Upgrading TRITON® APX Suite to v8.3

Upgrade Instructions | Web, Data, and Email Solutions | Version 8.3.x

This guide describes how to upgrade a TRITON system with multiple modules — web, email, and/or data—to v8.3.x. For information on upgrading systems that include stand-alone installations of data, email, or web protection solutions, refer to the Deployment and Installation Center in the Forcepoint Technical Library.

TRITON modules must be at least version 7.8.4 in order to upgrade to v8.3. For information on upgrading from earlier versions to version 7.8.4, see Upgrading TRITON Enterprise v7.7.x to v7.8.x.

Because TRITON AP-EMAIL includes data components, the upgrade procedure for combined web and email solutions is the same as the upgrade procedure for all TRITON modules.

To upgrade to v8.3, see the following sections:

- *Requirements for this version*, page 2
- *Before upgrading TRITON APX*, page 5
- *Upgrade sequence for TRITON Enterprise*, page 11
- *Upgrade procedure for TRITON Enterprise*, page 14

Perform the upgrade in the order described. This sequence is critical, because if you upgrade supplemental servers or agents before the management server, they stop communicating. If you upgrade the management server first, it continues communicating with the components until they are upgraded.

Important

TRITON APX v8.3 does not support dual-mode appliances. Dual-mode appliances host both TRITON AP-EMAIL and TRITON AP-WEB, or TRITON AP-EMAIL and Web Filter & Security.

If you are upgrading a dual-mode appliance, see Upgrading V-Series Dual Mode Appliances to v8.3.

Important

V-Series appliance users:

Some older V10000 and V5000 appliances are not supported with version 8.0.0 and higher.

See V-Series appliances supported with version 8.x.

Requirements for this version

The **TRITON management server** must be one of the following 64-bit machines:

- Windows Server 2008 Standard or Enterprise R2 SP1
- Windows Server 2012 Standard Edition
- Windows Server 2012 Standard or enterprise R2

It hosts TRITON Manager, which includes:

- The infrastructure uniting all management components
- A settings database for administrator account information and other shared data
- One or more management modules (Web, Data, Email), used to configure and report on a TRITON Advanced Protection solution.

Additional components may also reside on the TRITON management server.

Hardware requirements

The recommended hardware requirements for a TRITON management server vary depending on whether Microsoft SQL Server 2008 R2 Express (used only for evaluations or very small deployments) is installed on the machine.

Notes:

- TRITON AP-DATA allows for either local or remote installation of the forensics repository. If the repository is hosted remotely, deduct 90GB from the TRITON AP-DATA disk space requirements.
- The disk space recommendation allows for scaling as reporting data accumulates.
- If you install the product on a drive other than the main Windows drive (typically C), you still need at least 2GB free on the main drive to accommodate files extracted during installation.

With remote (standard or enterprise) reporting database

Management modules	Recommended	Minimum
Web module	4 CPU cores (2.5 GHz), 8 GB RAM, 150 GB Disk Space	4 CPU cores (2.5 GHz), 4 GB RAM, 70 GB Disk Space
Data module	8 CPU cores (2.5 GHz), 16 GB RAM, 400 GB Disk space	4 CPU cores (2.5 GHz), 12 GB RAM, 146 GB Disk Space
Web and Data modules	8 CPU cores (2.5 GHz), 20 GB RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 16 GB RAM, 146 GB Disk Space
Email and Data modules	8 CPU cores (2.5 GHz), 20 GB RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 16 GB RAM, 146 GB Disk Space
Web, Data, and Email modules	8 CPU cores (2.5 GHz), 24 GB RAM, 550 GB Disk Space	8 CPU cores (2.5 GHz), 20 GB RAM, 146 GB Disk Space

With local (express) reporting database

Management modules	Recommended	Minimum
Web module	4 CPU cores (2.5 GHz), 8 GB RAM, 240 GB Disk Space	4 CPU cores (2.5 GHz), 4 GB RAM, 100 GB Disk Space
Data module	8 CPU cores (2.5 GHz), 16 GB RAM, 400 GB Disk space	4 CPU cores (2.5 GHz), 12 GB RAM, 240 GB Disk Space
Web and Data modules	8 CPU cores (2.5 GHz), 20 GB RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 16 GB RAM, 240 GB Disk Space
Email and Data modules	8 CPU cores (2.5 GHz), 20 GB RAM, 400 GB Disk Space	4 CPU cores (2.5 GHz), 16 GB RAM, 240 GB Disk Space
Web, Data, and Email modules	8 CPU cores (2.5 GHz), 24 GB RAM, 600 GB Disk Space	8 CPU cores (2.5 GHz), 20 GB RAM, 240 GB Disk Space

TRITON Manager browser support

TRITON Manager is a web-based tool runs on a variety of popular browsers. For a list of browsers and versions that are supported, see the Certified Product Matrix on the Forcepoint website.

