FORCEPOINT
POWERED BY Raytheon

Upgrading to TRITON AP-DATA v8.3.x

Forcepoint™ TRITON® AP-DATA Gateway and Discover

v8.3.x

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin TX 78759

Published 2017

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint LLC makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint LLC shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Contents

1 Upgrading to TRITON AP-DATA v8.3

Data Security must be at least version 7.8.4 to upgrade to TRITON AP-DATA v8.3.x. If you have an earlier version, there are interim steps to perform. These are shown in the table below.

Your current version	Step 1	Step 2	Step 3	Step 4
7.6.x	Upgrade to 7.7.2	Upgrade to 7.8.4	Upgrade to 8.3.x	
7.7.x	Upgrade to 7.8.4	Upgrade to 8.3.x		
7.8.1 - 7.8.3	Upgrade to 7.8.4	Upgrade to 8.3.x		
7.8.4 - 8.2.x	Upgrade to 8.3.x			

Step-by-step guides to upgrading early Data Security installation can be found here:

- Upgrading to TRITON AP-DATA from v7.7.x - 7.8.x
- Upgrading to TRITON AP-DATA from v7.6.x - 7.8.x
- Migrating to TRITON AP-DATA from v7.5.x - 7.8.x

This guide describes how to upgrade stand-alone installations of Data Security or TRITON AP-DATA to TRITON AP-DATA v8.3.x:

1. *Upgrade the TRITON management server*
2. *Upgrade supplemental servers and agents*
3. *Upgrade protectors and mobile agents*
4. *Deploy settings*
5. *Upgrade endpoints*

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.

For information on upgrading systems that include Web Security and/or Email Security as well as Data Security, refer to the Deployment and Installation Center in the Forcepoint Technical Library.

For high-level flow charts of the Data Security upgrade process, see:

- Manager upgrade
- Servers and agents upgrade
- Protector/mobile agent upgrade
- Endpoint upgrade

Upgrade the TRITON management server

To ensure a successful upgrade, do the following before you begin.

- Unless instructed otherwise by Forcepoint Technical Support, ensure your system is functional prior to upgrade.
- Make sure your base version is 7.8.4 or later.
- Perform a full backup of your system before upgrading.
  a. Use the TRITON backup utility to back up your TRITON Settings information (administrator accounts, for example).
     - On the TRITON management server machine, go to **Start > Administrative Tools > Task Scheduler**, then select **Task Scheduler Library**.
     - If the Triton Backup task is disabled, right-click the task and select **Enable**.
     - Right-click the **Websense TRITON AP-DATA Backup** task and select **Run**.

  b. Back up Data Security software as described in How do I back up and restore Data Security software?
- 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

Upgrade steps

You upgrade your TRITON management server using the TRITON installation package, **TRITON83*x*Setup.exe**, where *x* is the version number. This is the same executable used for scratch installations.

1. Obtain the installer from My Account on the Forcepoint website.
2. Select **TRITON AP-DATA**, **version** (8.3), and **operating system** (Windows), then click **download** next to the installer description.
3. Launch the installer.

The installation package detects that earlier versions of the product are installed, and automatically starts a series of wizards.

The TRITON AP-DATA wizard upgrades all necessary components on the TRITON management server.

After upgrade, your system has the same configuration as before the upgrade. The upgrade process does not allow you to change your configuration or settings.

✓ **Note**

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.

TRITON Infrastructure

The TRITON infrastructure provides basic framework for all of the components that make up TRITON management server. 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, so if your installation appears to freeze, locate the hidden popup by moving the main installer window, and click **OK** to proceed with the installation. In addition, if you see a Data Task Scheduler window, you have the option to stop the Work Scheduler service in Windows services, or continue running the installer and reboot at the end. Reboot is the recommended approach.
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. Restart the computer if prompted.

TRITON AP-DATA

Before running the TRITON AP-DATA 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 TRITON AP-DATA upgrade wizard contains the following screens.

Wizard Screen	Fields
Welcome	This screen welcomes you to the installation and upgrade wizard for TRITON AP-DATA. The system checks the disk space on the machine. When prompted, click **Next** to launch the installation wizard.
Configuration	Step through the screens you configured on initial install, including Fingerprinting Database, Temporary File Location, and Local Administrator. Click **Next** on each to retain your settings.
Installation Confirmation	Review the settings on the Installation Confirmation screen and click **Install** to continue the upgrade.
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. Restart the computer if prompted.

