v8.5 Release Notes for Forcepoint Email Security in Microsoft Azure

Release Notes | Forcepoint Email Security in Azure | Version 8.5 | Updated: 16-May-2018

Forcepoint Email Security in Azure is an enterprise and DLP solution that prevents malicious email threats from entering an organization's network and protects sensitive data from unauthorized email transmission.

Prior to this release, Forcepoint Email Security was solely an on-premises solution; now, Forcepoint Email Security version 8.5 can be deployed in a Microsoft Azure cloud environment.

Deploying Forcepoint Email Security in Azure requires a valid Forcepoint Email Security license and the installation of Forcepoint Email Security v8.5 and/or Forcepoint DLP Network v8.5.x.

Contents

Use these Release Notes to find information about version 8.5 Forcepoint Email Security in Azure. Release Notes are also available for version 8.5 Forcepoint Email Security on-premises:

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

Version 8.5 Release Notes are available for the following Forcepoint products:

- Forcepoint Security Manager
- Forcepoint Web Protection Solutions (including Content Gateway)
- Forcepoint Data Protection Solutions (version 8.5.1)
- Forcepoint Appliances
- Forcepoint Security Appliance Manager

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

New in version 8.5 in Azure

Network interface

The C interface is now used for all email traffic in Forcepoint Email Security in Azure. Only Azure appliances can be installed in a deployment of Forcepoint Email Security in Azure.

Command-line interface

Certain command-line interface (CLI) commands have been 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 in Azure | Version 8.5 | Updated: 16-May-2018

Requirements

Forcepoint Email Security in Azure is supported on the following platforms:

- Microsoft Azure

  Deploy a new Forcepoint Email Security solution from the Azure Marketplace. See Installing Forcepoint Email Security in Microsoft Azure.

The Forcepoint Security Manager and Email Log Server are hosted on a separate, on-premises Windows Server machine. (This server must be running an English language instance of Windows Server.) Forcepoint Email Security in Azure requires the Forcepoint Security Manager and Email Log Server to be installed on-premises.

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**
>
> Forcepoint Security Manager does not allow both on-premises and Azure appliances to be added on the Email Appliances page.

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 AP-DATA Email Gateway version 8.3 or Forcepoint Email Security in Azure v8.5, you can migrate configuration settings and data to a new installation of Forcepoint Email Security in Azure version 8.5.

See Upgrading to Forcepoint Email Security v8.5 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 in Azure version 8.5:

Current Version	Upgrade Path	Migration Required?
8.3 Azure	8.5 Azure	Yes
8.5 Azure	8.5 Azure	Yes

Known issues

Release Notes | Forcepoint Email Security in Azure | Version 8.5 | Updated: 16-May-2018

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

Published 2018

Printed in the United States of America

Every effort has been made to ensure the accuracy of this manual. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Copyrights and Trademarks