Although it is possible to launch TRITON Manager using non-supported browsers, you may not receive full functionality and proper display of the application.

Virtualization systems

- Windows Server 2008 R2 SP1 over Hyper-V 2008 R2
- Windows Server 2008 R2 SP1 and Windows Server 2012 over Hyper-V 2012
- Windows Server 2008 R2 SP1, Windows Server 2012 and Windows Server 2012 R2 over Hyper-V 2012 R2
- Windows Server 2008 R2 SP1 over VMware ESXi v5.x
- Windows Server 2008 R2 SP1, Windows Server 2012 and Windows Server 2012 R2 over VMware ESXi 6.x

Note that this support is for TRITON Manager only. Other components (used for enforcement, analysis, or reporting) may have additional requirements that are not supported by these virtualization environments.

Directory services for administrator authentication

If you allow users to log on to TRITON Manager using their network accounts, the following directory services can be used to authenticate administrator logons:

- Microsoft Active Directory
- Lotus Notes
- Generic LDAP directories
- Novell eDirectory
- Oracle Directory Services

Reporting database requirements

For all TRITON solutions, Microsoft SQL Server is used to host the reporting database.

- For evaluations and small deployments, the TRITON Unified Installer can be used to install Microsoft SQL Server 2008 R2 Express on the TRITON management server machine.

  Use only the version of SQL Server 2008 R2 Express included in the TRITON Unified Installer.
- Larger organizations are advised to use Microsoft SQL Server Standard, Business Intelligence, or Enterprise. These SQL Server editions cannot reside on the TRITON management server.

  SQL Server clustering may be used with all supported standard and enterprise versions of Microsoft SQL Server for failover or high availability.

The supported database engines for web, data, and email solutions in v8.3 are:

- SQL Server 2008

  All editions except Web, Express, and Compact; all service packs, 32- and 64-bit, but not IA64
- SQL Server 2008 R2 Express (installed by the TRITON Unified Installer)
- SQL Server 2008 R2

  All editions except Web and Compact; all service packs; not IA64

- SQL Server 2012 and SQL Server 2012 SP2

  Standard, Business Intelligence, and Enterprise editions
- SQL Server 2014 - Standard, Business Intelligence, and Enterprise editions
- SQL Server 2016 - Standard, Business Intelligence, and Enterprise editions

If you are using a remote database, the SQL Server logon ID and password for the SQL account must have a **sysadmin** role.

Before upgrading TRITON APX

This section lists the steps you must take to prepare for the TRITON upgrade.

- Read the relevant release notes.
  - TRITON AP-DATA v8.3.0 Release Notes
  - TRITON AP-EMAIL v8.3.0 Release Notes
  - TRITON Web Protection v8.3.0 Release Notes
  - TRITON APX Suite v8.3.0 Release Notes
  - TRITON Appliances v8.3.0 Release Notes
- Unless instructed otherwise by Forcepoint Technical Support, ensure your system is functional prior to upgrade.
- Ensure the time set on all appliances is synchronized prior to upgrade.
- Make sure the installation machine meets the *Requirements for this version*.
- If you are already using Virtual Machines (VMs) for TRITON Manager or for Microsoft SQL Server, take a snapshot of the VMs before you start a TRITON upgrade.
- If you have a remote database, ensure that the SQL account has a sysadmin role.
- Back up all of your TRITON components before starting the upgrade process. If you are upgrading from v7.x, see Backup and Restore FAQ for instructions. If you are upgrading from v8.x, see Backup and Restore FAQ v8.x.

  The Backup and Restore FAQ includes instructions for backing up all of the pieces that make up Web Security Gateway Anywhere (now TRITON AP-WEB with Hybrid Web module) on all platforms:
  - TRITON Infrastructure
  - Web Security components
  - Content Gateway
  - Data Security components

The upgrade process guides you through upgrading **all** components on the selected machine.

