v8.3 Release Notes for On-Premises TRITON AP-EMAIL

Release Notes | TRITON AP-EMAIL | Version 8.3 | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

Forcepoint™ TRITON® AP-EMAIL version 8.3 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.

The Forcepoint TRITON AP-EMAIL solution is available on a V-Series appliance or an X-Series appliance security blade. You may also deploy TRITON AP-EMAIL on a virtual appliance, which can be downloaded from the Forcepoint My Account downloads page. See the TRITON Appliances Getting Started Guide for detailed information about configuring any Forcepoint 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.

Use these Release Notes to find information about version 8.3 TRITON AP-EMAIL. Version 8.3 Release Notes are also available for the following Forcepoint products:

- TRITON Manager
- Forcepoint Web Protection Solutions (including Content Gateway)
- Forcepoint Data Protection Solutions
- TRITON Appliances

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

Important updates

This version of Forcepoint TRITON AP-EMAIL includes several security updates for cross-site scripting, weak SSL ciphers, the Apache Commons Collections library (CWE-502), and the Java runtime. The following OpenSSL vulnerabilities are also addressed in this release:

- CVE-2016-2106
- CVE-2016-2107
- CVE-2016-2108
- CVE-2016-2176

Contents

New in version 8.3

Release Notes | TRITON AP-EMAIL | Version 8.3 | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

TRITON AP-EMAIL version 8.3 includes the following new features:

- *New appliance architecture*
- *Spoofed email detection policy rule*
- *TRITON web protection URL category updates*
- *URL analysis policy rule enhancements*
- *Enhanced antivirus engine*
- *Modified left navigation pane design*

New appliance architecture

In version 8.3, the Forcepoint V-Series appliance on which TRITON AP-EMAIL runs has been re-architected for enhanced performance. The new 64-bit container-based appliance uses a command-line interface (CLI) for individual appliance management.

Also beginning with this version, the V-Series appliance no longer supports dual security mode. An appliance may be set up in either Email or Web security mode, but not both.

Upgrades from dual-mode appliances require that one product module be removed before you upgrade the remaining product. For TRITON AP-EMAIL, this process involves migrating Email protection system data from a dual-mode appliance to a new version 8.3 hardware or virtual appliance and then removing the Email module from the appliance. See Upgrading V-Series Dual-Mode Appliances to Version 8.3 for detailed information.

TRITON AP-WEB (which includes the Content Gateway) does not have a migration path and cannot be removed from the dual-mode appliance. However, you can remove a TRITON Web Filter & Security module and perform a fresh installation of that product on a new appliance.

A new 64-bit virtual appliance is also available in this release. See the TRITON Appliances Getting Started Guide for setup and installation details. Upgrades from an existing virtual appliance involve migrating Email protection system data to a new version 8.3 virtual appliance. See Upgrading Email Security Gateway v7.8.4 to TRITON AP-EMAIL v8.3 for information.

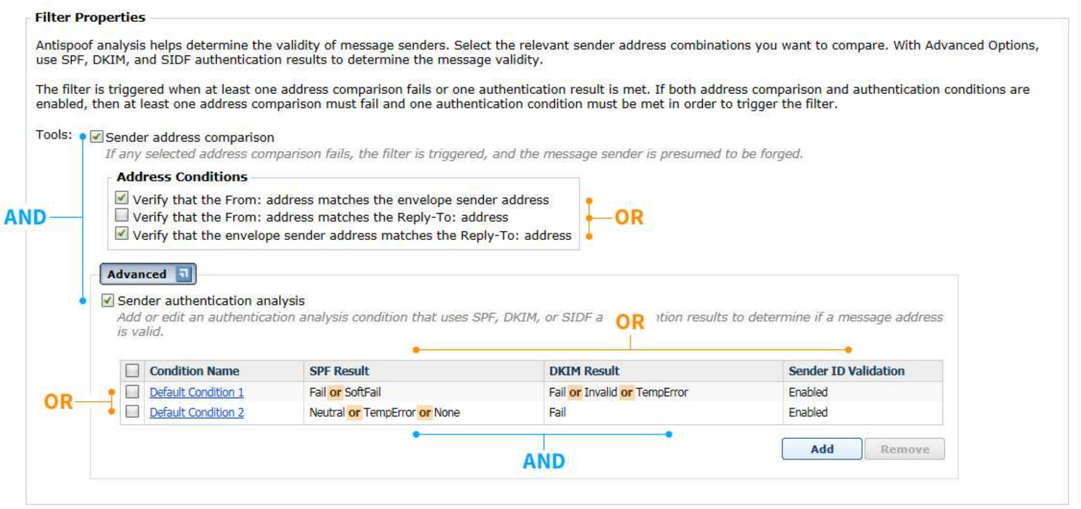
The X-Series appliance architecture is unchanged from previous versions.

