITON Data Security	Websense TRITON AP-DATA

Original Name	New Name
Websense TRITON Email Security Gateway	Websense TRITON AP-EMAIL with • Email DLP Module • Email Encryption Module • Email Sandbox Module
Websense TRITON Email Security Gateway Anywhere	Websense TRITON AP-EMAIL with • Email DLP Module • Email Sandbox Module • Email Hybrid Module • Image Analysis Module

The TRITON Unified Security Center is now known as TRITON Manager.

For more information about how these changes may affect you, or to change the add-on modules activated by your subscription, contact your sales partner or Forcepoint Sales representative.

Depending on the solutions installed on your appliances, after upgrade perform the following:

- If your appliance includes TRITON AP-EMAIL, perform the TRITON AP-EMAIL Post-upgrade activities.
- If your appliance hosts a Web Protection Policy Server (is a *User directory and filtering* appliance), log onto the TRITON Manager, go to the Web module **Settings > General > Policy Servers** page, and add the Policy Server instance. Next, go to the TRITON Manager **Appliances** tab and register the appliance.
- 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 8.1.0

  - 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

  Version 8.0.0

  - v8.0.0 Web Protection Release Notes
  - v8.0.0 TRITON AP-EMAIL Release Notes

  Version 7.8.4

  - v7.8.4 Web Security Release Notes
  - v7.8.4 Content Gateway Release Notes
  - v7.8.4 Email Security Gateway Release Notes

Version 7.8.3

- v7.8.3 Web Security Release Notes
- v7.8.3 Content Gateway Release Notes
- v7.8.3 Email Security Gateway Release Notes

Version 7.8.2

- v7.8.2 Web Security Release Notes
- v7.8.2 Content Gateway Release Notes
- v7.8.2 Email Security Gateway Release Notes

Upgrading V Series appliances from v7.8.x, 8.0.x, or 8.1.x to v8.2.x

V Series Appliance Upgrade Guide | Upgrades to v8.2.x

Related topics:

- *Estimates of time to complete upgrade*, page 64
- *Pre-upgrade activities*, page 65
- *Upgrade instructions*, page 66
- *Upgrading multiple V-Series appliances*, page 68
- *Post-upgrade activities*, page 70

This upgrade process applies to the following TRITON solutions and platforms:

- V10000 and V5000 appliances; see V-Series appliances supported with v8.x for a list of supported models
- TRITON AP-WEB and Web Filter & Security
- Web Security, Web Security Gateway, and Web Security Gateway Anywhere
- TRITON AP-EMAIL, Email Security Gateway, and Email Security Gateway Anywhere

If you are upgrading TRITON APX, see Upgrading to TRITON APX v8.2.

If you are upgrading TRITON AP-DATA, see Upgrading to TRITON AP-DATA v8.2.x.

The table lists the upgrade paths to version 8.2.x. The table also includes the path for upgrading from version 7.7.x to 7.8.1. You must upgrade to version 7.8.1 (or later) before upgrading to version 8.2.x:

To upgrade from	To this version	Step One	Step Two	Step Three	Step Four
7.8.4, 8.0.x, 8.1.x	8.2.x	Upgrade to 8.2.x			
7.8.1, 7.8.2, 7.8.3	8.2.x	Upgrade to 7.8.4	Upgrade to 8.2.x		
7.7.x	8.2.x	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.4	Upgrade to 8.2.x

The upgrade from 7.8.4, 8.0.x, or 8.1.x to 8.2.x is applied to V Series appliances with a software patch. Patches are installed via the Appliance console under the **Administration > Patches/Hotfixes > Patches** page.

Important

If you have multiple appliances, and:

- They are running version 7.8.4, 8.0.0, or 8.0.1
- You plan to download the upgrade patch and then upload it to a local host for download to the other appliances

You may run into a Java version error. For a complete description and work around, please see the knowledge base article V-Series patch upload Java version error.

Estimates of time to complete upgrade

V Series Appliance Upgrade Guide | Upgrades to v8.2.x

The table below provides estimates of the time needed for the 8.2.0 patch to be installed on an appliance. The amount of time varies, as indicated. Not all V Series configurations are shown.

System	Configuration	Elapsed time
V10000	Dual mode: **TRITON AP-WEB** (formerly Web Security Gateway) Full policy source or, User directory and filtering or, Filtering only and **TRITON AP-EMAIL** (formerly Email Security Gateway)	40 - 60 minutes
V10000	Web security only: TRITON AP-WEB (formerly Web Security Gateway) Full policy source	35 - 45 minutes
V10000 V5000	Web security only: TRITON AP-WEB (formerly Web Security Gateway) User directory and filtering	35 - 45 minutes
V10000 V5000	TRITON AP-EMAIL (formerly Email Security Gateway) only	20 - 30 minutes
V5000	TRITON AP-WEB (formerly Web Security Gateway) Filtering only	30 minutes

The following provides a basic sample scenario:

Approximate total upgrade time, beginning to end, for all upgrade tasks:

- 1 Dual mode V10000 appliance
- 2 Windows 2012 servers: 1 for the TRITON Manager, 1 for Web and Email Log Server

Approximate upgrade time: 3 to 4 hours

The download speed for each patch depends on your network environment and can vary significantly.

Activity breakout:

- 1 hour to download the 8.2.x upgrade (patch) file (assuming the download speed is 512 kilobytes per second). This is the estimated time per patch. Depending on the upgrade path you take, your upgrade may involve more than one patch.

- 10 minutes to back up the V Series appliance
- 60 to 70 minutes for the patch to perform the upgrade and to verify that the upgrade was successful
- 20 minutes to download the version 8.2.x TRITON Unified Installer
- 40 to 60 minutes to run the installer to upgrade the TRITON management server and the Log Server host
- 5 minutes to restart the Windows servers and verify that the upgrade was successful

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied to the appliance, continuing until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 64.

Note

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

Pre-upgrade activities

V Series Appliance Upgrade Guide | Upgrades to v8.2.x

Before applying the 8.2.x patch, perform these tasks and be aware of the following issues.

If you are 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 Web Security to v8.2.x.
- For email protection solutions, see Preparing for the upgrade.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to the **Administration > Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, save the backup file to an off-appliance location.

Content Gateway logs

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

To ensure that all Content Gateway logs are retained, you can download the Content Gateway logging directory.

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.

Policy databases and TRITON databases are not affected by the upgrade.

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. Keep this record where you can easily retrieve it after the upgrade.

Administrator accounts

Make sure administrator accounts authenticated by a directory service have an email address specified in the directory service. In versions 7.8.1 and later, an email address is required for each administrator account (except group accounts).

Content Gateway changes

See the Forcepoint Web Protection Release Notes for information about enhancements and changes in version 8.2.0.

Upgrade instructions

V Series Appliance Upgrade Guide | Upgrades to v8.2.x

Important

V Series appliance services are not available while the patch is being applied and until the appliance completes restarting. See *Estimates of time to complete upgrade*, page 64.

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

1. If you have multiple V Series appliances, read *Upgrading multiple V-Series appliances*, page 68, **before** following this procedure.

2. Take all precautions to ensure that power to the V Series appliance is not interrupted during the upgrade. Power failure can result in operating system and software component corruption.
3. Back up appliance configuration and settings. See *Back up appliance configuration and settings*, page 65.
4. Restart the appliance (in Appliance Manager: **Status** > **General** > **Restart Appliance**). This ensures that the appliance is in a clean state for the upgrade.
5. If Policy Broker and Policy Database are installed on an off-appliance server, make sure they're upgraded to version 8.2.x and are running. You should simultaneously upgrade all TRITON services that are installed on the off-box server with Policy Broker and Policy Database.
6. To download the upgrade patch, in the Appliance Manager go to the **Administration > Patches/Hotfixes > Patches** tab. The upgrade patch for version 8.2.x should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The patch should be listed as available.

