FORCEPOINT
POWERED BY Raytheon

Upgrading to TRITON AP-DATA v8.2.x

Forcepoint™ TRITON® AP-DATA Gateway and Discover

v8.2.x

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

Published 2016

Trademarks

Contents

Chapter 1 **Upgrading to TRITON AP-DATA v8.2 . . . . . 1**

Upgrade the TRITON management server. 2

Preparing for upgrade 2

Upgrade steps 3

Upgrade supplemental servers and standalone agents 6

Upgrade protectors and mobile agents 6

Deploy settings 7

Upgrade endpoints 8

1 Upgrading to TRITON AP-DATA v8.2

Data Security must be at least version 7.8.4 to upgrade to TRITON AP-DATA v8.2. 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
7.5.x	Migrate to 7.6.0	Upgrade to 7.7.2	Upgrade to 7.8.4	Upgrade to 8.2
7.6.x	Upgrade to 7.7.2	Upgrade to 7.8.4	Upgrade to 8.2	
7.7.x	Upgrade to 7.8.4	Upgrade to 8.2		
7.8.1 - 7.8.3	Upgrade to 7.8.4	Upgrade to 8.2		
7.8.4	Upgrade directly to 8.2			
8.0.x	Upgrade directly to 8.2			
8.1.x	Upgrade directly to 8.2			

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 v7.8.4, 8.0.x, or 8.1.x to TRITON AP-DATA v8.2:

1. *Upgrade the TRITON management server*
2. *Upgrade supplemental servers and standalone agents*
3. *Upgrade protectors and mobile agents*
4. *Upgrade Email Gateway for Office 365 virtual machines*
5. *Deploy settings*
6. *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, 8.0.x, or 8.1.x.
- 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 Triton 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, **TRITON82*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** (8.2), 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 8, for instructions.

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

   If you removed applications from 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 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 standalone agents

Complete these steps to upgrade a supplemental Data Security server or stand-alone agents to v8.2.x.

1. To upgrade a supplemental server, launch the installer, **TRITON82*x*Setup.exe**, where *x* is the version number. The software is detected, and the upgrade wizard appears.

   To upgrade the FCI agent, launch the installer, **DataAgents82x-x64.msi**, where x is the version number.

   Other agents, such as the SMTP, printer, or TMG agent, have been discontinued.

2. Click **Next** until you complete the wizard.

   Any v7.8.4 - 8.1.x Data Security components found on this machine are upgraded.

3. Once you are done, you must deploy changes to finish the upgrade. See *Deploy settings*, page 8 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".

Upgrade protectors and mobile agents

Support for protector inline mode was dropped in v8.1. If you are using inline mode in an earlier version and you upgrade your protector to v8.2, it will audit and report on web incidents but no longer enforce them. To enforce the HTTP/S channel, use TRITON AP-WEB, AP-DATA Web Content Gateway, or a 3rd party proxy via ICAP.

Do the following to upgrade your protector or mobile agent to v8.2.x.

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. Download and unzip the protector update script, **DataProtectorUpdate82.zip**, from My Account on the Forcepoint website.
2. Copy the file, **protector-update-8.2.*x-yyyy***, into the directory `/tmp` where *x-yyyy* is the latest version and build number, such as 8.2.0-3456.
3. Enter the command:

   ```
   chmod +x /tmp/protector-update-8.2.x-yyyy
   ```

4. Run the following command:

   ```
   bash /tmp/protector-update-8.2.x-yyyy
   ```

5. Answer **Y** on the "Are you sure?" question, and complete the wizard, accepting the defaults.
6. Restart the protector or mobile agent machine when the wizard completes.
7. Once you are done, you must deploy changes to finish the upgrade. See *Deploy settings*, page 8 for instructions.
8. It is strongly recommended you wait 30 minutes before routing traffic though the upgraded system.

   When you upgrade a protector, 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.

Upgrade Email Gateway for Office 365 virtual machines

Use the following steps to upgrade the Email Gateway virtual machine in Azure.

1. Visit My Account and select **TRITON AP-DATA Gateway > Version 8.2 > AP-DATA Email Gateway for Microsoft Office 365**.
2. Download and unzip the gateway upgrade package, **DataEmailGatewayUpdate82_VA.tgz**. (It can take more than an hour to download.)
3. Using PuTTY or a similar utility, log on to the email gateway virtual appliance in Azure.
4. Type the following steps to install an FTP server:

   ```
   yum install vsftpd
   yum install ftp
   service vsftpd restart
   chkconfig vsftpd on
   ```

5. Copy the upgrade tgz file into the /var/ftp/pub/ folder.
6. Run the **email_va_config.py** command from /usr/local/sbin to open the TRITON AP-DATA Email Gateway Configuration screen.
7. Select **Upgrade Email Appliance** and click **Configure**.
8. On the Upgrade Virtual Appliance page, enter the complete FTP server path for the virtual appliance upgrade package in the **Upgrade URL** field.
9. Click **Upgrade** to initiate the upgrade process. This process can take several minutes.
10. After the upgrade process is complete, check the following log file for any upgrade alerts or messages: **/var/log/upgrade.log**.

