

Installing Forcepoint Email Security

Installation | Forcepoint Email Security | Version 8.5.x

Forcepoint Email Security is a cloud or 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 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, or in a Microsoft Azure cloud environment.

See the following topics for related Forcepoint Email Security deployment and configuration information.

- [Forcepoint Appliances Getting Started Guide](#)
- [System requirements](#)
- [Single-appliance deployments](#)
- [Multiple-appliance deployments](#)
- [Initial configuration](#)
- [Installing Forcepoint Email Security in Microsoft Azure](#)

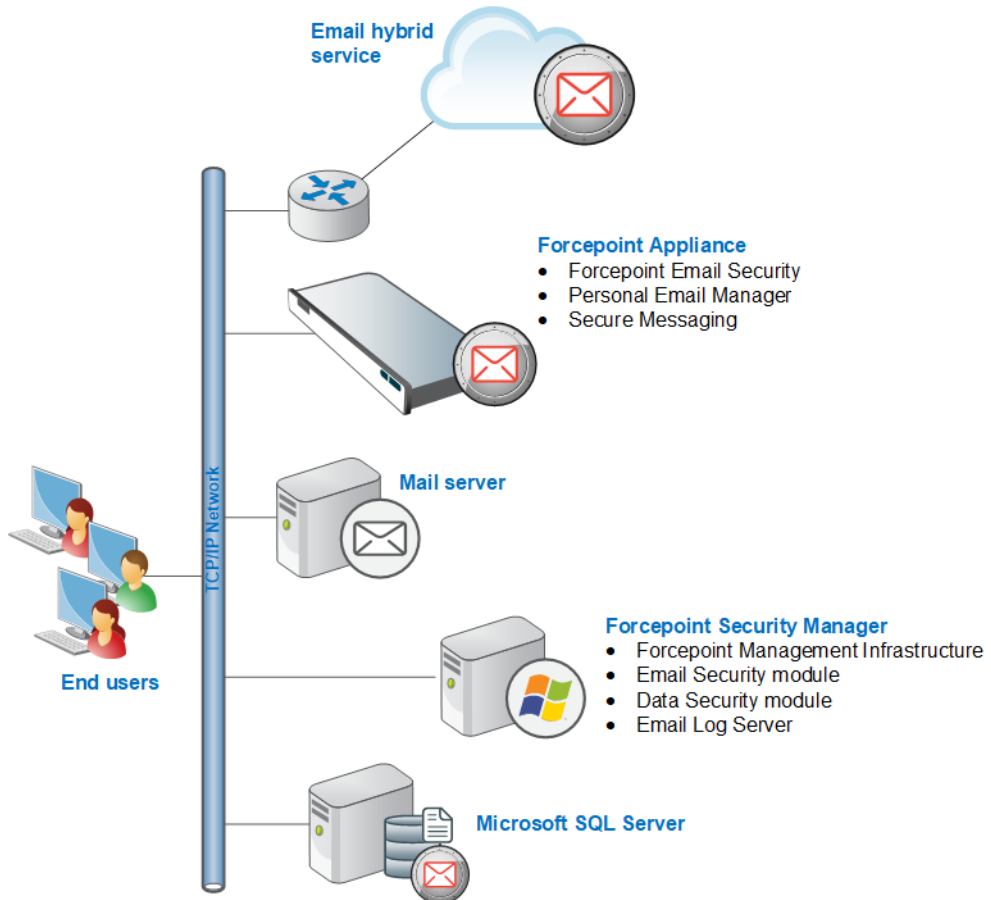
Contents

- *Forcepoint Email Security: Brief overview*
- *Installation steps for email protection solutions*

Forcepoint Email Security: Brief overview

The following illustration is a high-level diagram of a basic on-premises, appliance-based deployment of Forcepoint Email Security that includes the Forcepoint Email Security Hybrid Module. The Forcepoint Security Manager must also include the Data Security module (Forcepoint DLP) for access to email DLP functions.

This illustration is intended to show the general distribution of components and does not include network details (such as segmenting, firewalls, routing, or switching).



Installation steps for email protection solutions

Complete the following procedures in the order in which they are listed. These steps are needed when installing an on-premises Forcepoint Email Security solution (on a V Series, X Series, or virtual appliance).

- Deployment in a Microsoft Azure environment includes options for installing Forcepoint Email Security appliances and Forcepoint Security Manager and SQL Server entirely in Azure, or combining certain on-premises and Azure components. See [Installing Forcepoint Email Security in Microsoft Azure](#) for all deployment options and installation instructions.



Important

All components in the deployment, including those running off-appliance, must run the same version of Forcepoint software.

1. Ensure that Microsoft SQL Server is installed and running in your network (see [Obtaining Microsoft SQL Server](#) and [Installing with SQL Server](#)).

Refer to the [Certified Product Matrix](#) for information about supported versions of SQL Server. Forcepoint Email Security version 8.5.3 is only certified with the following versions of SQL Server: 2012 SP3, 2012 SP4, 2016 SP1, 2017 Express, and 2017 Windows.

If you intend to use SQL Server Express (installed using the Forcepoint Security Installer), skip this step. You will install the database engine with Forcepoint Security Manager components. Keep in mind that the performance limitations of SQL Server Express make it more appropriate for evaluation environments or small organizations than for larger deployments.

Additional configuration for your Log Database can be completed using Microsoft SQL Server tools. It is recommended to encrypt the database connection as a best practice. See [Microsoft documentation](#) for more information on securing SQL Server, and [Administering Forcepoint Databases](#) for more information about configuring the Log Database.

2. Install and configure your Forcepoint appliances. See [Forcepoint Appliances Getting Started Guide](#) for detailed setup and configuration instructions.

Continue with the next step if you have already completed the appliance setup steps.

3. Install Email Log Server.

When deploying Email Log Server and Forcepoint Email Security on the same machine, both components are installed together. When deploying Email Log Server and Forcepoint Email Security on separate machines, it is recommended to install Email Log Server before installing other Forcepoint Email Security components.

See [Installing email protection components](#).

4. Install Forcepoint Management Infrastructure, the Data Security module (for email DLP functions), and the Email Security module.

See [Creating a Forcepoint Management Server](#).

5. Install all other off-appliance product components.



Important

To ensure that you install all required components of your email protection solution, including data loss prevention, we recommend that you select Forcepoint Email Security on the Installation Type page of the Forcepoint Security Installer, rather than performing a Custom installation of the product.

When you select Forcepoint Email Security on this page, Forcepoint DLP is automatically selected as well. Data loss prevention (DLP) functions are installed along with email protection functions.

A Custom installation does not automatically install Forcepoint DLP with Forcepoint Email Security.

© 2018 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.