v8.2 Release Notes for On-Premises TRITON AP-EMAIL

Topic 70199 | Release Notes | TRITON AP-EMAIL | Version 8.2 | Updated: 02-May-2016

Applies To:	TRITON AP-EMAIL v8.2

Forcepoint™ TRITON® AP-EMAIL version 8.2 is a feature and correction release that includes email protection improvements and fixes, some requested by our customers. See *Important updates* for a list of vulnerability fixes included in this version.

Part of the TRITON APX security solutions, TRITON AP-EMAIL is a Forcepoint on-premises, appliance-based system that prevents malicious email threats from entering an organization's network, and protects sensitive data from unauthorized email transmission.

TRITON AP-EMAIL may be deployed on a Forcepoint V-Series appliance (V10000 or V5000). See the V-Series appliance Getting Started Guide for information about configuring the appliance.

> **Important**
>
> Some older V10000 and V5000 appliances are not supported with version 8.0.0 and later. See V-Series appliances supported with version 8.0 for details.

You can also deploy TRITON AP-EMAIL on a virtual appliance. Download the appropriate image file from the My Account downloads page. See the virtual appliance Quick Start Guide for deployment information.

In addition, TRITON AP-EMAIL can be deployed on a Forcepoint X-Series modular chassis blade server, part of a high-performance network security system. This support has the benefit of making on-premises email protection available on a platform that is scalable for large enterprise organizations. See the following resources for information about X-Series appliance deployment:

- X-Series Appliance Getting Started Guide
- X-Series Appliance Command Line Interface Guide

Use these Release Notes to find information about version 8.2 TRITON AP-EMAIL. Version 8.2 Release Notes are also available for the following Forcepoint products:

- TRITON Manager
- Forcepoint Web Protection Solutions (including Content Gateway)
- Forcepoint Data Protection Solutions
- V-Series Appliance
- X-Series Appliance

See the Administrator Help for details about on-premises TRITON AP-EMAIL operations.

If you are installing this on-premises email protection solution for the first time, see Installing Forcepoint Appliance-Based Solutions.

If you are upgrading from a previous email protection system version, see Upgrading Email Protection Solutions.

Important updates

This version of Forcepoint TRITON AP-EMAIL includes several security updates.

- The TRITON Manager Email module is enhanced to secure backup/restore remote storage credentials.
- Email protection system analytics engine is updated for enhanced threat detection.

The following vulnerabilities are also addressed in this release:

- **glibc** vulnerability updates (CVE-2015-7547)
- OpenSSL vulnerability updates, including:
  - ■ CVE-2015-3193
  - ■ CVE-2015-3194
  - ■ CVE-2015-3195
  - ■ CVE-2015-3196
  - ■ CVE-2015-1794
  - ■ CVE-2015-1788
  - ■ CVE-2015-1789
  - ■ CVE-2015-1790
  - ■ CVE-2015-1791
  - ■ CVE-2015-1792
  - ■ CVE-2014-8176
- Apache Tomcat vulnerability updates, including:
  - ■ CVE-2014-0230
  - ■ CVE-2014-7810
  - ■ CVE-2014-0227

Contents

New in version 8.2

Topic 70200 | Release Notes | TRITON AP-EMAIL | Version 8.2 | Updated: 02-May-2016

Applies To:	TRITON AP-EMAIL v8.2

TRITON AP-EMAIL version 8.2 includes the following new features:

- *Forcepoint LLC branding*
- *Secure message delivery as backup encryption method*
- *Advanced file analysis*

This release also contains these enhancements:

- Support for Federal Information Processing Standards (FIPS) 140-2
- Improvements to optimize the detection of virus and malware threats in email, including an option to increase the frequency of database download server updates. An administrator may now select a 5-minute frequency option (**Settings > General > Database Downloads**). Click **Edit** in the Schedule column, and select **Every 5 minutes** in the Reschedule Update dialog box.

Forcepoint LLC branding

To support the transition from Raytheon | Websense to Forcepoint LLC, the TRITON Manager has a new look and feel. The colors and logos throughout the manager, including the logon screen, have been updated to reflect the Forcepoint brand.

End-user tools like the Personal Email Manager and Forcepoint Secure Messaging portals and login screens also reflect the new branding.

These changes do not affect product functionality.

Over time, you may notice the branding extended to other areas of the product, like the Help system, as well as to external content, like the Knowledge Base.

Secure message delivery as backup encryption method

In previous versions, secure message delivery has been a standalone, on-premises function for securing outbound email that contains sensitive or personal information. You can configure a secure message delivery portal where your organization's customers view and manage messages that contain sensitive information (**Settings > Inbound/Outbound > Encryption**).

In this version, you can now specify Secure Message Delivery as a backup encryption method for outbound email when mandatory TLS encryption is selected as the primary encryption method. Your email recipients can use this secure portal to view email in the event an outbound TLS connection for message encryption is not successful.

See the topic titled Handling encrypted messages in TRITON AP-EMAIL Administrator Help for details.

Advanced file analysis

Previous versions of the TRITON AP-EMAIL on-premises solution included a cloud-hosted File Sandbox function for analysis of file attachment content. This version introduces an additional on-premises sandbox option, the Threat Protection appliance system. Together, these options constitute the TRITON AP-EMAIL Advanced File Analysis function.

Select the advanced file analysis platform you want to use (File Sandbox or Threat Protection) on the **Settings > General > Advanced File Analysis** page. Note that only 1 sandbox platform may be used; you cannot select both platforms.

Use the advanced file analysis filter and action based on your platform selection (**Main > Policy Management > Filters**). Based on your selection on the **Settings > General > Advanced File Analysis** page, you can configure either a File Sandbox or Threat Protection filter.