   Alternatively, the patch can be downloaded from www.forcepoint.com and uploaded to the appliance.

   a. Go to My Account (formerly MyWebsense), and select the **Downloads** tab. Click **Hotfixes & Patches**. In the **Product** drop down, select your appliance model. In the **Version** drop down, select 8.2.x.

   b. Download the upgrade patch.

   c. Log on to the Appliance manager and navigate to **Administration > Patches /Hotfixes**.

   d. Click **Upload Patch Manually,** then **Browse,** and then select the upgrade file for version 8.2.x.

   e. Click **Upload** to initiate upload of the patch to the appliance. Depending on the speed of the network, upload can take as long as 20 minutes. When the upload is complete the upgrade is listed in the **Available patches** list.

   Because local network speeds are usually faster than the Internet gateway, this is an efficient method when your deployment has many appliances. The upgrade patch is downloaded only once from patch download server. Other appliances upload the patch from the local location.
7. Click **Install** to apply the upgrade.

   If the subscription agreement is not displayed within 60 seconds, close and re-open the browser, return to the **Patches / Hotfixes > Patches** page, and initiate the patch installation again.

   Note that patch installation may take significantly longer than warned. See *Estimates of time to complete upgrade*, page 64.
8. The patch first performs a **system check** to make sure the appliance is set up correctly for the upgrade to succeed. This may take several minutes.
9. When you see that all patch pre-requisites have been met, you can continue to install the patch by clicking **Install Patch**.
10. Review the subscription agreement. Check **I accept this agreement** and **Continue**.

11. A confirmation message tells you that during the upgrade you are logged out of the Appliance manager and the appliance restarts. Click **OK** to begin the upgrade.

    While the upgrade is performed, services are **unavailable** to users.

12. After the appliance has automatically restarted, log on to the Appliance manager and go to **Administration** > **Patches/Hotfixes** > **Patches** tab. Under **Patch History**, for version 8.2.x, it should say "Patch has been installed successfully" in the **Comments** section. In the Appliance manager, you can also check the appliance version number by going to the **Configuration > System** page and looking under **System Information**.

    On the **Configuration** > **System** page, you can also confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.

13. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and subsequent appliances. See *Upgrading multiple V-Series appliances*, page 68.

14. Upgrade all TRITON components that you haven't already upgraded and which run off the appliance. These may include Web and Email Log Server, transparent identification agents, and the TRITON Manager. If Policy Broker and Policy Server are on the same off-appliance server as the TRITON Manager, you should have already upgraded all components on that box.

    See Upgrading Web Protection Solutions and Upgrading Email Protection Solutions for instructions.

If the upgrade fails, contact Technical Support.

Upgrading multiple V-Series appliances

V Series Appliance Upgrade Guide | Upgrades to v8.2.x

When multiple V Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is an Email mode (only) appliance

Apply the upgrade patch for the version you want before upgrading the off-appliance components.

If the appliance includes a Web protection mode

It is a best practice to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

Best practice for upgrade sequence if Full policy source is on V-Series appliance

Follow this sequence whether the Full policy source is a Web mode (only) or Web and Email mode appliance.

Upgrade the **Full policy source** V Series appliance. Each time the upgrade completes, the appliance automatically restarts.

1. Sequentially apply the upgrade to all **User directory and filtering** appliances.
2. Sequentially apply the upgrade to all **Filtering only** appliances.
3. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on V-Series appliance

If you have multiple V Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure Policy Broker and Policy Server are upgraded to the version you want and are running. You should simultaneously upgrade all TRITON services that are installed on the off-appliance server with Policy Broker and Policy Server. Use the version 8.2.x TRITON Unified Installer to upgrade the Policy Broker system. See Upgrading Web Protection Solutions for instructions.
2. Sequentially apply the upgrade to all **User directory and filtering** appliances. Each time the upgrade completes on an appliance, the appliance automatically restarts.
3. Sequentially apply the upgrade to all **Filtering only** appliances.
4. Use the version 8.2.x Forcepoint installer to upgrade remaining off-appliance components. See Upgrading Web Protection Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source* appliance is unavailable, is being replaced, or is being re-imaged, then set a *User directory and filtering* or *Filtering only* appliance (temporarily) to be the Full policy source. To do this:

1. Back up the Full backup file of the User directory and filtering or Filtering only appliance in case changing the policy source fails.
2. On the secondary appliance, in the V Series manager, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **Full policy source**. Save the setting.
4. Upgrade this appliance to the version you want. The appliance automatically restarts when the upgrade finishes.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance. When the upgrade is done, the appliance automatically restarts.
2. On the previously upgraded secondary appliance, in the V Series console, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **User directory and filtering** or **Filtering only** and enter the IP address of the primary appliance. Save the setting.
4. Use the version 8.2.x TRITON installer to upgrade remaining off-appliance components. See Upgrading Web Protection Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.8.x, 8.0.x, or 8.1.x to v8.2.x*, page 62.

Post-upgrade activities

V Series Appliance Upgrade Guide | Upgrades to v8.2.x

If you have upgraded from version 7.8.4 or earlier you need to know that version 8.0.0 and later use simplified product naming and grouping of the familiar TRITON product line.

Original Name	New Name
Websense Web Filter & Security	Web Filter & Security
Websense TRITON Web Security Gateway	TRITON AP-WEB
Websense TRITON Web Security Gateway Anywhere	TRITON AP-WEB with: ● Web Hybrid Module ● Web DLP Module ● Web Sandbox Module
Websense TRITON Data Security	TRITON AP-DATA
Websense TRITON Email Security Gateway	TRITON AP-EMAIL with ● Email DLP Module ● Email Encryption Module ● Email Sandbox Module
Websense TRITON Email Security Gateway Anywhere	TRITON AP-EMAIL with ● Email DLP Module ● Email Sandbox Module ● Email Hybrid Module ● Image Analysis Module

The TRITON Unified Security Center is now known as TRITON Manager.

For more information about how these changes may affect you, or to change the add-on modules activated by your subscription, contact your sales partner or Forcepoint Sales representative.

Depending on the solutions installed on your appliances, after upgrade perform the following:

- If your appliance includes TRITON AP-EMAIL, perform the TRITON AP-EMAIL Post-upgrade activities.
- If your appliance hosts a Web Protection Policy Server (is a *User directory and filtering* appliance), log onto the TRITON Manager, go to the Web module **Settings > General > Policy Servers** page, and add the Policy Server instance. Next, go to the TRITON Manager **Appliances** tab and register the appliance.
- 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 8.2.0

  - 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

  Version 8.0.0

  - v8.0.0 Web Protection Release Notes
  - v8.0.0 TRITON AP-EMAIL Release Notes
  - v8.0.0 TRITON AP-DATA Release Notes

Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.3.x

Related topics:

- *Estimates of time to completion*, page 89
- *Rollback*, page 90
- *Summary of upgrade procedure*, page 90
- *Pre-upgrade activities*, page 91
- *Upgrade procedure*, page 93
- *Upgrading multiple V Series appliances*, page 95
- *Post-upgrade activities*, page 97

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.

