v8.4 Release Notes for On-Premises Forcepoint Email Security

Release Notes | Forcepoint Email Security | Version 8.4 | Updated: 31-July-2017

Applies To:	Forcepoint Email Security v8.4

Forcepoint Email Security version 8.4 (the email protection solution formerly known as TRITON AP-EMAIL) 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.

Forcepoint Email Security is an 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 Email Security solution is available on a V Series appliance or an X Series appliance security blade. You may also deploy Forcepoint Email Security on a virtual appliance, which can be downloaded from the Forcepoint My Account downloads page. See the Forcepoint 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 8.4 Forcepoint Email Security. Version 8.4 Release Notes are also available for the following Forcepoint products:

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

See the Administrator Help for details about on-premises Forcepoint Email Security operations.

Important updates

This version of Forcepoint Email Security includes several security updates, including some fixes in the Forcepoint Security Manager, Forcepoint Secure Messaging end-user portal, and Personal Email Manager. The following vulnerabilities are also addressed in this release:

- libcurl library vulnerability updates, including:

  CVE-2016-5420

  CVE-2016-5421

  CVE-2016-8615

  CVE-2016-8624

- OpenSSL vulnerability updates, including:

  CVE-2017-3730

  CVE-2017-3731

  CVE-2017-3732

- Tomcat vulnerability updates, including:

  CVE-2015-5174

  CVE-2015-5345

  CVE-2015-5346

  CVE-2015-5351

  CVE-2016-0706

  CVE-2016-0714

  CVE-2016-0763

Contents

- *New in version 8.4*
- *Installation and upgrade*
- *Resolved and known issues*

New in version 8.4

Release Notes | Forcepoint Email Security | Version 8.4 | Updated: 31-July-2017

Applies To:	Forcepoint Email Security v8.4

Forcepoint Email Security version 8.4 includes the following new features:

- *Forcepoint product renaming*
- *Email Attachment policy rule*
- *Cloud-based URL analysis option*

- *Relay control SPF settings*
- *Product license behavior*
- *Other changes and enhancements*

Forcepoint product renaming

Forcepoint continues to define its brand and unify its product lines under a single branding scheme. To this end, product names and some product component names have changed in version 8.4. The following table summarizes the naming evolution for the Forcepoint Email Security product (and its components):

Version 7.8.x Name	Version 8.0, 8.1, 8.2, 8.3 Name	Version 8.4 Name
Email Security Gateway	TRITON AP-EMAIL with: ● Email DLP Module	Email Security ● Email Security DLP Module
Email Security Gateway Anywhere	TRITON AP-EMAIL with: ● Email DLP Module ● Email Hybrid Module ● Email Sandbox Module (if purchased)	Email Security with: ● Email Security DLP Module ● Email Security Hybrid Module ● The Email Sandbox module is no longer available as a separate item. URL Sandbox and phishing education and reporting capabilities are generally available to email protection system subscribers who purchase the Email Security Hybrid Module (formerly known as the Email Hybrid Module).
Advanced Email Encryption	Email Encryption Module	Email Security Encryption Module
ThreatScope	ThreatScope/File Sandbox	Advanced Malware Detection for Email - Cloud
N/A	*Introduced in v8.2:* Threat Protection appliance	Advanced Malware Detection for Email - On-Premises
Email Security Manager	TRITON Manager	Forcepoint Security Manager

Email Attachment policy rule

A new Email Attachment policy rule allows Forcepoint Email Security to examine email attachment content and determine an attachment’s true file type. The rule comprises a default Email Attachment filter and an Email Attachment Default filter action. This rule is enabled by default and is applied to email that matches policy conditions after the Antivirus policy rule is applied.

The rule is triggered when a specified true file type is detected. Default rule behavior is:

- Drop the email.
- Save it to a new **attachment** queue for administrator action.
- Ensure that the email recipient does not have Personal Email Manager access to that message.

An additional option to check for a custom file attachment extension or file name detects the specified extension or file name, which triggers the rule. However, in this instance, attachment content is not inspected for true file type.

A new Email Attachment message analysis result appears in the Message Log and in the Personal Email Manager end-user portal. You can search the Message Log by a new Email Attachment analysis result. Email attachments that trigger the filter are listed in the Message Log details entry for the message.

A message that triggers the Email Attachment rule appears in the Blocked Messages queue (**Main** > **Message Management** > **Blocked Messages**) with a message type of Email Attachment. Detected attachments are displayed in the Quarantined Reason column of the queue.

The following default presentation reports are added in this release for the Email Attachment policy rule:

- Top Email Attachments Detected by the Email Attachment Filter
- Top Attachment File Types Detected by the Email Attachment Filter
- Top Inbound Email Attachment Recipients
- Inbound Email Attachment Detection Volume Summary
- Outbound Email Attachment Detection Volume Summary

With the addition of this filter, the **Treat encrypted files as infected** default Virus filter properties option is removed. Upgrading customers who have configured the Virus filter option will see encrypted files analyzed as part of the new Email Attachment filter.

For configuration information, see Forcepoint Email Security Administrator Help.

Cloud-based URL analysis option

URL analysis compares a URL embedded in email with a database of categorized URLs, providing category information to allow Forcepoint Email Security to properly handle the URL. Existing functionality provides URL analysis via a Forcepoint web security solution, using either Forcepoint Filtering Service or Linking Service to access a URL database.

This version of Email Security introduces a new service for URL analysis that does not require a Forcepoint web protection solution to be installed. The Threat Intelligence Cloud Service allows direct access to the cloud-hosted Forcepoint Master Database, which is a real-time repository of classified URLs. This cloud database is used by many Forcepoint solutions to identify potentially dangerous or simply unwanted URLs.