> **Important**
> The Threat Protection appliance system is a highly sophisticated, multiple-appliance analysis environment that is part of a Forcepoint **controlled release** for version 8.2. Contact your Forcepoint sales representative or partner for information about the new system and how your organization may qualify to use Threat Protection.

Installation and upgrade

Topic 70201 | Release Notes | TRITON AP-EMAIL | Version 8.2 | Updated: 02-May-2016

Applies To:	TRITON AP-EMAIL v8.2

If you are installing the on-premises email protection system for the first time, see Installing Forcepoint Appliance-Based Solutions.

Important

To ensure that you install all required components of your email protection solution, including data loss prevention, we recommend that you select **TRITON AP-EMAIL** on the Installation Type page of the TRITON Unified Installer, rather than performing a Custom installation of the product.

When you select TRITON AP-EMAIL on this page, then TRITON AP-DATA is automatically selected as well. Data loss prevention functions are installed along with email protection functions.

A Custom installation does not automatically install TRITON AP-DATA with TRITON AP-EMAIL.

If you are upgrading from a previous email protection version, see Upgrading Email Protection Solutions.

Warning

On the Select Components screen in the TRITON upgrade installer, ensure that the **TRITON AP-EMAIL** option is selected. This option is required if you are running your email protection system on a V- or X-Series appliance or an on-premises (ESXi server) virtual appliance.

The **TRITON AP-DATA Email Gateway** option applies to a cloud-hosted virtual appliance running with TRITON AP-DATA. See the topic titled “Email Gateway for Microsoft Office 365” in the TRITON AP-DATA Installation Guide for details about this product feature.

Requirements

On-premises TRITON AP-EMAIL is supported on the following platforms:

- Forcepoint V-Series appliance (V10000 or V5000)

Important

Some older V10000 and V5000 appliances are not supported with version 8.0.0 and later. See V-Series appliances supported with version 8.0 for details.

- Forcepoint X-Series modular chassis security blade (X10G)

See the X-Series appliance Getting Started Guide and Command Line Interface (CLI) Guide for information about setting up and configuring an X-Series modular chassis and email security blades.

- Virtual appliance (ESXi VMware version 4.0 or later)

  Download the appropriate image file from the My Account downloads page. See the virtual appliance Quick Start Guide for deployment information.

✓ **Note**

You may encounter a set of warning messages during virtual appliance installation. These postfix warnings do not affect virtual appliance operation.

Note that you cannot cluster a V-Series appliance or an X-Series security blade with a virtual appliance.

The TRITON Manager and Email Log Server are hosted on a separate Windows Server machine. (This server must be running an English language instance of Windows Server.)

Microsoft SQL Server is used for the Email Log Database. See System requirements for this version for detailed information about supported applications and versions.

! **Important**

Although a version 8.0 and later Email management console can allow an earlier version appliance (e.g., version 7.8.4) to be added on the Email Appliances page, the management settings for that appliance are read-only and cannot be modified.

For optimal system efficiency and performance, we strongly recommend that manager console and appliance versions match.

If your Microsoft SQL Server installation uses a named instance, port 1433 is opened on the firewall even if you specify a different port during TRITON AP-EMAIL installation. You must manually change this port setting after installation is complete.

Web browser support

TRITON AP-EMAIL on-premises version 8.2 supports the use of the following Web browsers:

- Microsoft Internet Explorer (IE) 8, 9 (compatibility view not supported), 10, and 11
- Microsoft Edge 15, 20, and 25
- Mozilla Firefox versions 4.4 through 44
- Google Chrome 13 through 49

Upgrade paths

If you are running Email Security Gateway version 7.8.4 or TRITON AP-EMAIL version 8.x, you can upgrade directly to TRITON AP-EMAIL version 8.2. You must perform intermediate upgrades if you are running any other previous version of Email Security Gateway.

See Upgrading Email Protection Solutions for:

- Links to all intermediate upgrade instructions
- Important information about backing up your system before you upgrade

The following upgrade paths are available for TRITON AP-EMAIL version 8.2:

Current Version	Upgrade Path			
7.6.x	7.7.0	7.8.0	7.8.4	8.2.0
7.7.x	7.8.0	7.8.4	8.2.0	
7.8.x (7.8.2 or 7.8.3)	7.8.4	8.2.0		
7.8.4	8.2.0			
8.x	8.2.0			

Any version 7.6.x Email Security Gateway component that is currently installed on Windows Server 2003 must be migrated to Windows Server 2008 R2 before an upgrade to version 7.7.0. Migration to Windows Server 2012 may be performed after an upgrade to version 7.8.0.

Important

See Upgrading Email Protection Solutions for detailed upgrade preparation and process instructions.

Ensure that you perform all recommended activities before and after your upgrade, including the repair to your Data module registration.

You may upgrade an Email Security Gateway virtual appliance directly from version 7.8.4 to TRITON AP-EMAIL version 8.2. See Upgrading Email Protection Solutions for complete instructions.

You must upgrade a version 7.8.4 Email Security Gateway X-Series chassis security blade to TRITON AP-EMAIL version 8.0.0 before you can upgrade to version 8.2. To upgrade an X-Series security blade, see the following materials:

- X-Series Appliance Release Notes
- X-Series Appliance Command Line Interface Guide

Resolved and known issues

Topic 70202 | Release Notes | TRITON AP-EMAIL | Version 8.2 | Updated: 02-May-2016

Applies To:	TRITON AP-EMAIL v8.2

A list of resolved and known issues for this version of Forcepoint TRITON AP-EMAIL is available in the Technical Library. If you are not already logged on to the Forcepoint My Account site, this link takes you to the log in screen.