- You cannot choose which components to upgrade.
- Partial upgrades are not supported.

When upgrading the TRITON management server, if upgrade fails for any component **except** TRITON Infrastructure, you can either continue to upgrade the rest of the components or exit the process and modify component settings.

- You cannot continue if the infrastructure upgrade fails.
- You cannot roll back a component that was upgraded successfully.

After upgrade, your system has the same configuration as before the upgrade. Apart from the option to edit the TRITON AP-EMAIL database IP address if it has changed since installation, the upgrade process does not allow you to change your configuration or settings.

TRITON AP-WEB upgrade preparation

Before upgrading to TRITON AP-WEB v8.3:

1. Verify that third-party components work with Web Security Gateway or TRITON AP-WEB, including your database engine and directory service, are supported. See Requirements for web protection solutions.
2. Before upgrading Filtering Service, make sure that the Filtering Service machine and the TRITON management server have the same locale settings (language and character set).

   After the upgrade is complete, Filtering Service can be restarted with any locale settings.
3. If your product includes Web DLP features, before upgrading the management server, make sure your Web DLP components are ready for upgrade:
   a. Stop all discovery and fingerprinting tasks.
   b. Route all traffic away from the system.
   c. Ensure that your supplemental fingerprint repositories are fully synchronized with the primary repository.
   d. Make sure all settings are deployed successfully. Log onto the Data Security manager. If the **Deploy** button is highlighted, click it.
   e. If your organization was supplied with custom file types, change the name of the following files in the **policies_store\custom_policies\config_files** folder on the management server; otherwise they will be overwritten during upgrade.
      - Change **extractor.config.xml** to **custom_extractor.config.xml**.
      - Change **extractorlinux.config.xml** to **custom_extractorlinux.config.xml**.

      The filenames are case-sensitive.
   f. If custom policies were provided, submit a request for updated versions before proceeding.

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

> ⚠ **Warning**
>
> If database operations are active during upgrade, the web protection Log Database may be left in an inconsistent state, rendering it unusable.
>
> When this occurs, it can be difficult to fix.
>
> Make **sure** to stop Log Server and the database jobs, as described below, before upgrading the database.

   a. Back up your Web product’s reporting databases.

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

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

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

   Stop the Log Database jobs using these steps:

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

      ○ Log in to the Microsoft SQL Server Management Studio and expand **SQL Server Agent** > **Jobs** (in Object Explorer).

      ○ To disable all currently active Forcepoint SQL Server Agent jobs, right-click each of the following jobs and select **Disable**:

         Websense_ETL_Job_wslogdb70

         Websense_AMT_ETL_wslogdb70

         Websense_IBT_DRIVER_wslogdb70

         Websense_Trend_DRIVER_wslogdb70

         Websense_Maintenance_Job_wslogdb70

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

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

      ○ After upgrade, verify that the jobs have been to enabled.

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

      ○ Continue with step 9.

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

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

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

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

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

If your deployment includes TRITON appliances, also see the V-Series Appliance Upgrade Guide and X-Series Appliance Upgrade Guide.

Restart services before starting the upgrade

Most TRITON services must be running before the upgrade process begins. If any service (other than Log Server) is stopped, start it before initiating the upgrade.

The installer will stop and start TRITON services as part of the upgrade process. If the services have been running uninterrupted for several months, the installer may not be able to stop them before the upgrade process times out.

- To ensure the success of the upgrade, manually stop and start all the TRITON services **except Log Server** before beginning the upgrade. (Log Server should remain stopped, as described in *TRITON AP-WEB upgrade preparation*, page 6.)
  - *Windows*: Navigate to the **Web Security** directory (C:\Program Files (x86)\Websense\Web Security\, by default) and enter the following command:

    ```
    WebsenseAdmin restart
    ```
  - *Linux*: Navigate to the directory (/opt/Websense/, by default) and enter the following command:

    ```
    ./WebsenseAdmin restart
    ```
- On Windows machines, if you have configured the **Recovery** properties of any TRITON service to restart the service on failure, use the Windows Services dialog box to change this setting to **Take No Action** before upgrading.

Internet access during the upgrade process

When you upgrade, policy enforcement stops when TRITON services are stopped. Users have unrestricted access to the Internet until the TRITON services are restarted.

The Master Database is removed during the upgrade process. Filtering Service downloads a new Master Database after the upgrade is completed.