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

- Upgrade Instructions for TRITON AP-WEB
  (also applies to v7.8.4 Web Security Gateway/Anywhere)
- Upgrade Instructions for Web Filter & Security
  (also applies to v7.8.4 Web Filter and v7.8.4 Web Security)
- TRITON AP-EMAIL: Upgrading email protection solutions

Important

v8.3 does not support Dual Mode appliances—appliances that host *both* TRITON AP-EMAIL and TRITON AP-WEB, or TRITON AP-EMAIL and Web Filter & Security.

Before upgrading a **Dual Mode** appliance, either the email or web module must be migrated to a new TRITON appliance. Migration of TRITON AP-EMAIL is recommended. To ease the email migration effort, special tools have been developed, and a special procedure is recommended. For details, see Upgrading V-Series Dual Mode Appliances to Version 8.3.

Important

In this upgrade, the V-Series Appliance Manager is replaced with the TRITON Appliance command-line interface (CLI). (The new TRITON Appliance Manager is coming in 2017.)

The upgrade process begins in the Appliance Manager, as usual, and ends in the CLI to perform several post-upgrade activities.

For an introduction to the CLI, see V-Series Appliances: Visual Primer for the v8.3 Appliance CLI.

This upgrade process applies to the following platforms and TRITON solutions:

- **V10000 and V5000 appliances**. For a list of supported models, see V-Series appliances supported with v8.x.
- **TRITON AP-WEB and Web Filter & Security, v8.0 and higher**
- **Web Security, and Web Security Gateway / Anywhere, v7.8.4**
- **TRITON AP-EMAIL, v8.0 and higher**
- **Email Security Gateway / Anywhere, v7.8.4**

If you are upgrading TRITON APX (multiple TRITON solutions), see Upgrading to TRITON APX v8.3.

If you are upgrading TRITON AP-DATA, see Upgrading to TRITON AP-DATA v8.3.x.

Following is a list of upgrade paths to v8.3.x. You must upgrade to v7.8.4 (or higher) before upgrading to v8.3.x:

To upgrade from	To this version	Step One	Step Two	Step Three	Step Four
7.8.4, 8.0.x, 8.1.x, 8.2.x	8.3.x	Upgrade to 8.3.x			
7.8.1, 7.8.2, 7.8.3	8.3.x	Upgrade to 7.8.4	Upgrade to 8.3.x		
7.7.x	8.3.x	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.4	Upgrade to 8.3.x

The upgrade is applied with a software patch and is initiated in the Appliance Manager on the **Administration > Patches/Hotfixes > Patches** page. The upgrade procedure ends with some tasks performed in the TRITON Appliances command-line interface (CLI). Accessing the CLI is unchanged from past versions. If you're

unfamiliar with the CLI, see the CLI section of the v8.3.0 TRITON Appliances Release Notes.

Important

The upgrade process is designed for functional appliances 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

If you have multiple appliances, and:

- They are running version 7.8.4, 8.0.0, or 8.0.1
- You plan to download the upgrade patch to a local host and then upload it to multiple appliances

You may run into a Java version error. For a complete description and work around, please see the knowledge base article V-Series patch upload Java version error.

Estimates of time to completion

Below are estimates of the time it takes for the 8.3.0 upgrade patch to run. The amount of time is variable, as indicated. As a best practice, allow the patch to run at least 90 minutes before aborting the install and contacting Forcepoint Technical Support.

Mode	Model	Elapsed time
TRITON AP-WEB (v7.8.4: Web Security Gateway)	**V10000 G3, G4** **V10000 G2R2** **V5000 G3, G4** **V5000 G2R2**	30 - 45 minutes 50 - 70 minutes 65 - 85 minutes 70 - 90 minutes
Web Filter & Security (7.8.4: Web Security, Web Filter)	**V5000 G3, G4** **V5000 G2R2**	40 - 60 minutes 50 - 70 minutes
TRITON AP-EMAIL (v7.8.4: Email Security Gateway)	**V10000 G3, G4** **V10000 G2R2** **V5000 G3, G4** **V5000 G2R2**	20 - 35 minutes 35 - 55 minutes 50 - 65 minutes 60 - 80 minutes

The following is a sample start-to-finish upgrade scenario:

Approximate total upgrade time for all upgrade tasks:

- 1 TRITON AP-WEB V10000 appliance
- 2 Windows 2012 servers: 1 for the TRITON Manager, 1 for Web Log Server

Approximate upgrade time: 3 to 4 hours

The download speed for each patch depends on your network environment and can vary significantly.

Activity breakout:

- 20 minutes to download the 8.3.x upgrade patch file, assuming the download speed is 1024 kilobytes per second. This is the estimated time per patch. Depending on the upgrade path you take, your upgrade may involve more than one patch.
- 40 to 60 minutes for the patch to perform the upgrade and for you to verify that the upgrade was successful.
- 15 minutes to download the version 8.3.x TRITON Unified Installer.
- 40 to 60 minutes to run the installer to upgrade the TRITON management server and the Log Server host.
- 5 minutes to restart the Windows servers and verify that the upgrade was successful.

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied to the appliance, continuing until the appliance completes its final restart.

Note

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

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 fully restored. In this case, off-appliance components may need to be restarted.

Summary of upgrade procedure

1. Perform the pre-upgrade activities.
2. Download the v8.3.x TRITON Unified Installer.
3. Download the appliance upgrade patch file.
4. If the appliance hosts TRITON AP-WEB or Web Filter & Security, upgrade the **Full policy source machine** (hosts Policy Broker/Policy Database). Note that all TRITON components on the machine are upgraded when Policy Broker/Policy Database are upgraded.
5. Apply the appliance upgrade patch.
6. Upgrade the TRITON management server (if not upgraded when Policy Broker/Policy Database were upgraded), and other servers that host TRITON components.
7. Log on to the CLI and perform post-upgrade activities.

Pre-upgrade activities

Before applying the v8.3.x 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.

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

At the end of the upgrade procedure you will need to log on to the v8.3 appliance CLI and perform a small number of checks.

The v8.3 appliance CLI is accessed in the same way as the 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 in 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

All 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 TRITON 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

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 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.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to the **Administration > Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, **save the backup file to an off-appliance location**.

Content Gateway logs

If the appliance hosts TRITON AP-WEB (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. Keep this record where you can easily retrieve it after the upgrade.

Administrator accounts

Make sure administrator accounts authenticated by a directory service have an email address specified in the directory service. In versions 7.8.1 and higher, an email address is required for each administrator account (except group accounts).

Upgrade procedure

Important

V-Series appliance services are not available while the patch is being applied and until the appliance completes restarting. See *Estimates of time to completion*, page 89.

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

1. If you have multiple V-Series appliances, read *Upgrading multiple V Series appliances*, page 95, **before** following this procedure.
2. If you are upgrading a TRITON AP-WEB or Web Filter & Security deployment and Policy Broker and Policy Database are installed on an off-appliance server, upgrade that machine now. Upon completion confirm that Policy Broker and Policy Database services are running. See Upgrading Web Protection Solutions.

   Note that at the same time that Policy Broker and Policy Database are upgraded, all other TRITON components on the machine are upgraded.

   

   Important

   For the upgrade to complete successfully, the appliance must be able to communicate with the Policy Broker and Policy Database services.

3. 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 policy server instance. In the Web module of TRITON Manager, go to the **Settings > General > Policy Servers** page and unregister the instance.
4. If not already done, perform a full appliance backup and save the backup file to an off-appliance location.See *Back up appliance configuration and settings*, page 92.
5. Restart the appliance (in Appliance Manager: **Status** > **General** > **Restart Appliance**). This ensures that the appliance is in a clean state for the upgrade.
6. Download the upgrade patch.

