Installing Forcepoint Email Security

Installation | Forcepoint Email Security | Version 8.4

Forcepoint Email Security is a Forcepoint 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.

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

- System requirements
- Single-appliance deployments
- Multiple-appliance deployments
- Initial configuration

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 appliance-based deployment of Forcepoint Email Security, which 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.

Note that this illustration is intended to show the general distribution of components and does not include network details (such as segmenting, firewalls, routing, switching, and so forth).
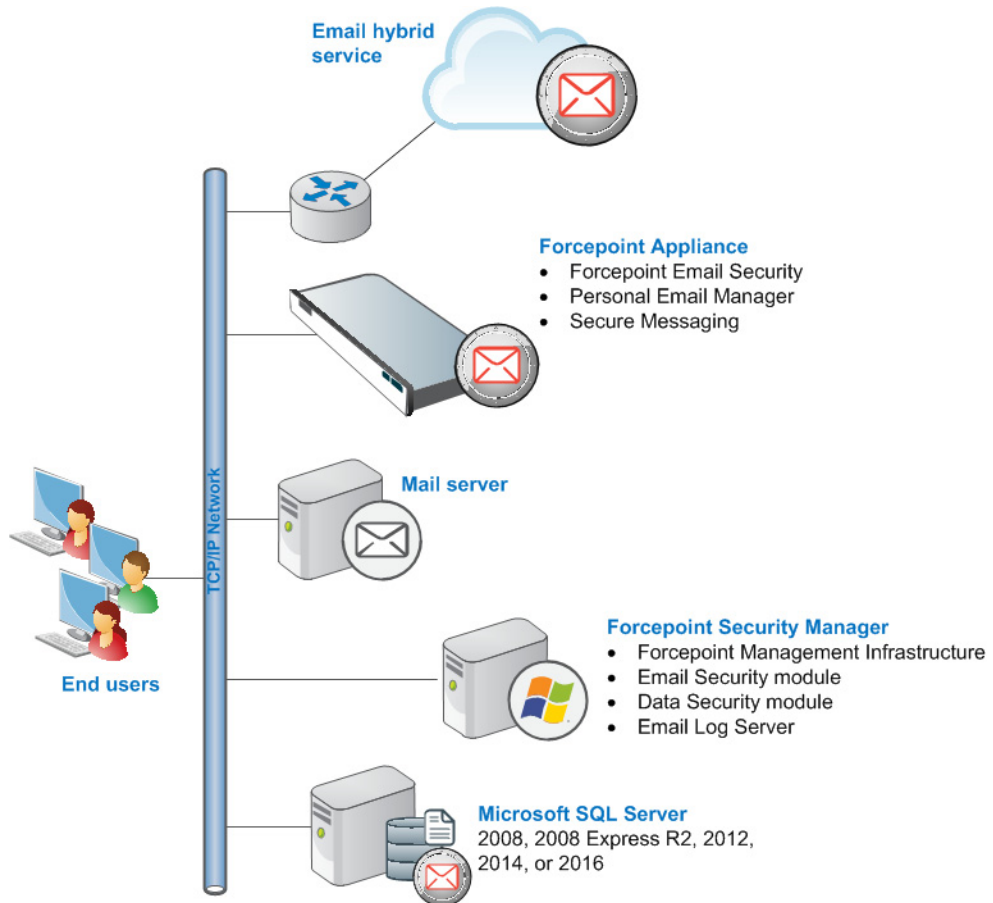
Installation steps for email protection solutions

Complete the following procedures in the order in which they are listed.

1. Make sure that Microsoft SQL Server is installed and running in your network (see Obtaining Microsoft SQL Server and Installing with SQL Server).

   If you intend to use SQL Server 2008 R2 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.

2. Install and configure your Forcepoint appliances. See Forcepoint Appliances Getting Started Guide for detailed set-up and configuration instructions.

   > **Note**
   >
   > If you have already completed the appliance set-up steps, continue with the next step.

3. Install Email Log Server.

   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](#).

> **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 functions are installed along with email protection functions.
>
> A Custom installation does not automatically install Forcepoint DLP with Forcepoint Email Security.

> **Important**
>
> On the Select Components screen in the Forcepoint Security Installer, ensure that the **Forcepoint Email Security** option is selected. This option is required if you are running your email protection system on a V or X Series appliance or an on-premises virtual appliance.
>
> The **Forcepoint DLP Cloud Email** option applies to a cloud-hosted virtual appliance running with Forcepoint DLP. **This product component is not supported in version 8.4.** If you want to install and use this product, you must use version 8.3. See the topic titled "Email Gateway for Microsoft Office 365" in the version 8.3 TRITON AP-DATA Installation Guide for details about this product feature.