TRITON AP-DATA upgrade preparation

Before upgrading to TRITON AP-DATA v8.3:

- Stop all discovery and fingerprinting tasks.
- Route all traffic away from the system.
- Ensure that your supplemental fingerprint repositories are fully synchronized with the primary repository.
- Make sure all settings are deployed successfully. Log onto the Data Security manager. If the **Deploy** button is highlighted, click it.
- If Forcepoint supplied your organization with custom file types, change the name of 2 configuration files located in the \policies_store\custom_policies\config_files folder where Data Security is installed; otherwise they will be overwritten during upgrade.
  a. Change **extractor.config.xml** to **custom_extractor.config.xml**.
  b. Change **extractorlinux.config.xml** to **custom_extractorlinux.config.xml**.

  The filenames are case-sensitive.
- If you have custom policies provided by Forcepoint, submit a request for updated versions before proceeding.
- If you removed applications from AP-DATA's predefined endpoint application groups, make a list of the changes you made. Application groups are restored after upgrade, so you will need to remove the applications again. Custom user-defined groups are unaffected.

Note that the speed and success of your upgrade are affected by many factors, including:

- Number of online incidents.
- Size of the forensics folder.
- Number of policies or rules in use
- User directory import size
- Whether GPO restrictions are enforced on the server in domain membership scenarios

TRITON AP-EMAIL upgrade preparation

Before upgrading to TRITON AP-EMAIL v8.3:

- Redirect all email from the appliance being upgraded. You may lose cached messages if you do not put a redirect in place.

See the V-Series Appliance Upgrade Guide or X-Series Appliance Upgrade Guide for additional upgrade preparation steps.

Preparing to upgrade Content Gateway

Before upgrading Content Gateway, be aware of the following.

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

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

CPU	Quad-core running at 2.8 GHz or faster
Memory	6 GB minimum 8 GB recommended
Disk Space	2 disks: ● 100 GB for the operating system, Content Gateway, and temporary data.

	● Max 147 GB for caching If caching will not be used, this disk is not required. The caching disk: – Should be at least 2 GB and no more than 147 GB – Must be a raw disk, not a mounted file system – Must be dedicated – Must *not* be part of a software RAID – Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64 MB of write-through cache
Network Interfaces	2

- In addition, to support **transparent proxy** deployments:

Router	Must support WCCP v2. A Cisco router must run IOS 12.2 or later. The latest version is recommended. To support IPv6, WCCP v2.01 and Cisco router version 15.4(1)T or later are required. Client machines, the destination Web server, and Content Gateway must reside on different subnets.
—or—	
Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). Content Gateway must be Layer 2 adjacent to the switch. The switch must be able to rewrite the destination MAC address of frames traversing the switch. The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Upgrade sequence for TRITON Enterprise

If you are upgrading multiple TRITON components, upgrade them in the following order. For information on upgrading systems that include stand-alone installations of data, email, or web protection solutions, refer to the Deployment and Installation Center in the Forcepoint Technical Library.

> **Important**
>
> TRITON APX v8.3 does not support dual-mode V-Series appliances — appliances that host TRITON AP-EMAIL and TRITON AP-WEB, or TRITON AP-EMAIL and Web Filter & Security.
>
> If you are upgrading a dual-mode appliance, see Upgrading V-Series Dual Mode Appliances to v8.3.

1. The machine hosting Web **Policy Broker**
   - For a software installation, run the TRITON Unified Installer or Web Linux installer.
   - If Policy Broker is on the TRITON management server, you can upgrade the TRITON infrastructure and Web, Email, and Data management components at the same time as upgrading Policy Broker.
   - After Policy Broker is upgraded, Content Gateway stops managing Web traffic until it is upgraded.
2. Additional instances of Web **Policy Server**
   - May be software-based or on **user directory and filtering** appliances. For a software installation, run the TRITON Unified Installer. For an appliance, install the v8.3 upgrade patch.
   - If Policy Server is on an appliance, it *does not matter* whether the appliance is running in Web or Web and Email mode.
3. Additional instances of Web **Filtering Service** or **User Service**
   - Additional instances of Filtering Service may be software-based or on **filtering only** appliances.
   - If Filtering Service is on an appliance, the appliance security mode *does not matter*.
   - If you have filtering only appliances in your deployment, upgrade these appliances **after** the corresponding full policy source or user directory and filtering appliance has been upgraded. This is because appliances that have instances of Policy Server must be upgraded before you upgrade any components that point to it.
4. Web and Email **Log Server**

   If these components are on separate machines, it does not matter which is upgraded first.

