v8.5.3 Release Notes for Forcepoint Email Security

Release Notes | Forcepoint Email Security | Version 8.5.3 | Updated: 30-Nov-2018

Applies To:	Forcepoint Email Security v8.5.3

Forcepoint Email Security version 8.5.3 is a feature and correction release that includes email protection improvements and fixes, some requested by our customers.

Forcepoint Email Security is an 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, an X Series appliance security blade, or 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.

Starting in version 8.5, Forcepoint Email Security can be deployed in Microsoft Azure, which provides the same features and protections as with an Email Security deployment on an appliance, but with the flexibility of virtualization. Version 8.5.3 adds support for deploying Forcepoint Security Manager in Azure, allowing your full email protection solution to reside within the Azure cloud environment.

Contents

Use these Release Notes to find information about version 8.5.3 Forcepoint Email Security. Version 8.5.3 and 8.6 Release Notes are also available for the following Forcepoint products:

- Forcepoint Security Manager
- Forcepoint Web Protection Solutions (including Content Gateway)
- Forcepoint Data Protection Solutions (version 8.6)
- Forcepoint Appliances

- Forcepoint Security Appliance Manager

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

New in version 8.5.3

Release Notes | Forcepoint Email Security | Version 8.5.3 | Updated: 30-Nov-2018

Applies To:	Forcepoint Email Security v8.5.3

Forcepoint Email Security version 8.5.3 includes the following new features:

- *Forcepoint Email Security and Forcepoint Security Manager deployed in Azure*
- *Support for FIPS 140-2 Level 1 certified cryptography*
- *Azure-related updates*

Forcepoint Email Security and Forcepoint Security Manager deployed in Azure

The Forcepoint Security Manager is the browser-based management console that provides a central, graphical interface to the general configuration, policy management, and reporting functions of your security software. Prior to this release, Forcepoint Security Manager was solely an on-premises solution.

Options added in version 8.5.3 for Microsoft Azure deployment allow Forcepoint Email Security appliances in addition to Forcepoint Security Manager and Email Log Server virtual machines to be deployed together in the cloud. Additional deployment options allow any of these elements to remain on-premises with connection to Azure. This solution will be available in the Azure Marketplace in early 2019. An existing on-premises Forcepoint Security Manager must be upgraded to version 8.5.3 before it can be migrated to Azure.

See Installing Forcepoint Email Security in Microsoft Azure for more information and installation procedures. See the Forcepoint Email Security in Azure Quick-Start Guide for a high-level overview of the installation procedure.

Support for FIPS 140-2 Level 1 certified cryptography

This version of Forcepoint Email Security updated support for the use of FIPS 140-2 Level 1 certified cryptography for the protection of sensitive data. FIPS-certified cryptography is enabled for all internal communication by default. A new command-line interface (CLI) command has been added to enable FIPS-certified

cryptography for third-party communications. See the Forcepoint Appliances CLI Guide for more information about CLI commands.

Use the following steps to enable FIPS-certified cryptography for communication between your email appliance and third-party applications or services.

1. Log in to the CLI and elevate to config mode:

   ```
   config
   ```

2. Log in to the email module CLI:

   ```
   login email
   ```

3. Enable FIPS mode:

   ```
   set openssl-fips --status enable
   ```

   To disable FIPS mode, use the command:

   ```
   set openssl-fips --status disable
   ```

   FIPS mode can only be disabled for third-party communications.

Azure-related updates

Azure Government

Version 8.5.3 adds support for deploying Forcepoint Email Security in an Azure Government cloud environment, bringing cloud flexibility to U.S. government agencies. Deployment in Azure Government requires Microsoft Office 365 Government. Azure Active Directory is not currently supported in Azure Government. See Installing Forcepoint Email Security in Microsoft Azure for more information and installation steps.

Network interface

The C interface is now used for all email traffic in Forcepoint Email Security in Azure. A combination of Azure and on-premises appliances can be installed in a deployment of Forcepoint Email Security in Azure.

Command-line interface

Certain command-line interface (CLI) commands were removed from the appliance CLI for Forcepoint Email Security in Azure. These commands are noted in the Forcepoint Appliances CLI Guide with the text “Not supported in Azure.”

IP address for Forcepoint Email Security Hybrid Module

If your Forcepoint Email Security in Azure deployment includes the Forcepoint Email Security Hybrid Module, it is necessary to use a static public IP address. This is a best

practice because a dynamic public IP address will change when you reboot your machine. See Email hybrid service configuration.

Installation and upgrade

Release Notes | Forcepoint Email Security | Version 8.5.3 | Updated: 30-Nov-2018

Requirements

On-premises Email Security is supported on the following platforms:

- Forcepoint V Series appliance (V20000, 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 system requirements and deployment information.
- Microsoft Azure

  Deploy a new Forcepoint Email Security solution from the Azure Marketplace, with or without the Forcepoint Security Manager. See Installing Forcepoint Email Security in Microsoft Azure.

The Forcepoint Security Manager and Email Log Server are hosted on a separate Windows Server machine or virtual machine in Azure. 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.

See Installing Forcepoint Email Security for installation procedures.

Supported operating systems

This version adds support for:

- Windows Server 2012
- Windows Server 2016
- CentOS 7.5 64-bit
- SQL Server 2017 (including Express)

This version ends support for:

- Windows Server 2008
- SQL Server 2008

See the Certified Product Matrix for information about all supported platforms.

Upgrade paths

If you are running TRITON AP-EMAIL version 8.2 or 8.3, or Forcepoint Email Security version 8.4 or 8.5, you can upgrade directly to Forcepoint Email Security version 8.5.3. You must perform intermediate upgrades if you are running any other previous version of Email Security Gateway or TRITON AP-EMAIL.

If you are running Forcepoint Email Security in Azure version 8.5, you can migrate configuration settings and data to a new installation of Forcepoint Email Security in Azure version 8.5.3. It is also possible to migrate from version 8.2, 8.3, 8.4, 8.5, and 8.5.3 on-premises to version 8.5.3 in Azure. All upgrades to version 8.5.3 in Azure require a migration.

If you are running AP-DATA Email Gateway version 8.3, it is not possible to upgrade to version 8.5.3; a new appliance must be installed.

See Upgrading Email Protection Solutions for:

- Detailed upgrade paths
- 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		Migration Required?
7.8.4	8.4.0	8.5.3	No
8.0.x	8.3.0	8.5.3	No
8.1.x	8.5.0	8.5.3	No

Current Version	Upgrade Path		Migration Required?
8.2.x, 8.3.x, 8.4.x, 8.5.x	8.5.3		No
8.2.x, 8.3.x, 8.4.x, 8.5.x	8.5.3 Azure		Yes

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 8.5.3 | Updated: 30-Nov-2018

Applies To:	Forcepoint Email Security v8.5.3

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.