   In the Appliance Manager go to the **Administration > Patches/Hotfixes > Patches** tab. The upgrade patch for version 8.3.x should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The patch should be listed as available.

   Alternatively, the patch can be downloaded from www.forcepoint.com and uploaded to the appliance.

   a. Go to My Account (formerly MyWebsense) and select the **Downloads** tab. Find your Forcepoint appliance model (for example, V10000) and click **8.3.0**.

   b. Click on **v8.3 V-Series upgrade patch** and on the resulting page, click **Download**.

   c. Log on to the Appliance manager and navigate to **Administration > Patches /Hotfixes**.

   d. Click **Upload Patch Manually,** then **Browse,** and then select the upgrade file for version 8.3.x.

   e. Click **Upload** to initiate upload of the patch to the appliance. Depending on the speed of the network, upload can take 20 minutes or more. When the upload is complete the upgrade is listed in the **Available patches** list.

   Because local network speeds are usually faster than the Internet gateway, this is an efficient method when your deployment has many appliances. The upgrade

patch is downloaded only once from the patch download server. Other appliances upload the patch from the local location.

7. Take all precautions to ensure that power to the appliance is not interrupted during the upgrade.
8. Click **Install** to apply the upgrade.

   The patch performs several system checks to ensure that the appliance is ready for upgrade. The checks can take several minutes.
9. When you see that all pre-requisites have been met, you can continue to install the patch by clicking **Install Patch**.
10. Review the subscription agreement. Check **I accept this agreement** and **Continue**.
11. A confirmation message tells you that during the upgrade you are logged out of the Appliance manager and the appliance restarts. Click **OK** to begin the upgrade.

    While the upgrade is performed, services are **unavailable** to users.

Important

On rare occasions, these problems have been seen.

- Shortly after the install begins, the Appliance Manager page refreshes and displays the message **Patch 8.3.0 installed successfully**.
- The upgrade progress bar stays at 0% for a long time.

Should you experience either problem, exit the Appliance Manager and then log on again and restart the upgrade.

12. After the appliance restarts, perform *Post-upgrade activities*, page 13.
13. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and subsequent appliances. See *Upgrading multiple V Series appliances*, page 95.
14. Upgrade all TRITON components that you haven't already upgraded and which run off the appliance. These may include Web and Email Log Server, transparent identification agents, and the TRITON Manager. If Policy Broker and Policy Server are on the same off-appliance server as the TRITON Manager, you should have already upgraded all components on that box.

    See Upgrading Web Protection Solutions and Upgrading Email Protection Solutions for instructions.

If the upgrade fails, contact Technical Support for assistance.

Upgrading multiple V-Series appliances

Important

Dual-mode appliances are not supported by v8.3.x and higher.

If you are upgrading a dual-mode appliance, use the special guide Upgrading V-Series Dual Mode Appliances to version 8.3.

When multiple V-Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is a TRITON AP-EMAIL appliance

Apply the upgrade patch to all TRITON AP-EMAIL appliances before upgrading the off-appliance components.

If the appliance includes a Web protection mode

It is a best practice to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

Best practice for upgrade sequence if Full policy source is on a V-Series appliance

1. Upgrade the **Full policy source** appliance.
2. Upgrade all **User directory and filtering** appliances.
3. Upgrade all **Filtering only** appliances.
4. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on a V-Series appliance

If you have multiple V-Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure Policy Broker and Policy Server are upgraded to the version you want and that the services are running. Other TRITON components installed on the Policy Broker and Policy Server machine are upgraded at the same time. Use the version 8.3.x TRITON Unified Installer to upgrade the Policy Broker machine. See Upgrading Web Protection Solutions for instructions.
2. Upgrade all *User directory and filtering* appliances. Each time the upgrade completes on an appliance, the appliance automatically restarts.
3. Upgrade all *Filtering only* appliances.
4. Use the version 8.3.x Forcepoint installer to upgrade remaining off-appliance components. See Upgrading Web Protection Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source* appliance is unavailable, is being replaced, or is being re-imaged, then set a *User directory and filtering* or *Filtering only* appliance (temporarily) to be the *Full policy source*. To do this:

1. Create a full backup of the appliance in case changing the policy source fails.
2. On the secondary appliance, in the V-Series manager, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **Full policy source**. Save the setting.
4. Upgrade this appliance to the version you want. The appliance automatically restarts when the upgrade finishes.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance. When the upgrade is done, the appliance automatically restarts.
2. On the previously upgraded secondary appliance, in the CLI enter **config** mode and change the policy mode:

   ```
   set mode <user|filter> --policy-source <policy_src_ip_addr>
   ```

3. Use the version 8.3.x TRITON installer to upgrade remaining off-appliance components. See Upgrading Web Protection Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.4.x*, page 86.

Post-upgrade activities

If you have upgraded from version 7.8.4, you need to know that version 8.0.0 and higher use simplified product naming.

Original Name	New Name
Websense Web Filter & Security	Web Filter & Security
Websense TRITON Web Security Gateway	TRITON AP-WEB
Websense TRITON Web Security Gateway Anywhere	TRITON AP-WEB with: • Web Hybrid Module • Web DLP Module • Web Sandbox Module

Original Name	New Name
Websense TRITON Data Security	TRITON AP-DATA
Websense TRITON Email Security Gateway	TRITON AP-EMAIL with • Email DLP Module • Email Encryption Module • Email Sandbox Module
Websense TRITON Email Security Gateway Anywhere	TRITON AP-EMAIL with • Email DLP Module • Email Sandbox Module • Email Hybrid Module • Image Analysis Module

The TRITON Unified Security Center is renamed TRITON Manager.

For more information about how these changes may affect you, or to change the add-on modules activated by your subscription, contact your sales partner or Forcepoint Sales representative.

Depending on the solutions installed on your appliances, after upgrade perform the following:

In the CLI

For information about accessing the CLI, see *Configure and test access to the command-line interface (CLI)*, page 91.

- In the CLI, elevate to **config** mode and perform system checks and verify some configuration settings.
  - Check 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                : TRITON AP-WEB
    Policy_mode         : Filtering only
    Policy_source_ip:   : 10.222.21.10
    ```

  - View the upgrade history.

    ```
    show upgrade --history
    ```

  - Check appliance status.

    ```
    show appliance status
    ```

    ```
    show <module>
    ```

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

    ```
    restart <module>
    ```

- Check network interface settings.

  ```
  show interface info
  ```

  If you have bonded interface, note that the names used to indicate the type of bond 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 traffic to 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 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.

- 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 because most files that you want to save, or load, must be done with a filestore. Only system backup and log files are kept on the appliance.