> **Important**
>
> Make sure that no Email Log Database or Web Log Database jobs are running while the Log Server instances are being upgraded.

5. **TRITON management server** (if not already upgraded as part of an earlier step)
   - Whenever possible, upgrade the management server before any other TRITON AP-DATA components. This ensures that TRITON AP-DATA policy engines (and thus analysis) continue to function until they are upgraded themselves.

     Note that you cannot deploy new policies to the policy engines until they are upgraded to the same version as the management server.
   - If you need to upgrade a TRITON AP-DATA policy engine before upgrading the TRITON management server—because the policy engine resides on a full policy source appliance—detection of fingerprinted content might not work on the appliance until the management server is upgraded.

     The TRITON AP-DATA policy engine embedded in Content Gateway and TRITON AP-EMAIL continues to monitor the old Web and Email DLP policies and block/permit accordingly.
6. Upgrade all other appliances in your network. This can be done in any order, and can be completed in parallel.
   - If you have deployed Email Security Gateway or TRITON AP-EMAIL in cluster mode, ensure you upgrade the primary appliance before any secondary appliances. You do not need to release the appliances from the cluster in order to perform the upgrade.
   - The Email MTA continues to function after the management server upgrade, but the logs are cached on the appliance until TRITON AP-EMAIL is upgraded as well. For best practice, redirect email traffic to another MTA as cached messages may be lost otherwise.
7. Upgrade all other **Web** and **Data** components. This can be done in parallel. For example:
   - Network Agents
   - Transparent user identification agents
   - Remote Filtering Server
   - Data Security secondary servers
   - Data Security components on ISA and TMG servers
   - Software-based installations of Content Gateway

Upgrade procedure for TRITON Enterprise

This procedure covers the steps required to upgrade either the whole of TRITON Enterprise or a Web and Email solution. (Note that Email Security Gateway and Gateway Anywhere, and TRITON AP-EMAIL, always include Data components.)

> **Important**
>
> TRITON APX v8.3 does not support dual-mode V-Series appliances — appliances that host TRITON AP-EMAIL and TRITON AP-WEB, or TRITON AP-EMAIL and Web Filter & Security.
>
> If you are upgrading a dual-mode appliance, see Upgrading V-Series Dual Mode Appliances to v8.3.

- *Step 1: Upgrade the Policy Broker machine*, page 14
- *Step 2: Upgrade additional Policy Server machines*, page 16
- *Step 3: Upgrade additional Filtering Service and User Service machines*, page 18
- *Step 4: Upgrade Log Servers*, page 19
- *Step 5: Upgrade the TRITON Management Server*, page 19
- *Step 6: Upgrade appliances*, page 24
- *Step 7: Upgrade additional components*, page 24

Step 1: Upgrade the Policy Broker machine

You must upgrade the machine that hosts **Policy Broker** first, regardless of which other components on are on the machine. Policy Broker may reside on:

- A **full policy source** appliance
- A Windows Server 2008 R2 SP1, 2012, or 2012 R2 machine.
- A RHEL 6.5 or later, 7.0, 7.1, or 7.2 machine.

Any other components on the Policy Broker machine are upgraded along with Policy Broker.

If your configuration includes a primary Policy Broker and one or more replica Policy Brokers, you **must** upgrade the primary Policy Broker first.

Upgrade replica Policy Brokers after the primary has been upgraded and before attempting to upgrade any Policy Servers associated with the replicas. If Policy Server is installed on the Policy Broker machine, it is upgraded at the same time.

If Policy Broker resides on the TRITON management server, running the TRITON Unified Installer also upgrades the TRITON infrastructure and web, data, and email management components as described in *Step 5: Upgrade the TRITON Management Server*, page 19. Ensure you also follow the steps in *Post-upgrade steps*, page 24, to configure the TRITON management server.

The instructions in this section cover the upgrade of a Windows machine. For instructions on upgrading an appliance or a Linux machine, see the Upgrade Instructions for TRITON AP-WEB.

1. Make sure that no administrators are logged on to TRITON Manager.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

> **Important**
>
> If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

> **Warning**
>
> Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of My Account to download the TRITON Unified Installer.
   - The installer file is **TRITON83xSetup.exe**.
   - The installer and its extracted files require approximately 7 GB of disk space.
5. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web Security components from an earlier version and asks whether you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. Accept the subscription agreement. When you click **Next**, a *Stopping All Services* progress message appears. Wait for services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.