Post-upgrade

1. Once you are done, you must deploy changes to finish the upgrade. See *Deploy settings*, page 9, for instructions.

   For best practice, finish upgrading all other TRITON AP-DATA components, then you can deploy changes once.

   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.
2. If you upgraded from v8.0.1 to v8.3, re-run any machine learning scans you have. Select **Content Classifiers > Machine Learning**, then select the classifier of interest and click **Start** from the menu bar. The system needs to re-learn from your positive and negative examples after upgrade.
3. If you want to install management components for the Email Gateway for Microsoft Office 365, 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.

Upgrade supplemental servers and agents

Complete these steps to upgrade a supplemental TRITON AP-DATA server or stand-alone agents to v8.3.x.

1. To upgrade a supplemental server or agent, launch the installer, **TRITON83*x*Setup.exe**, where *x* is the version number. The software is detected, and the upgrade wizard appears.
2. Click **Next** until you complete the wizard.

   Any v7.8.4 and later Data Security and TRITON AP-DATA components found on this machine are upgraded.
3. Once you are done, you must deploy changes to finish the upgrade. See *Deploy settings*, page 9 for instructions. For best practice, finish upgrading all other TRITON AP-DATA components, then you can deploy changes once.
4. It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

   When you upgrade a Data Security server it takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in:

   - Potential false positives and negatives.

- File-system discovery starts but immediately indicates "completed with errors”.

Note

Version 8.3 of TRITON AP-DATA Email Gateway for Microsoft Office 365 is for fresh installations only, not upgrades.

It will be available in the Azure Marketplace in early Q1-2017, and it will support the new appliance CLI for user administration of the virtual appliance.

TRITON AP-DATA v8.3 does not support older TRITON AP-DATA Email Gateways versions.

Upgrade protectors and mobile agents

Version 8.3 of the protector includes CentOS 7. You can upgrade protectors from v8.2.5 to v8.3 but you cannot upgrade from earlier versions because they are built on Cent OS 5.

If you have a version prior to 8.2.5, you must re-image the protector from scratch to use v8.3.

The protector and mobile agent are forward compatible, so you can retain your existing installation and still take advantage of v8.3.x management, analytic, and endpoint features.

Important

If you are upgrading your protector to new hardware, be sure to keep the original IP address/host name if you want to retain settings and information from the original machine.

If you assign a new IP, the protector’s settings are cleared to default when it registers with the management server. In this case, you should manually delete the protector with the original IP address from the system modules page of the Data Security manager.

1. Backup any customizations you have made, because the system will be wiped. This includes things like changes to the postfix configuration (/etc/postfix), network interface settings, and security certificates.

   Management configuration, such as policy and agent settings, are recovered when you deploy the new module.
2. Install the protector/mobile agent software as described in the TRITON AP-DATA Installation Guide: Protector or Mobile Agent.
3. Restore any customizations you require.

4. It is strongly recommended you wait 30 minutes before routing traffic though the new system. It takes time for it to download the information necessary for resolving source and destination resources such as people, computers, and printers. Routing traffic through the system before this is complete may result in false positives and negatives.

Upgrading the analytics engine

To upgrade the analytics engine from v8.2.5 to v8.3:

1. To download the analytics engine installer, **AnalyticsEngine83**, use the My Account link to log in to support.forcepoint.com, then select the Downloads page. The installer is under Forcepoint TRITON AP-DATA v8.3.
2. Log in as root and make sure the installation file is in your current working directory and has execution privileges. If you receive a “Permission denied” error, run the following command:

   ```
   chmod +x AnalyticsEngine83
   ```
3. To run the installer, enter:

   ```
   ./AnalyticsEngine83
   ```

   The installer recognizes that you have the module analytics engine and steps you through the upgrade process.

   If you receive an error message about missing packages, follow the message instructions to install the required packages using yum.

   After installing the required packages, run the **./AnalyticsEngine83** command again.

Upgrading Email Gateway for Microsoft Office 365

Because of a new appliance architecture, you must do fresh install and manual re-configuration to use Email Gateway for Office 365 v8.3. You cannot upgrade from an earlier version.

