v8.5 Release Notes for On-Premises Forcepoint Email Security

Release Notes | Forcepoint Email Security | Version 8.5 | Updated: 28-Feb-2018

Applies To:	Forcepoint Email Security v8.5

Forcepoint Email Security version 8.5 is a feature and correction release that includes email protection improvements and fixes, some requested by our customers.

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.x for details.

Contents

Use these Release Notes to find information about version 8.5 Forcepoint Email Security. Version 8.5 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

© 2018 Forcepoint LLC

- Forcepoint Security Appliance Manager

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

New in version 8.5

Release Notes | Forcepoint Email Security | Version 8.5 | Updated: 28-Feb-2018

Applies To:	Forcepoint Email Security v8.5

Forcepoint Email Security version 8.5 includes the following new features:

- *Message Log search enhancements*
- *Personal Email Manager General Settings*
- *SIEM logging customization*
- *URL neutralization*
- *Cloud MTA IP Groups*
- *Other changes and enhancements*

Message Log search enhancements

This version of Forcepoint Email Security offers enhanced search options for finding content in the Message Log. New options include the capacity to search on up to 10 filters. Further enhancements to the Advanced Options have added new sorting conditions for Message Log searches. Viewing of the Message Log has additionally been improved, with sortable and resizable columns.

The search filter functionality is used to narrow the search by filtering results by criteria such as Subject, Spam Score, Recipient Address, or Appliance. Each filter type includes conditions such as Contains, Starts with, or Does not equal. The relationship between filters is “and”, which allows the search to be greatly refined.

The Advanced Options functionality is used to further refine the search by direction (such as Inbound or Outbound), by analysis result (such as SMTP Authentication Fail or RBL), and by message status (such as Delivered or Rejected).

The Message Log is accessed on the Message tab of the page **Main > Status > Logs**. See Forcepoint Email Security Administrator Help for information about the Message Log.

Personal Email Manager General Settings

A new General Settings page was added to the Forcepoint Security Manager to configure both the end-user portal and Personal Email Manager notification messages. Configuration settings on the General Settings page include:

- End-user action auditing
- Sender options
- Quarantine message queue display
- Quarantine message delivery

The addition of Sender Options enables administrators to configure whether the Envelope Sender address or the From address in incoming messages is displayed in the Sender column of the end-user portal, Personal Email Manager notification messages, and Always Block and Always Permit lists.

For configuration information, see Forcepoint Email Security Administrator Help.

SIEM logging customization

Forcepoint Email Security version 8.5 adds additional support for Security Information Event Management (SIEM) logging. This support includes the capacity to send console and audit logs to SIEM, and to utilize SIEM formatting compatible with QRadar (LEEF) and Splunk (key-value pairs).

Enabling SIEM integration in Forcepoint Email Security allows log data to be saved to the SIEM server using several predefined formats: syslog/common event format (CEF) (for ArcSight), syslog/key-value pairs (Splunk), and syslog long event extended format (LEEF) QRadar). Custom formats can additionally be defined.

Forcepoint Email Security can now save the following logs to the SIEM server: Policy, Connection, Message, Delivery, Hybrid, Audit, and Console.

For configuration information, see Forcepoint Email Security Administrator Help and SIEM: Email Logs.

URL neutralization

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. This version of Forcepoint Email Security includes new settings for URL analysis that allow potentially malicious URLs classified by the filter to be removed or modified for neutralization.

The default action for when a message triggers the URL analysis filter is to drop the message and save it to the spam queue, where it may be released and delivered by a

Personal Email Manager user. As a result, a message that contains a malicious link may be delivered to an inbox in the network.

New URL analysis policy rules can be configured to detect and contain URLs triggering the filter so that they cannot be released by a Personal Email Manager end user. Options in version 8.5 include modifying any URLs detected by the filter as follows:

- Remove URLs from message subject and body
- Neutralize URLs by rewriting the scheme and bracketing the last dot of the URL domain
  - This changes a malicious URL as follows:

    Before neutralization: http://www.malicious.com.ca/index.html

    After neutralization: hXXp://www.malicious.com[.]ca/index.html
- Rewrite URLs and link text labels with custom settings
  - With this option, variables can be used to rewrite URLs as needed.

A customizable notification message can be sent to users with information about the URL filter action that was taken.

URL analysis is configured on the Forcepoint Email Security page **Main > Policy Management > Filters > Add** (or **Edit**) **Filter**. See Forcepoint Email Security Administrator Help.

Cloud MTA IP Groups

This version of Forcepoint Email Security adds new cloud MTA IP groups for Office 365 and G Suite. These IP addresses are automatically updated every hour and can be used to easily create SMTP routing or TLS connection policies. IP groups are configured on the page **Settings > Inbound/Outbound > IP Groups**. See Forcepoint Email Security Administrator Help.

Other changes and enhancements

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

- Email-specific command-line interface (CLI) commands are added to the appliance CLI.

```
save configuration
show email counter
set mta open-relay-trusted-ip --status <enable|disable>
set mta reject-empty-pass-auth --status <enable|disable>
set mta sender-domain-validation --status <enable|disable|>
```

```
set mta tls-auth-only --status <enable|disable>
set mta tls-received-header --status <enable|disable>
set mta treat-blank-sender-as-outbound --status
<enable|disable>
set mta trusted-ip-bypass-blocklist --status
<enable|disable>
set mta tls-incoming --cipher <RC4|medium> --protocol
<sslv2|sslv3|tls1_0|tls1_1|tls1_2> --status <enable|disable>
set mta tls-outgoing --cipher <RC4|medium> --protocol
<sslv2|sslv3|tls1_0|tls1_1|tls1_2> --status <enable|disable>
```

See Forcepoint Appliances Command Line Interface.

Installation and upgrade

Release Notes | Forcepoint Email Security | Version 8.5 | Updated: 28-Feb-2018

Applies To:	Forcepoint Email Security v8.5

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 TRITON AP-EMAIL version 8.1, 8.2, or 8.3, or Forcepoint Email Security version 8.4, you can upgrade directly to Forcepoint Email Security version 8.5. 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 8.5:

Current Version	Upgrade Path	
7.8.4	8.4.0	8.5.0
8.0.x	8.3.0	8.5.0
8.1.x, 8.2.x, 8.3.x, 8.4.x	8.5.0	

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 8.5. To upgrade an X Series security blade, see the X Series upgrade guide.

Resolved and known issues

Release Notes | Forcepoint Email Security | Version 8.5 | Updated: 28-Feb-2018

Applies To:	Forcepoint Email Security v8.5

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 login screen.

© 2018 Forcepoint. This document may not, in whole or in part, be reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Forcepoint.

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.