10. On the **Pre-Upgrade Summary** screen, review the list of components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized, and then the upgrade begins.

    If Policy Broker resides on the TRITON management server, or on the same machine as Log Server, the upgrade process checks for a required version of Microsoft SQL Server Native Client and related tools and installs them, if necessary.

11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

> **Important**
>
> The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Step 2: Upgrade additional Policy Server machines

The central Policy Server resides on the same machine as Policy Broker, and was automatically upgraded in the previous section.

If you have additional Policy Server instances, upgrade them next, regardless of what other services reside on the machines. Policy Server may reside on:

- TRITON **user directory and filtering** appliances
- Windows Server 2008 R2 SP1, 2012, or 2012 R2 machines
- RHEL 6.5 and later, 7.0, 7.1, or 7.2 machines

The instructions in this section cover the upgrade of a Windows machine. For instructions on upgrading an appliance or a Linux machine, see the Upgrade Instructions for TRITON AP-WEB.

1. Make sure that no administrators are logged on to TRITON Manager.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

> **Important**
>
> If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

3. Close all applications and stop any antivirus software.

Warning

Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of My Account to download the TRITON Unified Installer.
   - The installer file is **TRITON83xSetup.exe**.
   - The installer and its extracted files require approximately 7 GB of disk space.
   - Verify that the MD5 value of the downloaded file matches the value shown on the download page.
5. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
6. The installer detects Web components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
8. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.
9. Accept the subscription agreement. When you click **Next**, a *Stopping All Services* progress message appears. Wait for TRITON services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the TRITON services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.
10. On the **Pre-Upgrade Summary** screen, review the list of components that will be upgraded, and then click **Next**.

    Critical files are backed up and install properties initialized. And then the **Installing Forcepoint** screen appears.
11. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
12. Reboot the machine.

Important

The machine must be rebooted to complete the upgrade process.

13. If you stopped your antivirus software, restart it.

Step 3: Upgrade additional Filtering Service and User Service machines

If you have additional Filtering Service or User Service instances, upgrade them next, regardless of what other services reside on the machines. Filtering Service and User Service may reside on:

- Windows Server 2008 R2 SP1, 2012, or 2012 R2 machines
- RHEL 6.5 or later, 7.0, 7.1, or 7.2 machines

Filtering Service and Network Agent may also reside on **filtering only** appliances.

The instructions in this section cover the upgrade of a Windows machine. For instructions on upgrading an appliance or a Linux machine, see Upgrade Instructions for TRITON AP-WEB.

Make sure that no administrators are logged on to TRITON Manager.

1. Log on to the installation machine with an account having **domain** and **local** administrator privileges.

   Important

   If you are upgrading Log Server on this machine and it uses a Windows trusted connection to access the Log Database, you must log on to this machine using the same trusted account.

2. Close all applications and stop any antivirus software.

   Warning

   Be sure to close the Windows Event Viewer, or the upgrade may fail.

3. Go to the **Downloads** tab of My Account to download the TRITON Unified Installer.
   - The installer file is **TRITON83xSetup.exe**.
   - The installer and its extracted files require approximately 7 GB of disk space.
4. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears, as files are extracted.
5. The installer detects Web Security components from an earlier version and asks how you want to proceed.

   Click **OK**.
6. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens mentioned in the remaining steps.
7. On the **Upgrade** screen, select **Start the upgrade**, then click **Next**.

8. Accept the subscription agreement.When you click **Next**, a *Stopping All Services* progress message appears. Wait for TRITON services to be stopped.

   The **Pre-Upgrade Summary** screen appears when the services have been stopped.

   In some cases, the installer may be unable to stop the TRITON services. If this occurs, you are prompted to stop them manually (you do not need to exit the installer to do this). Use the Windows Services tool to stop the services, then return to the installer.

9. On the **Pre-Upgrade Summary** screen, review the list of components that will be upgraded, and then click **Next**.

   Critical files are backed up and install properties initialized. And then the **Installing Forcepoint** screen appears.

10. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
11. Reboot the machine.

> **Important**
>
> The machine must be rebooted to complete the upgrade process.