Threat Intelligence Cloud Service is the default URL analysis selection for all new installations of Forcepoint Email Security. Upgrading customer installations that have not previously configured the Forcepoint web security Filtering or Linking service for URL analysis also default to the new cloud service. URL analysis for customers who already use the Filtering or Linking service retain that configuration on upgrade.

URL analysis is configured in the Forcepoint Email Security **Settings > General > URL Analysis** page. You can use a proxy server for communication with the Threat Intelligence Cloud Service.

Information about Forcepoint Master Database categories can be found on the Forcepoint web site. See Forcepoint Email Security Administrator Help for information about URL analysis configuration.

Relay control SPF settings

This version of Forcepoint Email Security offers enhanced relay control options for Sender Policy Framework (SPF) settings. Combined with DMARC validation, the new options can provide improved email authentication and prevent malicious email from entering your network.

The new SPF option on the Email Security module **Settings > Inbound/Outbound > Relay Control** page is enabled by default.

You can also configure Forcepoint Email Security to reject mail for the following SPF check results:

- Fail
- SoftFail
- Neutral
- None
- PermError
- TempError

On a new installation, these options are not marked by default.

On upgrade, existing SPF settings, if enabled, are mapped to the new options as follows:

Current Setting	Version 8.4 Setting
Reject mail if no SPF record exists	None
Reject mail if the SPF record does not match the sender's domain or a soft fail occurs	Fail SoftFail
Reject mail if an SPF error occurs	TempError PermError

The version 8.4 **Neutral** option does not map to any previous setting and is not marked by default after an upgrade.

See Forcepoint Email Security Administrator Help for information about the SPF settings.

Product license behavior

This enhancement provides customers with valid subscriptions a grace period of two weeks to provide extra time to renew their product licenses. Alert message sent daily during the grace period remind users that the subscription has expired.

Mark the **Block incoming email connections when subscription expires** option on the **Settings > General > Subscription** page to block malicious traffic after this grace period.

Other changes and enhancements

This version of Forcepoint Email Security includes the following new features or functionalities:

- The following Email Security module default settings are changed:
  - Message size limitation for spam, URL analysis, and commercial bulk email is now 3072 KB.
  - SPF checks are enabled by default (**Settings > Inbound/Outbound > Relay Control**).
  - Real-time Black List checks are enabled by default (**Settings > Inbound/Outbound > Connection Control**).
  - Reputation service default sensitivity level is now Aggressive (**Settings > Inbound/Outbound > Connection Control**).
  - The Commercial Bulk policy filter default sensitivity setting is now High (**Main > Policy Management > Filters > Commercial Bulk**).

- The scheduled default update interval for some analytics database downloads is reduced from one hour to the following:

Database Type	**Update Every:**
Cyren	15 minutes
AD&RTSS	5 minutes
ThreatName	30 minutes
App Smart Hash	15 minutes
Digital Fingerprints	15 minutes
Heuristics	30 minutes

- The following configuration setting limits are increased:

Configuration Setting	**New Maximum Limit**
IP groups	2048
Always Block or Always Permit list entries	15,000
Policy rules	64
Message queues	48
Policy actions	64
Policy conditions	64
Policy filters	64
Custom content filter conditions	64
Filter bypass conditions	8
Data Security module policy actions	32

- Additional SIEM log entries are included for enhanced log information regarding embedded URLs and file attachments:
  - replyTo
  - from
  - url (includes URL category information)
  - file name (includes file attachment information)
  - file hash (includes file attachment information)
- Email-specific command-line interface (CLI) commands are added to the V Series appliance CLI.

  The following appliance CLI commands may be visible in the CLI, but they are available only for Forcepoint Technical Support operations. They are not supported for appliance administrator use.

  ```
  set analytic-update service --status <on|off>
  ```

```
set reporting --status <on|off>
set email subscription --key <blank|reset|subscription_key>
set mta delivery --status <on|off>
load analytic-db --file <analytics_file> --location
<filestore> [--factory]
```

- A user name and password are no longer required for a proxy server that is configured on the **Settings > General > Proxy Server** page.

Installation and upgrade

Release Notes | Forcepoint Email Security | Version 8.4 | Updated: 31-July-2017

Applies To:	Forcepoint Email Security v8.4

Requirements

On-premises Email Security 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 Forcepoint Appliances Getting Started Guide for deployment information.

The Forcepoint Security 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 Security Manager 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 Email Security installation. You must manually change this port setting after installation is complete.

Upgrade paths

If you are running Email Security Gateway version 7.8.4 or TRITON AP-EMAIL version 8.1, 8.2, or 8.3, you can upgrade directly to Forcepoint Email Security version 8.4. You must perform intermediate upgrades if you are running any other previous version of Email Security Gateway or TRITON AP-EMAIL.

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 Forcepoint Email Security version 8.4:

Current Version	Upgrade Path			
7.6.x	7.7.0	7.8.0	7.8.4	8.4.0
7.7.x	7.8.0	7.8.4	8.4.0	
7.8.x (7.8.2 or 7.8.3)	7.8.4	8.4.0		
7.8.4	8.4.0			
8.0.x	8.3.0	8.4.0		
8.1.x, 8.2.x, 8.3.x	8.4.0			

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

Resolved and known issues

Release Notes | Forcepoint Email Security | Version 8.4 | Updated: 31-July-2017

Applies To:	Forcepoint Email Security v8.4

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