  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 <name> --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
  ```

- Use the **set log archive** command to establish size and frequency values for archiving log files.

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.x

  - v8.0.1 Web Protection Release Notes
  - v8.0.0 Web Protection Release Notes
  - v8.0.1 TRITON 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

Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.4.x

Important

Forcepoint V Series 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.

Related topics:

- *Product renaming*, page 89
- *Estimates of time to completion*, page 89
- *Rollback*, page 90
- *Summary of upgrade procedure*, page 90
- *Pre-upgrade activities*, page 91
- *Upgrade procedure*, page 93
- *Upgrading multiple V Series appliances*, page 95
- *Post-upgrade activities*, page 97

Version 8.3 of the Forcepoint appliance platform introduced a new architecture. Before upgrading Forcepoint appliances to v8.4.0, it is important that you read the v8.3.0 TRITON Appliances Release Notes, in addition to the v8.4.0 Forcepoint Appliances Release Notes.

When upgrading your Forcepoint security products, always start with the product upgrade guide.

- Forcepoint Email Security: Upgrading email protection solutions
- Upgrade Instructions for Forcepoint Web Security
  (also applies to v7.8.4 Web Security Gateway/Anywhere)
- Upgrade Instructions for Forcepoint URL Filtering
  (also applies to v7.8.4 Web Security)

Important

Versions 8.3 and higher do not support dual-mode appliances—appliances that host *both* Forcepoint Email Security and Forcepoint Web Security, or Forcepoint Email Security and Forcepoint URL Filtering.

Before upgrading a dual-mode appliance, either the email or web module must be migrated to a new Forcepoint appliance. Migration of Forcepoint Email Security is recommended. To ease the email migration effort, special tools have been developed and a special procedure is recommended. For details, see Upgrading V-Series Dual-Mode Appliances.

The upgrade process applies to the following platforms and Forcepoint solutions:

- V5000 and V10000 appliances. For a list of supported models, including the V10K G2R2, see V-Series appliances supported with v8.x.
- TRITON AP-WEB and Web Filter & Security, v8.0.x, v8.1, v8.2, and v8.3
- Web Security, and Web Security Gateway / Anywhere, v7.8.4
- TRITON AP-EMAIL, v8.0.x, v8.1, v8.2, and v8.3
- Email Security Gateway / Anywhere, v7.8.4

If you are upgrading TRITON APX (multiple TRITON solutions), see Upgrading more than one Forcepoint solution.

If you are upgrading TRITON AP-DATA, see Upgrading to Forcepoint DLP v8.4.x.

Following is a list of upgrade paths to v8.4.x. You must upgrade to v7.8.4 (or higher) before upgrading to v8.4.x:

To upgrade from	To this version	Step One	Step Two	Step Three	Step Four
7.8.4, 8.1.x, 8.2.x, 8.3.x	8.4.x	Upgrade to 8.4.x			
8.0.x	8.4.x	Upgrade to 8.3.0	Upgrade to 8.4.x		
7.8.1, 7.8.2, 7.8.3	8.4.x	Upgrade to 7.8.4	Upgrade to 8.4.x		
7.7.x	8.4.x	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.4	Upgrade to 8.4.x

Important

If you are upgrading from version 8.0.x you must first upgrade to v8.3.0 and then upgrade to v8.4.0. To upgrade to v8.3.0, see *Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.3.x*, page 72. To upgrade from v8.3.0 to v8.4.0, follow the instruction in the V, X, & Virtual Appliance Upgrade Guide from v8.3 to v8.4.

The upgrade is applied with a software patch and is initiated in the Appliance Manager on the **Administration > Patches/Hotfixes > Patches** page. The upgrade procedure ends with some tasks performed in the Forcepoint Appliances command-line interface (CLI). Accessing the CLI is unchanged from past versions. If you are unfamiliar with the CLI, see the CLI section of the v8.3.0 TRITON Appliances Release Notes.

Important

The upgrade process is designed for appliances 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

If you have multiple appliances, and:

- They are running version 7.8.4, 8.0.0, or 8.0.1
- You plan to download the upgrade patch to a local host and then upload it to multiple appliances

You may run into a Java version error. For a complete description and work around, please see the knowledge base article V-Series patch upload Java version error.

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.

Estimates of time to completion

Below are estimates of the time it takes for the v8.4.0 upgrade patch to run. The amount of time is variable, as indicated. As a best practice, allow the patch to run at least 90 minutes before aborting the install and contacting Forcepoint Technical Support.

Mode	Model	Elapsed time
TRITON AP-WEB (v7.8.4: Web Security Gateway)	**V10000 G3, G4** **V5000 G3, G4** **V5000 G2R2**	30 - 45 minutes 65 - 85 minutes 70 - 90 minutes
Web Filter & Security (7.8.4: Web Security)	**V5000 G3, G4** **V5000 G2R2**	40 - 60 minutes 50 - 70 minutes
TRITON AP-EMAIL (v7.8.4: Email Security Gateway)	**V10000 G3, G4** **V5000 G3, G4** **V5000 G2R2**	20 - 35 minutes 50 - 65 minutes 60 - 80 minutes

The following is a sample start-to-finish upgrade scenario for:

- 1 TRITON AP-WEB V10000 appliance
- 2 Windows 2012 servers: 1 for the TRITON Manager, 1 for Web Log Server

Approximate total upgrade time for all upgrade tasks is 3 to 4 hours.

The download speed for each patch depends on your network environment and can vary significantly.

Activity breakout:

- 20 minutes to download the v8.4.x appliance upgrade patch file, assuming the download speed is 1024 kilobytes per second.
- 40 to 60 minutes for the patch to perform the upgrade and for you to verify that the upgrade was successful.
- 15 minutes to download the version v8.4.x Forcepoint Security Installer (for Windows components).
- 40 to 60 minutes to run the installer to upgrade the TRITON management server (renamed Forcepoint management server in v8.4) and the Log Server host.
- 5 minutes to restart the Windows servers and verify that the upgrade was successful.

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied to the appliance, continuing until the appliance completes its final restart.

Note

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

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 fully restored. In this case, off-appliance components may need to be restarted.

Summary of upgrade procedure

1. Perform the pre-upgrade activities.
2. Download the v8.4.x Forcepoint Security Installer.
3. Download the appliance upgrade patch file.
4. If the appliance hosts TRITON AP-WEB or Web Filter & Security, upgrade the **Full policy source machine** (hosts Policy Broker/Policy Database). Note that all TRITON components on the machine are upgraded when Policy Broker/Policy Database are upgraded.
5. Apply the appliance upgrade patch.
6. Upgrade the TRITON management server (if not upgraded when Policy Broker/Policy Database were upgraded), and other servers that host TRITON components.
7. Log on to the CLI and perform post-upgrade activities.

Pre-upgrade activities

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

If you are 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 to v8.4.x web protection solutions and v8.4.0 Release Notes for Web Protection Solutions.
- For email protection solutions, see Upgrading email protection solutions and v8.4.0 Release Notes for Forcepoint Email Security.

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

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

The v8.4 appliance CLI is accessed in the same way as the V Series CLI. If you have not used the V Series CLI, or have not 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 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 have an integrated DELL Remote Access Controller (iDRAC). If you have never worked with the iDRAC, see **Using the iDRAC** in the Forcepoint Appliances Getting Started Guide.

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

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 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.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to the **Administration > Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, **save the backup file to an off-appliance location**.

Content Gateway logs

If the appliance hosts TRITON AP-WEB (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. Keep this record where you can easily retrieve it after the upgrade.

Administrator accounts

Make sure administrator accounts authenticated by a directory service have an email address specified in the directory service. In versions 7.8.1 and higher, an email address is required for each administrator account (except group accounts).

Upgrade procedure

Important

V Series appliance services are not available while the patch is being applied and until the appliance completes restarting. See *Estimates of time to completion*, page 89.

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

1. If you have multiple V Series appliances, read *Upgrading multiple V Series appliances*, page 95, **before** following this procedure.
2. If you are upgrading a TRITON AP-WEB or Web Filter & Security deployment and Policy Broker and Policy Database are installed on an off-appliance server, upgrade that machine now. Upon completion confirm that Policy Broker and Policy Database services are running. See Upgrading Web Protection Solutions.

   Note that at the same time that Policy Broker and Policy Database are upgraded, all other TRITON components on the machine are upgraded.

Important

For the upgrade to complete successfully, the appliance must be able to communicate with the Policy Broker and Policy Database services.

3. 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 policy server instance. In the Web module of TRITON Manager, go to the **Settings > General > Policy Servers** page and unregister the instance.

4. If not already done, perform a full appliance backup and save the backup file to an off-appliance location.See *Back up appliance configuration and settings*, page 92.

5. Restart the appliance (in Appliance Manager: **Status** > **General** > **Restart Appliance**). This ensures that the appliance is in a clean state for the upgrade.

6. Download the upgrade patch.

   In the Appliance Manager go to the **Administration > Patches/Hotfixes > Patches** tab. The upgrade patch for version 8.4.x should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The patch should be listed as available.

   Alternatively, the patch can be downloaded from forcepoint.com and uploaded to the appliance.

   a. Go to My Account and select the **Downloads** tab. Find your Forcepoint appliance model (for example, V10000) and click **8.4.0**.

   b. Click on **v8.4 V Series upgrade patch** and on the resulting page, click **Download**.

   c. Log on to the Appliance manager and navigate to **Administration > Patches /Hotfixes**.

   d. Click **Upload Patch Manually,** then **Browse,** and then select the upgrade file for version 8.4.x.

   e. Click **Upload** to initiate upload of the patch to the appliance. Depending on the speed of the network, upload can take 20 minutes or more. When the upload is complete the upgrade is listed in the **Available patches** list.

   Because local network speeds are usually faster than the Internet gateway, this is an efficient method when your deployment has many appliances. The upgrade patch is downloaded only once from the patch download server. Other appliances upload the patch from the local location.

7. Take all precautions to ensure that power to the appliance is not interrupted during the upgrade.

8. Click **Install** to apply the upgrade.

   The patch performs several system checks to ensure that the appliance is ready for upgrade. The checks may take several minutes.

9. When you see that all pre-requisites have been met, you can continue to install the patch by clicking **Install Patch**.

10. Review the subscription agreement. Check **I accept this agreement** and **Continue**.

11. A confirmation message tells you that during the upgrade you are logged out of the Appliance manager and the appliance restarts. Click **OK** to begin the upgrade.

While the upgrade is performed, services are **unavailable** to users.

Important

On rare occasions, these problems have been seen in appliances prior to v8.3.

- Shortly after the install begins, the Appliance Manager page refreshes and displays the message **Patch 8.4.0 installed successfully**.
- The upgrade progress bar stays at 0% for a long time.

Should you experience either problem, exit the Appliance Manager and then log on again and restart the upgrade.

12. After the appliance restarts, perform *Post-upgrade activities*, page 13.
13. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and subsequent appliances. See *Upgrading multiple V Series appliances*, page 95.
14. Upgrade all TRITON components that you haven't already upgraded and which run off the appliance. These may include Web and Email Log Server, transparent identification agents, and the TRITON Manager. If Policy Broker and Policy Server are on the same off-appliance server as the TRITON Manager, you should have already upgraded all components on that box.

    See Upgrading Web Protection Solutions and Upgrading Email Protection Solutions for instructions.

If the upgrade fails, contact Technical Support for assistance.

Upgrading multiple V Series appliances

Important

Dual-mode appliances are not supported by v8.3.x and higher.

If you are upgrading a dual-mode appliance, use the special guide V Series Dual-mode Upgrade Guide.

When multiple V Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is a TRITON AP-EMAIL appliance

Apply the upgrade patch to all TRITON AP-EMAIL appliances before upgrading the off-appliance components.

If the appliance includes a Web protection solution

Best practice for upgrade sequence if Full policy source is on a V Series appliance

1. Upgrade the *Full policy source* appliance.
2. Upgrade all *User directory and filtering* appliances.
3. Upgrade all *Filtering only* appliances.
4. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on a V Series appliance

If you have multiple V Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure that the Policy Broker and Policy Server machine are upgraded to the version you want and that the services are running. Other TRITON components installed on the Policy Broker and Policy Server machine are upgraded at the same time. Use the version 8.4.x Forcepoint Security Installer to upgrade the Policy Broker machine. See Upgrading Web Protection Solutions for instructions.
2. Upgrade all *User directory and filtering* appliances. Each time the upgrade completes on an appliance, the appliance automatically restarts.
3. Upgrade all *Filtering only* appliances.
4. Use the version 8.4.x Forcepoint Security Installer to upgrade remaining off-appliance components. See Upgrading Web Protection Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance TRITON components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source* appliance is unavailable, is being replaced, or is being re-imaged, temporarily set a *User directory and filtering* or *Filtering only* appliance to be the *Full policy source*. To do this:

1. Create a full backup of the appliance in case changing the policy source fails.
2. On the secondary appliance, in the V Series manager, navigate to **Configuration > Web Security Components**.
3. For **Policy Source**, select **Full policy source**. Save the setting.
4. Upgrade this appliance to the version you want. The appliance automatically restarts when the upgrade finishes.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance. When the upgrade is done, the appliance automatically restarts.
2. On the previously upgraded secondary appliance, in the CLI enter **config** mode and change the policy mode:

   ```
   set mode <user|filter> --policy-source <policy_src_ip_addr>
   ```
3. Use the version 8.4.x Forcepoint Security Installer to upgrade remaining off-appliance components. See Upgrading Web Protection Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.4.x*, page 86.

Post-upgrade activities

Note

Product names have changed in v8.4.0. See *Product renaming*, page 89.

Depending on the solutions installed on your appliances, after upgrade perform the following:

In the CLI

For information about accessing the CLI, see *Configure and test access to the command-line interface (CLI)*, page 91.

- In the CLI, elevate to **config** mode and perform system checks and verify some configuration settings.
  - Check 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   : 8.4.0
    Mode                : Forcepoint Web Security
    Policy_mode         : Filtering only
    Policy_source_ip:   : 10.222.21.10
    ```
  - View the upgrade history.

    ```
    show upgrade --history
    ```
  - Check appliance status.

    ```
    show appliance status
    ```