12. If you stopped your antivirus software, restart it.

Step 4: Upgrade Log Servers

Upgrade the Web and Email Log Server machines, if they have not already been upgraded with other components. Any other services on the machine are also upgraded in the correct order.

For information on Web Security Log Server, see Upgrade Instructions for TRITON AP-WEB.

For information on Email Security Log Server, see Upgrade Instructions for TRITON AP-EMAIL.

Step 5: Upgrade the TRITON Management Server

If you have not already upgraded the TRITON management server in the course of upgrading another component, use the following steps to upgrade the management server machine.

1. Make sure that no administrators are logged on to the TRITON console.
2. Log on to the installation machine with an account having **domain** and **local** administrator privileges.
3. Close all applications and stop any antivirus software.

Warning

Be sure to close the Windows Event Viewer, or the upgrade may fail.

4. Go to the **Downloads** tab of My Account to download the TRITON Unified Installer.
   - The installer file is **TRITON83xSetup.exe**.
   - The installer and its extracted files require approximately 7 GB of disk space.
5. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. A progress dialog box appears as files are extracted.
6. The installer detects components from an earlier version and asks how you want to proceed.

   Click **OK**.
7. On the installer **Introduction** screen, click **Next**.

   Note the **Installer Dashboard** remains on-screen, behind the installer screens that appear in subsequent stages of the upgrade.
8. Follow the screens in the upgrade wizard as described in the sections below:
   - *TRITON Infrastructure*
   - *TRITON Infrastructure*
   - *TRITON AP-WEB*
   - *TRITON AP-DATA*
   - *TRITON AP-EMAIL*
9. Wait for the **Upgrade Complete** screen to appear. Click **Done** to exit the installer.
10. Reboot the machine.

Important

You may be prompted to restart the machine after each component is upgraded. This is optional. You may prefer to restart the machine once after all components are upgraded.

11. If you stopped your antivirus software, restart it.
12. Follow the instructions in *Post-upgrade steps*, page 24.

TRITON Infrastructure

The TRITON infrastructure provides basic framework for all of the management components that make up TRITON Manager. This framework includes a central settings database that stores shared configuration (like administrator directory and account information) for all management modules, as well as other internal shared services.

The infrastructure upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	Welcomes you to the installation and upgrade wizard. 1. Click **Next** to begin the upgrade process. The system checks disk space requirements. 2. When prompted, click **Next** to launch the installation wizard.
Pre-Installation Summary	Shows: ● The destination folder for the installation files. ● The name of the SQL Server machine and the user name of an authorized database administrator. ● The IP address of the TRITON management server and administrator credentials. Click **Next** to accept the properties.
Installation	Shows upgrade progress. The system stops processes, copies new files, updates component registration, removes unused files, and more. A popup message appears at this stage, warning that you must also upgrade all modules. This popup may be hidden behind the main installer window. If your installation appears to freeze, locate the hidden popup by moving the main installer window, and click **OK** to proceed with the installation.
Summary	When module upgrade is complete, summarizes your system settings, including: ● The destination folder for the installation files. ● The name of the SQL Server machine and the user name of an authorized database administrator. ● The IP address of the TRITON management server and administrator credentials. Click **Finish** to complete the upgrade for this module.

TRITON AP-WEB

The web upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	Welcomes you to the upgrade wizard. Click **Next** to continue.
Upgrade	Select **Start the upgrade**, then click **Next**. 1. Accept the subscription agreement and click **Next**. 2. The installer proceeds to stop all TRITON services.
Pre-Upgrade Summary	Provides a list of components that will be upgraded. Click **Next** to start the upgrade. The installer backs up critical files.

Wizard Screen	Fields
Installing	Shows installation progress. When complete, the installer configures your software. This can take up to 10 minutes.
Upgrade Complete	You're notified when installation of this module is complete. Click **Done** to exit the installer.

TRITON AP-DATA

Before running the data upgrade wizard, the installer validates system requirements to ensure your upgrade will be successful.

The pre-upgrade check validates hardware requirements, credentials for your SQL management database, endpoint security certificates, manager configuration, administrator upgrade permissions, and your database structure. As it proceeds, it reports whether a step succeeded or failed, or it gives you a warning.

If there is a failure, the upgrade stops. For details, see **\AP-DATA-PreUpgradeTests.log** in the directory where you installed TRITON AP-DATA.

If there are only warnings, you have the option to proceed with the upgrade or stop it. If you continue, your system may behave unexpectedly, but this will not have a critical impact.