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

For best practice, upgrade a handful of endpoints and ensure that they're working before upgrading all of the endpoints in your deployment.

Backward compatibility

TRITON AP-DATA v8.2 can support older endpoint versions if you upgrade your management server rather than un-install and re-install it from scratch.

Version 7.8.x, 8.0.x, and 8.1.x endpoints are fully compatible with the v8.2 management server. They can accept new policies, classifiers, profiles, incidents, fingerprint updates, and status notifications. To take advantage of new endpoint features, however, they must be upgraded to v8.2.

Version 8.2 does not support v7.7.x endpoints or earlier.

Forward compatibility

Version 8.2 endpoints can work with the following TRITON management servers and AP-DATA servers; however, endpoint features that were added after the manager release—such as support for screen captures on Mac—won't work. Version 8.2 endpoints will benefit from their updated operating system and browser support.

- v7.8.4
- v8.0
- v8.0.1
- v8.1

Windows

After you have upgraded the TRITON management server and all supplemental TRITON AP-DATA servers:

1. Select **Start > Programs > Websense > TRITON AP-DATA > Endpoint Package Builder** on the management server to launch the endpoint client package builder.

   On Windows Server 2012, browse to the Start page and select **Endpoint Package Builder**.
2. On the **Select Protection Options** screen, select **TRITON AP-ENDPOINT DLP**.
3. Choose Windows 32- and/or 64-bit when prompted.
4. On the Installation Path screen, confirm the location where you want the endpoint client software installed.
5. On the Server Connection screen, confirm the IP address of the TRITON AP-DATA server to use and your auto-update settings, if applicable.
6. Confirm the endpoint client settings.

7. Deploy the v8.2.x package to each endpoint using GPO, SMS, or a similar deployment method. You can install v8.2.x on top of earlier versions without uninstalling and re-installing them. The endpoint software package uninstalls earlier versions for you.
8. Restart the endpoint after installation is complete.

For best practice, deploy an endpoint auto-update server. This can be used to push an endpoint installation package to client machines and silently install the package in the background.

Linux

After you have upgraded the TRITON management server and all supplemental TRITON AP-DATA servers:

1. Select **Start > Programs > Websense > TRITON AP-DATA > Endpoint Package Builder** on the management server to launch the endpoint client package builder.
2. On the **Select Protection Options** screen, select **TRITON AP-ENDPOINT DLP**.
3. Choose Linux when prompted.
4. On the Installation Path screen, confirm the location where you want the endpoint client software installed.
5. On the Server Connection screen, confirm the IP address of the TRITON AP-DATA server to use and your auto-update settings, if applicable.
6. Confirm the endpoint client settings.
7. When the wizard completes, copy the correct installer onto the Linux machine and run it as root from the console.
   - **TRITONAP-ENDPOINT-Linux_el5** - should be used with Red Hat Enterprise Linux version 5.x.

   No reboot is necessary. The endpoint software starts automatically. You can install v8.2.x on top of earlier versions without uninstalling and re-installing them.

OS X

After you have upgraded the TRITON management server and all supplemental TRITON AP-DATA servers:

1. Select **Start > Programs > Websense > TRITON AP-DATA > Endpoint Package Builder** on the management server to launch the endpoint client package builder.
2. On the **Select Protection Options** screen, select **TRITON AP-ENDPOINT DLP**.
3. Choose Mac OS X when prompted.
4. On the Installation Path screen, note that the endpoint client software is installed in the /Applications directory. This setting cannot be modified.

5. On the Server Connection screen, confirm the IP address of the TRITON AP-DATA server to use and your auto-update settings, if applicable.
6. Confirm the endpoint client settings.
7. When the wizard completes, unzip the **TRITONAP-ENDPOINT_Mac.zip** package onto your Apple systems.
8. Run the **WebsenseEndpoint.pkg** from the unzipped folder /WebsenseEndpoint.
9. Follow the steps in the installation wizard.
10. End users may be prompted to log out and re-log on to their desktops.

See Installing and Deploying the TRITON AP-ENDPOINT or more information.

Post endpoint upgrade

Starting with v8.2, 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.