```
show <module>
```

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

```
restart <module>
```

- Check 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 Forcepoint servers** in Forcepoint Appliances Getting Started Guide.

- 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 because most files that you want to save, or load, must be done with a filestore. Only system backup and log files are kept on the appliance.

  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 <name> --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
  ```

- Use the **set log archive** command to establish size and frequency values for archiving log files.

Additional tasks

- If your appliance includes Forcepoint Email Security, perform the Forcepoint Email Security 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 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 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 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.x

  - v8.0.1 Web Protection Release Notes
  - v8.0.0 Web Protection Release Notes
  - v8.0.1 TRITON 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

Upgrading V Series appliances from 8.1.x, v8.2.x, 8.3.0, or 8.4.0 to 8.5.3

Important

Forcepoint V Series appliances cannot be upgraded directly from v8.0.x to v8.5.3. To upgrade from v8.0.x to v8.5.3, 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 v8.5.3.

Related topics:

- *Product renaming*, page 89
- *Estimates of time to completion*, page 89
- *Rollback*, page 90
- *Summary of upgrade procedure*, page 90
- *Pre-upgrade activities*, page 91
- *Upgrade procedure*, page 93
- *Upgrading multiple V Series appliances*, page 95
- *Post-upgrade activities*, page 97

When upgrading your Forcepoint security products, always start with the product upgrade guide.