A step-by-step guide to installing TRITON AP-DATA can be found here:

- Installing TRITON AP-DATA v8.3.x

Before you begin, open Windows Control Panel and verify that the “Current language for non-Unicode programs” in the Administrative tab of the Region and Language settings is set to English. After the installation, you can change it back to the original language.

Deploy settings

Once you've upgraded all TRITON AP-DATA servers, agents, and appliances, you must deploy your changes in the TRITON Manager. Endpoints do not require a separate deploy step in the manager.

1. Log onto the TRITON console as the service account (https://<IP_address_or_hostname>:9443/triton/).
2. Select the Data tab.
3. You are prompted to update your policies. Follow the prompts. Forcepoint research teams stay abreast of regulations across many industries and you should keep your policies and classifiers up-to-date. 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.
4. Click **Deploy**.

Upgrade endpoints

Although this endpoint is v8.3, it can be used in conjunction with Forcepoint products that are v7.8.4 and later. You do not need to uninstall earlier endpoint versions before installing v8.3.

To upgrade your existing on-premises version of the endpoint:

1. Make sure you have a v7.8.4 or later TRITON management server installed and functioning.
2. Make a backup copy of the Endpoint Package Builder executable file, **WebsenseEndpointPackageBuilder.exe,** found in one of the following locations:
   - For TRITON AP-ENDPOINT DLP: C:\Program Files (x86)\Websense\Data Security\client
   - For TRITON AP-ENDPOINT Web and combined endpoint solutions: C:\Program Files (x86)\Websense\Web Security\DTFAgent\RemoteFilteringAgentPack.
3. Download **EndpointPackage830_*nnnn*.zip**, from My Account and unzip it into the same folder. Four files are placed in the directory: **WebsenseEndpointPackageBuilder.exe**, **WebsenseEPClassifier.pkg.zip**, **EPA.msi**, and **EPA64.msi**.
   - The **exe** file is for building the Web and/or DLP software package to install on your endpoint client machines.
   - The **zip** file is a DLP endpoint classifier exclusively for Mac endpoints running TRITON AP-ENDPOINT DLP.

     Sites that are not running DLP on Mac can ignore the **WebsenseEPClassifier.pkg.zip**.file.
   - The **EPA.msi** file is the endpoint classifier for Win32 endpoints.

Sites that are not running DLP on Win32 machines can ignore the **EPA.msi** file.

- The **EPA64.msi** file is the endpoint classifier for Win64 endpoints.

  Sites that are not running DLP on Win 64 machines can ignore the **EPA64.msi** file.

4. If you have Mac endpoints running TRITON AP-ENDPOINT DLP:
   a. Back up the file **WebsenseEPClassifier.pkg.zip** in the following folder: C:\Program Files (x86)\Websense\Data Security\client\OS X.
   b. Copy the new **WebsenseEPClassifier.pkg.zip** from the folder in step 3 and place it into the \OS X folder.

      You do not need to unzip this file.
5. If you have Win32 endpoints running TRITON AP-ENDPOINT DLP:
   a. Back up the file **EPA.msi** in the following folder:

      C:\Program Files (x86)\Websense\Data Security\client.
   b. Copy the new **EPA.msi** from the folder in step 2 and place it into

      C:\Program Files (x86)\Websense\Data Security\client.
6. If you have Win64 endpoints running TRITON AP-ENDPOINT DLP:
   a. Back up the file **EPA64.msi** in the following folder:

      C:\Program Files (x86)\Websense\Data Security\client.
   b. Copy the new **EPA64.msi** from the folder in step 2 and place it into

      C:\Program Files (x86)\Websense\Data Security\client.
7. Run **WebsenseEndpointPackageBuilder.exe** to generate a new endpoint client installation package.
8. Deploy the v8.3 installation package to each endpoint client using one of the methods described in the Installation and Deployment Guide for Endpoint Solutions.
9. Restart the endpoint client machine after installation is complete.

Post endpoint upgrade

The system provides both name and serial number for each endpoint device, as in “SanDisk Cruzer Blade; 4C530103131102119495”.

An easy way to maintain compatibility with previous releases is to add an asterisk (*) to the end of each device name that you have listed in the TRITON Manager. For example, change “SanDisk Cruzer Blade” to “SanDisk Cruzer Blade*”.

If you do not, rules related to the existing endpoint devices may not monitor or enforce the removable media channel as expected. Only exact matches generate an incident.