If the pre-upgrade check succeeds or if you proceed with warnings, the TRITON AP-DATA wizard is launched, followed by wizards for each installed component.

The data upgrade wizard contains the following screens:

Wizard Screen	Fields
Welcome	This screen welcomes you to the installation and upgrade wizard. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
Installation Confirmation	Verify your system settings and click **Install** to continue the upgrade.

Wizard Screen	Fields
Installation	This screen shows the progress of the installation. The system stops processes, checks ports, copies new files, updates component registration, removes unused files, and more. In certain circumstances, you may receive an internal SQL error. If you do, do not click OK until you have resolved the issue with Forcepoint Technical Support. If you continue prematurely, you can cause problems with your reporting database.
Summary	When installation of this module is complete, this screen summarizes your system settings. 1. Click **Done** and you're prompted to update your predefined policies and content classifiers. 2. Click **OK** to install the updates. You're shown the status of the updates, the items being updated, and details such as how many policies are updated, deleted, or added. 3. Click **Close** when the updates are complete.

TRITON AP-EMAIL

The email upgrade wizard contains the following screens.

Wizard Screen	Fields
Introduction	This screen welcomes you to the upgrade wizard. Click **Next** to continue.
Select Components	This screen shows the components that will be upgraded (those that are currently installed). Click **Next** to continue.
Configuration	This page shows the IP address of the database engine configured to manage the Email Log Database and the logon type. If you have changed the database since your previous installation, modify the settings here.
Pre-Installation Summary	This screen shows: ● The components to be installed ● The pre-existing and new version numbers ● The destination folder for the installation files ● The required and available disk space Click **Install** to begin the upgrade.
Installation	This screen shows that the installation is progressing. The management component is upgraded on the TRITON management server. The Email Log Server is upgraded on machines where it is found. When complete, the installer configures your TRITON AP-EMAIL software. This can take up to 10 minutes.
Summary	You're notified when installation of this module is complete. Click **Done** to exit the installer.

Post-upgrade steps

Once the TRITON management server upgrade is complete:

1. Restart the management server.
2. Log onto TRITON Manager (https://<IP_address_or_hostname>:9443/triton/).
3. Select the Data module.
4. Follow the prompts that appear for updating data loss protection policies and classifiers.

   Depending on the number of policies you have, this can take up to an hour. During this time, do not restart the server or any of the services.
5. If you removed applications from TRITON AP-DATA's predefined endpoint application groups prior to upgrade, navigate to **Main** > **Resources** > **Endpoint Application Groups** after logging on and remove them again. The upgrade process restored these to their original state.
6. Click **Deploy**.
7. Select the Email module and navigate to the **Settings** > **General** > **Database Downloads** page. Click **Update Now** to perform an immediate database download update.
8. If you want to install management components for the TRITON AP-DATA Email Gateway for Microsoft Office 365 (this cannot exist on the same machine as TRITON AP-EMAIL), run the installer a second time and choose **Modify**. On the Modify screen, select **TRITON AP-EMAIL** and then follow the wizard. (See the TRITON AP-DATA Installation Guide for instructions.) Note that a VM image must be installed in the Microsoft Azure cloud as well.

Step 6: Upgrade appliances

Upgrade all appliances that have not been upgraded in the above steps. This can be done in any order, and can be completed in parallel.

If you have deployed TRITON AP-EMAIL in cluster mode, ensure that you upgrade the primary appliance before any secondary appliances. You do not need to release the appliances from the cluster in order to perform the upgrade.

For more information, see the V-Series Appliance Upgrade Guide and X-Series Appliance Upgrade Guide.

Step 7: Upgrade additional components

Once you have completed the above steps, you can upgrade any additional software components and client components:

1. Upgrade any additional software instances of Network Agent and Content Gateway. If these components run on TRITON appliances, this step has already been done.

2. Upgrade any additional Web server components, including transparent identification agents and Remote Filtering Server, that may be running on other machines.
3. Upgrade supplemental servers, protectors, mobile agents, and other TRITON AP-DATA agents.
4. Upgrade client components, including the logon application (LogonApp.exe), Remote Filtering Client, TRITON AP-ENDPOINT Web and TRITON AP-ENDPOINT DLP.

These actions can be done in parallel. For more information, see the following upgrade guides:

- Upgrade Instructions for TRITON AP-WEB
- Upgrade Instructions for TRITON AP-DATA