- Forcepoint Email Security: Upgrading email protection solutions
- Upgrade Instructions for Forcepoint Web Security
  (also applies to v7.8.4 Web Security Gateway/Anywhere)
- Upgrade Instructions for Forcepoint URL Filtering
  (also applies to v7.8.4 Web Security)

Important

Versions 8.3 and higher do not support dual-mode appliances—appliances that host *both* Forcepoint Email Security and Forcepoint Web Security, or Forcepoint Email Security and Forcepoint URL Filtering.

Before upgrading a dual-mode appliance, either the email or web module must be migrated to a new Forcepoint appliance. Migration of Forcepoint Email Security is recommended. To ease the email migration effort, special tools have been developed and a special procedure is recommended. For details, see Upgrading V-Series Dual-Mode Appliances.

The upgrade process applies to the following platforms and Forcepoint solutions:

- V5000 and V10000 appliances. For a list of supported models, see V Series appliances supported with v8.x.
- Forcepoint Web Security and Forcepoint URL Filtering, v8.1, v8.2, v8.3, and v8.4
- Forcepoint Email Security, v8.1, v8.2, v8.3, and v8.4

If you are upgrading TRITON APX (multiple solutions), see Upgrading more than one Forcepoint solution.

If you are upgrading Forcepoint DLP, see Upgrading to Forcepoint DLP.

Following is a list of upgrade paths to v8.5.3. You must upgrade to v8.1.0 (or higher) before upgrading to v8.5.3:

To upgrade from	To this version	Step One	Step Two	Step Three	Step Four
8.1.x, 8.2.x, 8.3.x, 8.4.x	8.5.3	Upgrade to 8.5.3			
8.0.x	8.5.3	Upgrade to 8.3.0	Upgrade to 8.5.3		
7.8.1, 7.8.2, 7.8.3	8.5.3	Upgrade to 7.8.4	Upgrade to 8.5.3		
7.7.x	8.5.3	Apply HF 90	Upgrade to 7.8.1	Upgrade to 7.8.4	Upgrade to 8.5.3

Important

If you are upgrading from version 8.0.x you must first upgrade to v8.3.0 and then upgrade to v8.5.0. To upgrade to v8.3.0, see *Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.3.x*, page 72. To upgrade from v8.3.0 to v8.5.0, follow the instruction in the V, X, & Virtual Appliance Upgrade Guide.

The upgrade is applied with a software patch and is initiated in the Appliance Manager on the **Administration > Patches/Hotfixes > Patches** page. The upgrade procedure ends with some tasks performed in the Forcepoint Appliances command-line interface (CLI). If you are unfamiliar with the CLI, see the CLI section of the v8.3.0 TRITON Appliances Release Notes.

Important

The upgrade process is designed for appliances 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.

Estimates of time to completion

Below are estimates of the time it takes for the v8.5.0 upgrade patch to run. The amount of time is variable, as indicated. As a best practice, allow the patch to run at least 90 minutes before aborting the install and contacting Forcepoint Technical Support.

Mode	Model	Elapsed time
Forcepoint Web Security	**V10000 G3, G4** **V5000 G3, G4** **V5000 G2R2**	30 - 45 minutes 65 - 85 minutes 70 - 90 minutes
URL Filtering	**V5000 G3, G4** **V5000 G2R2**	40 - 60 minutes 50 - 70 minutes
Forcepoint Email Security	**V10000 G3, G4** **V5000 G3, G4** **V5000 G2R2**	20 - 35 minutes 50 - 65 minutes 60 - 80 minutes

The following is a sample start-to-finish upgrade scenario for:

- One Forcepoint Web Security V10000 appliance

- Two Windows 2012 servers: one for the Forcepoint Security Manager, one for Web Log Server

Approximate total upgrade time for all upgrade tasks is 3 to 4 hours.

The download speed for each patch depends on your network environment and can vary significantly.

Activity breakout:

- 20 minutes to download the v8.5.3 appliance upgrade patch file, assuming the download speed is 1024 kilobytes per second.
- 40 to 60 minutes for the patch to perform the upgrade and for you to verify that the upgrade was successful.
- 15 minutes to download the version v8.5.3 Forcepoint Security Installer (for Windows components).
- 40 to 60 minutes to run the installer to upgrade the Forcepoint management server and the Log Server host.
- 5 minutes to restart the Windows servers and verify that the upgrade was successful.

Service disruption during upgrade

Appliance services are disrupted while the upgrade is applied to the appliance, continuing until the appliance completes its final restart.

Note

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

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 fully restored. In this case, off-appliance components may need to be restarted.

Summary of upgrade procedure

1. Perform the pre-upgrade activities.
2. Download the v8.5.3 Forcepoint Security Installer.
3. Download the appliance upgrade patch file.
4. If the appliance hosts Forcepoint Web Security or Forcepoint URL Filtering, upgrade the **Full policy source machine** (hosts Policy Broker/Policy Database). Note that all components on the machine are upgraded when Policy Broker/Policy Database are upgraded.
5. Apply the appliance upgrade patch.

6. Upgrade the Forcepoint management server (if not upgraded when Policy Broker/ Policy Database were upgraded), and other servers that host components.
7. Log on to the CLI and perform post-upgrade activities.

Pre-upgrade activities

Before applying the v8.5.3 patch, perform the following tasks and be aware of the following issues.

If you are 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 to v8.5.x web protection solutions and v8.5.0 Release Notes for Web Protection Solutions.
- For email protection solutions, see Upgrading email protection solutions and v8.5.0 Release Notes for Forcepoint Email Security.

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

At the end of the upgrade procedure you will need to log on to the v8.5 appliance CLI and perform a small number of checks.

The v8.5 appliance CLI is accessed in the same way as the V Series CLI. If you have not used the V Series CLI, or have not 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 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 have an integrated DELL Remote Access Controller (iDRAC). If you have never worked with the iDRAC, see **Using the iDRAC** in the Forcepoint Appliances Getting Started Guide.

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

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 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.

Back up appliance configuration and settings

Perform a **full appliance configuration** backup:

1. Log on to Appliance Manager and go to the **Administration > Backup Utility** page.
2. Under Perform Backup, select **Full Appliance Configuration** as the backup type.
3. Click **Run Backup Now**.
4. When the backup file appears in the **Local Backup Files** list, click the backup file name. When prompted, **save the backup file to an off-appliance location**.

Content Gateway logs

If the appliance hosts TRITON AP-WEB (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. Keep this record where you can easily retrieve it after the upgrade.

Administrator accounts

Make sure administrator accounts authenticated by a directory service have an email address specified in the directory service. In versions 7.8.1 and higher, an email address is required for each administrator account (except group accounts).

Upgrade procedure

Important

V Series appliance services are not available while the patch is being applied and until the appliance completes restarting. See *Estimates of time to completion*, page 89.

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

1. If you have multiple V Series appliances, read *Upgrading multiple V Series appliances*, page 95, **before** following this procedure.
2. If you are upgrading a Forcepoint Web Security or Forcepoint URL Filtering deployment and Policy Broker and Policy Database are installed on an off-appliance server, upgrade that machine now. Upon completion confirm that Policy Broker and Policy Database services are running. See Upgrading Web Protection Solutions.

Note that at the same time that Policy Broker and Policy Database are upgraded, all other TRITON components on the machine are upgraded.

Important

For the upgrade to complete successfully, the appliance must be able to communicate with the Policy Broker and Policy Database services.

3. 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 policy server instance. In the Web module of Forcepoint Security Manager, go to the **Settings > General > Policy Servers** page and unregister the instance.