Spoofed email detection policy rule

A new default Antispoof policy rule can help determine the validity of message senders and reduce instances of sender impersonation. The policy rule can provide assistance in determining, for example, whether an email that appears to be a request to the Finance team from the company CEO to wire a large sum of money to a specified account is not, in fact, from the CEO.

The new rule comprises a default Spoofed Email filter and Spoof filter action. Filter functionality uses a combination of message sender comparisons and rules based on the authentication results from Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Sender ID Framework (SIDF) to determine the likelihood that a sender address may be forged.

The following screen shot of Spoofed Email filter properties summarizes the relationships among the spoofed email filter options (**Main** > **Policy Management** > **Filters**):



Filter Properties

Antispoof analysis helps determine the validity of message senders. Select the relevant sender address combinations you want to compare. With Advanced Options, use SPF, DKIM, and SIDF authentication results to determine the message validity.

The filter is triggered when at least one address comparison fails or one authentication result is met. If both address comparison and authentication conditions are enabled, then at least one address comparison must fail and one authentication condition must be met in order to trigger the filter.

Tools: ☑ Sender address comparison

If any selected address comparison fails, the filter is triggered, and the message sender is presumed to be forged.

Address Conditions

☑ Verify that the From: address matches the envelope sender address
☐ Verify that the From: address matches the Reply-To: address
☑ Verify that the envelope sender address matches the Reply-To: address

Advanced

☑ Sender authentication analysis

Add or edit an authentication analysis condition that uses SPF, DKIM, or SIDF a tion results to determine if a message address is valid.

☐	Condition Name	SPF Result	DKIM Result	Sender ID Validation
☐	Default Condition 1	Fail **or** SoftFail	Fail **or** Invalid **or** TempError	Enabled
☐	Default Condition 2	Neutral **or** TempError **or** None	Fail	Enabled

Add Remove

For detailed configuration information about the new policy rule, see Spoofed email in TRITON AP-EMAIL Administrator Help.

By default, a message that triggers the Antispoof rule is passed to the next rule in the policy for processing. If the message is delivered after all rule processing is complete, the email subject is modified with the addition of “POSSIBLY SPOOFED”. The default behavior can be changed via different configuration settings.

To derive maximum benefit from the Antispoof rule, ensure that it is positioned ahead of the Antispam rule in the policy Rules list. When message processing resumes, the results of spoofed email analysis are added to the message header. The email protection system uses these results along with subsequent analysis results to determine a spam score.

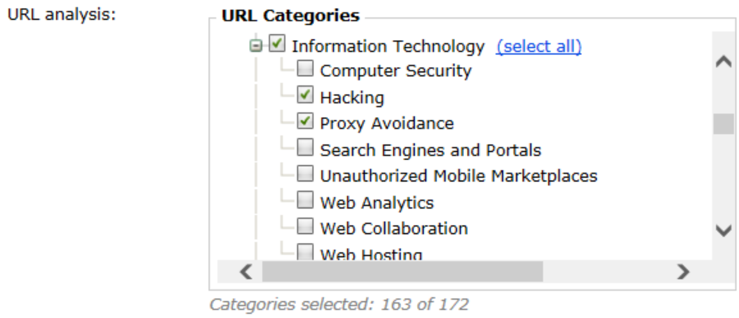
The new feature allows an administrator to specify sender IP address groups that can bypass the Antispoof rule. Add an IP address group filter bypass condition on the **Main** > **Policy Management** > **Policies** > **Add** (or **Edit**) **Policy** > **Add** (or **Edit**) **Rule** page.

The Message Log can now be searched based on a Spoofed Email message analysis result, and Message Log message detail entries include spoofed email information.

TRITON web protection URL category updates

In previous versions, the URL Analysis filter URL Categories list that appeared in the TRITON AP-EMAIL **Main** > **Policy Management** > **Filters** > **Add** (or **Edit**) **Filter** page was a special version of the TRITON web protection solution list adapted for the TRITON AP-EMAIL user interface. In this release, the URL Categories list is replaced with the full URL categories list and the category mappings from the TRITON web protection solution.

