v8.5.4 Release Notes for Forcepoint Email Security

Release Notes | Forcepoint Email Security | Version 8.5.4 | Updated: 08-Jun-2020

Applies To:	Forcepoint Email Security v8.5.4

Forcepoint Email Security version 8.5.4 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.

Forcepoint Email Security and Forcepoint Security Manager can additionally be deployed in Microsoft Azure, allowing your full email protection solution to reside within the Azure cloud environment. This provides the same features and protections as with an Email Security deployment on an appliance, but with the flexibility of virtualization.

Contents

Use these Release Notes to find information about version 8.5.4 Forcepoint Email Security. Release Notes are also available for the following Forcepoint products:

- Forcepoint Web Protection Solutions (including Content Gateway)
- Forcepoint Data Protection Solutions (version 8.7.1)
- Forcepoint Appliances
- Forcepoint Security Appliance Manager

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

New in version 8.5.4

Release Notes | Forcepoint Email Security | Version 8.5.4 | Updated: 08-Jun-2020

Applies To:	Forcepoint Email Security v8.5.4

Forcepoint Email Security version 8.5.4 includes the following updates:

Security enhancements

Security for all inter-modular communication for Forcepoint Email Security has been enhanced to operate via TLS v1.2 using secure ciphers by default.

For more information about adjusting TLS/SSL protocols for your components, see Security Enhancements for Forcepoint On-Premises Products.

Helpful features and improvements

The following new features have been added to improve the appearance and usability of Forcepoint Email Security:

- Message queue size limits during creation and modification are now based on available space on the database partition responsible for storing the queue files.
- An option was added for displaying images within Personal Email Manager and Forcepoint Secure Messaging portals.
- Log rotation rules have been added for many log files to help prevent disk space issues.
- The log export mechanism now considers all applied filters when exporting message logs.
- The maximum potential number of log database partitions has been greatly increased to approximately 2 billion.
- Audit logs for administrative changes to the Global Always Permit and Always Block Lists now show the modifications between each list.

New command-line interface commands

Two new command-line interface (CLI) commands were added in this release:

- A command that enables filter actions to use the True Source IP of a message in header modifications.
- A command that disables or enables native load balancing for Forcepoint Secure Messaging and Personal Email Manager components. This feature is intended for users utilizing an alternate load balancing solution.

See Forcepoint Appliances CLI Guide for more information.

Installation and upgrade

Release Notes | Forcepoint Email Security | Version 8.5.4 | Updated: 08-Jun-2020

Requirements

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

- Forcepoint V Series appliance: V20000 G1, V10000 G4 (R1 and R2) or V5000 G4 (R1 and R2)
- Forcepoint X Series modular chassis security blade: X10G G2 (R1 and R2)
- 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.

  Version 8.5.4 Email Virtual Appliances are certified and supported for VMware ESXi 7 / 6.7 / 6.5 / 6.0. A stable release of ESXi is recommended to avoid unexpected issues.

  

  Note

  For ESXi 7 and 6.7, users **must** use the v8.5.4 OVA file to create a new VM. Versions 8.5.3 and earlier will **not** deploy and are **not** supported on ESXi 7 or 6.7.

- 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 2019
- CentOS 7.7 64-bit
- SQL Server 2017 (including Express)

This version ends support for:

- Windows Server 2008
- SQL Server 2008, 2012, 2014

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

Upgrade paths

If you are running Forcepoint Email Security version 8.4 or 8.5, you can upgrade directly to Forcepoint Email Security version 8.5.4. 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 or 8.5.3, you can migrate configuration settings and data to a new installation of Forcepoint Email Security in Azure version 8.5.4. It is also possible to migrate from version 8.4, 8.5,

and 8.5.3 on-premises to version 8.5.4 in Azure. All upgrades to version 8.5.4 in Azure require a migration.

If you are running AP-DATA Email Gateway version 8.3, it is not possible to upgrade to version 8.5.4; 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 8.5.4:

Current version	First upgrade	Second upgrade	Final version	Migration required?
7.8.4	8.4.0		8.5.4	No
8.0.x	8.3.0	8.5.0	8.5.4	No
8.1.x, 8.2.x, 8.3.x	8.5.0		8.5.4	No
8.4.x, 8.5.x	8.5.4			No
8.4.x, 8.5.x	8.5.4 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 8.5.4 | Updated: 08-Jun-2020

Applies To:	Forcepoint Email Security v8.5.4

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 login screen.