4. If not already done, perform a full appliance backup and save the backup file to an off-appliance location.See *Back up appliance configuration and settings*, page 92.

5. Restart the appliance (in Appliance Manager: **Status** > **General** > **Restart Appliance**). This ensures that the appliance is in a clean state for the upgrade.

6. Download the upgrade patch.

   In the Appliance Manager go to the **Administration > Patches/Hotfixes > Patches** tab. The upgrade patch for version 8.5.3 should be listed in the **Table of available patches**. If it's not, click **Check for Patches**. The patch should be listed as available.

   Alternatively, the patch can be downloaded from forcepoint.com and uploaded to the appliance.

   a. Go to My Account and select the **Downloads** tab. Find your Forcepoint appliance model (for example, V10000) and click **8.5.0**.

   b. Click on **v8.5 V Series upgrade patch** and on the resulting page, click **Download**.

   c. Log on to the Appliance manager and navigate to **Administration > Patches /Hotfixes**.

   d. Click **Upload Patch Manually,** then **Browse,** and then select the upgrade file for version 8.5.3.

   e. Click **Upload** to initiate upload of the patch to the appliance. Depending on the speed of the network, upload can take 20 minutes or more. When the upload is complete the upgrade is listed in the **Available patches** list.

   Because local network speeds are usually faster than the Internet gateway, this is an efficient method when your deployment has many appliances. The upgrade patch is downloaded only once from the patch download server. Other appliances upload the patch from the local location.

7. Take all precautions to ensure that power to the appliance is not interrupted during the upgrade.

8. Click **Install** to apply the upgrade.

The patch performs several system checks to ensure that the appliance is ready for upgrade. The checks may take several minutes.

9. When you see that all pre-requisites have been met, you can continue to install the patch by clicking **Install Patch**.
10. Review the subscription agreement. Check **I accept this agreement** and **Continue**.
11. A confirmation message tells you that during the upgrade you are logged out of the Appliance manager and the appliance restarts. Click **OK** to begin the upgrade.

    While the upgrade is performed, services are **unavailable** to users.

> **Important**
>
> On rare occasions, these problems have been seen in appliances prior to v8.3.
>
> - Shortly after the install begins, the Appliance Manager page refreshes and displays the message **Patch 8.5.0 installed successfully**.
> - The upgrade progress bar stays at 0% for a long time.
>
> Should you experience either problem, exit the Appliance Manager and then log on again and restart the upgrade.

12. After the appliance restarts, perform *Post-upgrade activities*, page 13.
13. If you have multiple appliances, after identifying the Policy Broker and Policy Database machine and upgrading that machine, you can move on to upgrading the next appliance and subsequent appliances. See *Upgrading multiple V Series appliances*, page 95.
14. Upgrade all components that you haven't already upgraded and which run off the appliance. These may include Web and Email Log Server, transparent identification agents, and the Forcepoint Security Manager. If Policy Broker and Policy Server are on the same off-appliance server as the Forcepoint Security Manager, you should have already upgraded all components on that box.

    See Upgrading Web Protection Solutions and Upgrading Email Protection Solutions for instructions.

If the upgrade fails, contact Technical Support for assistance.

Upgrading multiple V Series appliances

> **Important**
>
> Dual-mode appliances are not supported by v8.3.x and higher.
>
> If you are upgrading a dual-mode appliance, use the special guide V Series Dual-mode Upgrade Guide.

When multiple V Series appliances are deployed in the same network, it is very important that they be upgraded in the prescribed order.

If the appliance is a Forcepoint Email Security appliance

Apply the upgrade patch to all Forcepoint Email Security appliances before upgrading the off-appliance components.

If the appliance includes a Web protection solution

Best practice for upgrade sequence if Full policy source is on a V Series appliance

1. Upgrade the *Full policy source* appliance.
2. Upgrade all *User directory and filtering* appliances.
3. Upgrade all *Filtering only* appliances.
4. After all appliances have been upgraded, upgrade off-box components.

Best practice for upgrade sequence if Full policy source is not on a V Series appliance

If you have multiple V Series appliances and the policy source (Policy Broker and Policy Server) is located off-appliance:

1. Make sure that the Policy Broker and Policy Server machine are upgraded to the version you want and that the services are running. Other components installed on the Policy Broker and Policy Server machine are upgraded at the same time. Use the version 8.4.x Forcepoint Security Installer to upgrade the Policy Broker machine. See Upgrading Web Protection Solutions for instructions.
2. Upgrade all *User directory and filtering* appliances. Each time the upgrade completes on an appliance, the appliance automatically restarts.
3. Upgrade all *Filtering only* appliances.
4. Use the version 8.4.x Forcepoint Security Installer to upgrade remaining off-appliance components. See Upgrading Web Protection Solutions for instructions.

If the Full policy source appliance is down or unavailable

Best practice is to upgrade the *Full policy source* appliance first, then the *User directory and filtering*, then *Filtering only* appliances, and finally the off-appliance components.

However, if your site must upgrade a *User directory and filtering* or *Filtering only* appliance before the *Full policy source* appliance, or if your *Full policy source* appliance is unavailable, is being replaced, or is being re-imaged, temporarily set a *User directory and filtering* or *Filtering only* appliance to be the *Full policy source*. To do this:

1. Create a full backup of the appliance in case changing the policy source fails.
2. On the secondary appliance, in the V Series manager, navigate to **Configuration > Web Security Components**.

3. For **Policy Source**, select **Full policy source**. Save the setting.
4. Upgrade this appliance to the version you want. The appliance automatically restarts when the upgrade finishes.

After the original *Full policy source* appliance has been upgraded, replaced, or re-imaged, change the upgraded temporary *Full policy source* machine to point to the original *Full policy source* again for its policy information. To do this:

1. Upgrade the primary appliance. When the upgrade is done, the appliance automatically restarts.
2. On the previously upgraded secondary appliance, in the CLI enter **config** mode and change the policy mode:

   ```
   set mode <user|filter> --policy-source <policy_src_ip_addr>
   ```
3. Use the version 8.5.3 Forcepoint Security Installer to upgrade remaining off-appliance components. See Upgrading Web Protection Solutions for instructions.

To see all upgrade instructions go to *Upgrading V Series appliances from v7.8.4, 8.0.x, 8.1.x, or v8.2.x to 8.4.x*, page 86.

Post-upgrade activities

Depending on the solutions installed on your appliances, after upgrade perform the following:

In the CLI

For information about accessing the CLI, see *Configure and test access to the command-line interface (CLI)*, page 91.

- In the CLI, elevate to **config** mode and perform system checks and verify some configuration settings.
  - Check 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   : 8.5.0
    Mode                : Forcepoint Web Security
    Policy_mode         : Filtering only
    Policy_source_ip:   : 10.222.21.10
    ```
  - View the upgrade history.

    ```
    show upgrade --history
    ```
  - Check appliance status.

    ```
    show appliance status
    ```

    ```
    show <module>
    ```

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

```
restart <module>
```

- Check 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 Forcepoint servers** in Forcepoint Appliances Getting Started Guide.

- 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 because most files that you want to save, or load, must be done with a filestore. Only system backup and log files are kept on the appliance.

  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 <name> --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
  ```

- Use the **set log archive** command to establish size and frequency values for archiving log files.

Additional tasks

- If your appliance includes Forcepoint Email Security, perform the Forcepoint Email Security 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 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 8.5.0

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

  Version 8.4.0

  - v8.4.0 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 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