On the **Main > Policy Management > Filters > Add** (or **Edit**) **Filter** page, select the categories you want the URL Analysis filter to detect by marking the associated check box in the categories list. Marking a major category does not automatically select all the categories listed with it. For example, marking the check box for the Information Technology category does not automatically select all that category's sub-categories.



URL analysis:

URL Categories

- ☑ Information Technology (select all)
  - □ Computer Security
  - ☑ Hacking
  - ☑ Proxy Avoidance
  - □ Search Engines and Portals
  - □ Unauthorized Mobile Marketplaces
  - □ Web Analytics
  - □ Web Collaboration
  - □ Web Hosting

Categories selected: 163 of 172

As in previous versions, the master database location settings are configured on the **Settings > General > URL Analysis** page. Select a URL analysis service installed with your TRITON web protection solution from the drop-down list:

- Filtering Service (default)

  The Filtering Service has been used in all previous versions of TRITON AP-EMAIL for URL analysis master database access and category updates.

- Linking Service

  Like the Filtering Service, the Linking Service can be used for database access. In addition, the Linking Service provides enhanced database functionality, including dynamic custom URL category and category mapping updates from the web protection solution master database. Because Linking Service is an optional web protection component, you must ensure that it is installed before you configure URL analysis.

For configuration information, see URL analysis with Forcepoint Web protection solutions in TRITON AP-EMAIL Administrator Help.

URL analysis policy rule enhancements

In previous versions of TRITON AP-EMAIL, the URL Analysis default rule treated a message that triggered the URL Analysis filter as a spam message. Unless the default rule was modified to quarantine these types of messages, end users with Personal Email Manager privileges could inadvertently deliver malicious embedded URLs to their inboxes. You could not configure multiple URL Analysis type rules.

In this version, you can create and configure additional URL analysis policy rules to detect and quarantine messages that contain malicious URLs so that they cannot be released by an end user. A new “url-analysis” default queue is provided to store the quarantined email.

You can add a URL Analysis rule to handle email with suspicious embedded URLs by:

1. Creating a new URL analysis filter in the **Main** > **Policy Management** > **Filters** page (URL analysis in TRITON AP-EMAIL Administrator Help)
2. Creating a URL analysis filter action in the **Main** > **Policy Management** > **Actions** page (Managing filter actions in TRITON AP-EMAIL Administrator Help)
3. Adding a new rule on the **Main** > **Policy Management** > **Policies** > **Add** (or **Edit**) **Policy** page using your new URL analysis filter and filter action (Adding a rule in TRITON AP-EMAIL Administrator Help).

A new URL Analysis message type appears in the message type or message analysis result fields in the Message Log, Personal Email Manager, presentation reports, and dashboard charts.

Enhanced antivirus engine

In this release of TRITON AP-EMAIL, the virus filter includes an additional analytics engine that can improve the detection of malicious threats contained in Microsoft Office attachments in inbound email. The new tool comprises a set of rules, each of which determines part of a threshold score for an individual attachment. The cumulative total of these scores determines how the email protection system handles that attachment.

In the **Main** > **Policy Management** > **Filters** > **Add** (or **Edit**) **Filter** page, filter properties include 2 types of analysis:

- Standard
- Advanced

The standard analysis antivirus tool is the engine that has been included in all previous versions of the on-premises email protection solution. Advanced analysis is the new antivirus engine.

You may select either one or both types of analysis to perform, along with the sensitivity level of each analysis type. Standard analysis is performed first, before advanced analysis. The higher the sensitivity level, the larger the volume of email that is designated as virus. Note that enabling the advanced antivirus engine may affect system performance.

Important

If you have configured multiple antivirus filters, ensure that the sensitivity level settings are the same for all the filters. Different sensitivity levels may interrupt message processing and require an appliance restart.

Schedule advanced attachment analysis downloads on the **Settings** > **General** > **Database Downloads** page.

