FORCEPOINT
POWERED BY Raytheon

Upgrading to TRITON AP-DATA v8.2.5

Forcepoint™ TRITON® AP-DATA Gateway and Discover

v8.2.5

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

Published 2016

Trademarks

Contents

1 Upgrading to TRITON AP-DATA v8.2.5

Data Security must be at least version 8.2.0 to upgrade to TRITON AP-DATA v8.2.5. 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 8.2.0	Upgrade to 8.2.5
7.7.x	Upgrade to 7.8.4	Upgrade to 8.2.0	Upgrade to 8.2.5	
7.8.1 - 7.8.3	Upgrade to 7.8.4	Upgrade to 8.2.0	Upgrade to 8.2.5	
7.8.4	Upgrade to 8.2.0	Upgrade to 8.2.5		
8.0.x	Upgrade to 8.2.0	Upgrade to 8.2.5		
8.1.x	Upgrade to 8.2.0	Upgrade to 8.2.5		
8.2.0	Upgrade to 8.2.5			

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 v8.2.0 to TRITON AP-DATA v8.2.5:

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
- Email Gateway for Microsoft Office 365 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 8.2.0.
- 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.

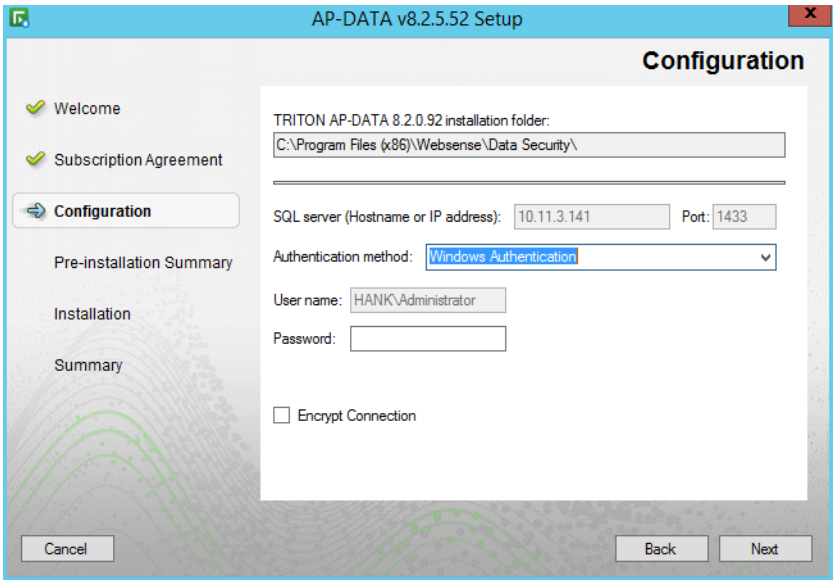
Note that the speed and success of your upgrade are affected by many factors, including:

- 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

1. Obtain the package from My Account on the Forcepoint website.
2. On the Downloads page, select **TRITON AP-DATA**, **8.2.5**, then click **TRITON AP-DATA upgrade package**.
3. Click **Download** on the resulting page.
4. Double-click the installer, **DataUpgrade825.exe,** to launch it.
5. Proceed through the **Welcome** and **Subscription Agreement** screens.

6. On the **Configuration** page, complete the fields as shown below, then click **Next**. The installer tries to connect with the SQL Server database before proceeding.



Field	Description
TRITON AP-DATA 8.2.0.nn installation folder	Shows the installation folder used for your existing installation. Not editable.
SQL server (Hostname or IP address)	Shows the hostname or IP address of the SQL server database currently serving your TRITON AP-DATA installation. The SQL settings are retrieved from your TRITON infrastructure setup. If missing, supply the value here.
Port	Shows the port number for accessing SQL Server. If missing, supply the value here.
Authentication method	The authentication method to use when connecting with the database: **SQL Server Authentication** (to use a SQL Server account) or **Windows Authentication** (to use a Windows trusted connection).
User name	A user with system administrator rights on SQL Server. If you select Windows authentication, this field is not editable. It uses the current user.
Password	The administrator's password. Edit this as needed.
Encrypt connection	Shows whether the connection with your SQL database is encrypted.

7. Once SQL connection is achieved, the installer presents a **Pre-installation Summary** page. Click **Next** and it begins the installation. A **Summary** page shows the results.

Upon completion, all necessary components on the TRITON management server are upgraded. No restart is necessary.

After upgrade, your system has the same configuration as before the upgrade.

8. If you plan to use the new incident risk scoring feature, install the analytics engine as described in the TRITON AP-DATA Installation Guide. The Analytics Engine is used to calculate the risk of user activity, correlate it with other risky activity, and assign it a risk score.

Upgrade supplemental servers and standalone agents

No changes have been made to supplemental TRITON AP-DATA servers, FCI agents, or Email Gateway for Office 365 in v8.2.5, so no upgrade is required. Version 8.2.5 management servers can work with v8.2.0 secondary servers and agents.

Upgrade protectors and mobile agents

Version 8.2.5 of the protector includes CentOS 7. You cannot upgrade from previous versions of the protector, including v8.2.0, because they are built on Cent OS 5. You must re-image the protector from scratch to use the new CentOS 7 version.

The protector and mobile agent are forward compatible, so you can retain your existing installation and still take advantage of v8.2.5 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.

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

TRITON AP-DATA v8.2.5 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, 8.1.x, and 8.2.0 endpoints are fully compatible with the v8.2.5 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 v8.2.5.

Version 8.2.5 does not support v7.7.x endpoints or earlier.

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

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 v8.2.5 package to each endpoint using GPO, SMS, or a similar deployment method. You can install v8.2.5 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.

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.