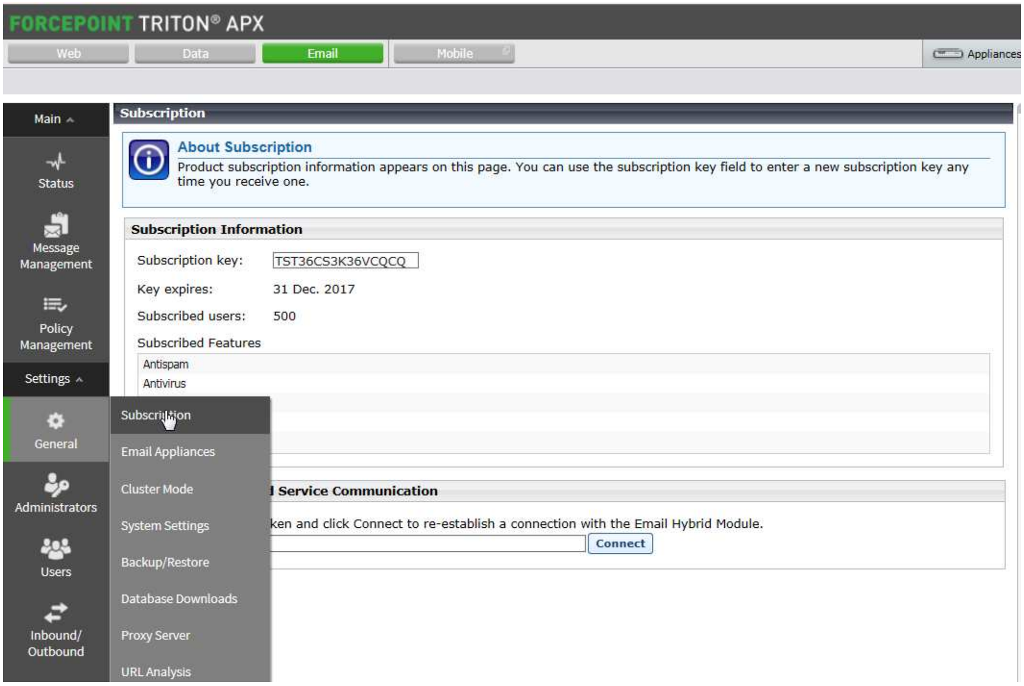
For configuration information, see Antivirus in TRITON AP-EMAIL Administrator Help.

Modified left navigation pane design

The Main and Settings tabs in the left navigation pane are redesigned in this release for a more streamlined look and feel. The new design also allows more workspace in the TRITON Manager.

Both tabs are collapsed into a single pane, with the Main menu selections at the top of the pane. The Settings menu options are located beneath the **Main** > **Policy Management** options.

Mouse over a primary menu item to view the available menu options in that section. For example, the selection of **Settings** > **General** > **Subscription** is show here:



Subscription

About Subscription

Product subscription information appears on this page. You can use the subscription key field to enter a new subscription key any time you receive one.

Subscription Information

Subscription key: TST36CS3K36VCQCQ

Key expires: 31 Dec. 2017

Subscribed users: 500

Subscribed Features

Antispam

Antivirus

d Service Communication

ken and click Connect to re-establish a connection with the Email Hybrid Module.

Installation and upgrade

Release Notes | TRITON AP-EMAIL | Version 8.3 | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

Requirements

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

- Forcepoint V-Series appliance (V10000 or V5000)
- Forcepoint X-Series modular chassis security blade (X10G)
- Virtual appliance

  Download the appropriate image file from the My Account downloads page. See the TRITON Appliances Getting Started Guide for deployment information.

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 8.3 supports the use of the following Web browsers:

- Microsoft Internet Explorer (IE) 9 (compatibility view not supported), 10, and 11
- Microsoft Edge 15, 20, and 25

- Mozilla Firefox versions 47 through 49
- Google Chrome 50 through 53

Some TRITON Manager Email module screens may not display or scroll properly in Microsoft Internet Explorer (IE). You should consider using a different browser.

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 8.3. 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 direct and intermediate upgrade instructions
- Important information about backing up your system before you upgrade

The following upgrade paths are available for TRITON AP-EMAIL version 8.3:

Current Version	Upgrade Path			
7.6.x	7.7.0	7.8.0	7.8.4	8.3.0
7.7.x	7.8.0	7.8.4	8.3.0	
7.8.x (7.8.2 or 7.8.3)	7.8.4	8.3.0		
7.8.4	8.3.0			
8.x	8.3.0			

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.

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 8.3. To upgrade an X-Series security blade, see the X-Series upgrade guide for details.

Resolved and known issues

Release Notes | TRITON AP-EMAIL | Version 8.3 | Updated: 19-Dec-2016

Applies To:	TRITON AP-EMAIL v8.3

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