Forcepoint

Email Security

8.5.x

Installation Guide

Revision A

Contents

Introduction

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.

Forcepoint Email Security is available on Forcepoint V Series and X Series appliance security blades, and on virtual appliances, which can be downloaded from the Forcepoint Customer Hub downloads menu. You may also deploy Forcepoint Email Security in a Microsoft Azure cloud environment. 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.

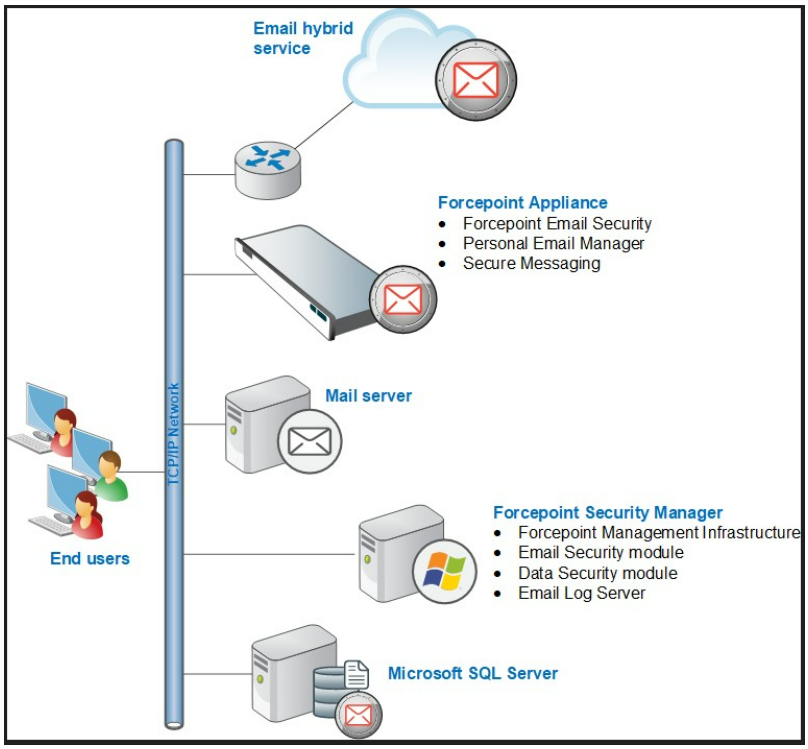
See the following topics for related Forcepoint Email Security deployment and configuration information.

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

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.

Steps

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

   In certain versions, you may have the option to install SQL Server Express using the Forcepoint Security Installer. If you intend to use SQL Server Express, 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 setup and configuration instructions.

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

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 (Windows only), the Data Security module (for email DLP functions), and the Email Security module. You must install the Data Security module in addition to the Email Security module in order to access and configure email DLP functions in Forcepoint Email Security Solutions. 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.

Initial configuration for all security modules

Steps

1) Some of the ports required during installation are no longer needed when installation is complete. For information about the ports required for component communication, as well as details about which components need Internet access, see Default ports for on-premises Forcepoint security solutions.

2) To avoid performance issues, exclude certain folders and files from antivirus scans. See Excluding Forcepoint files from antivirus scans.

3) If administrators use Internet Explorer to access the Forcepoint Security Manager, make sure that Enhanced Security Configuration is disabled on their machines.

   In Windows Servers:

   a) Open the **Server Manager**.

   b) Under **Server Summary**, in the **Security Information** section, click **Configure IE ESC**.

   c) In the **Internet Explorer Enhanced Security Configuration** dialog box, under **Administrators**, select the **Off** radio button, and then click **OK**.
   Administrators may also need to restore default settings in their browser in order for the Forcepoint Security Manager to display properly in Internet Explorer. To do this, in Internet Explorer go to **Tools** > **Internet Options** and select the **Advanced**tab, then click **Reset**. When prompted, click **Reset** again.

   If you are installing version 8.5.4 or 8.5.5: during installation, ensure that you use a hostname or fully qualified domain name (FQDN) for your Email Log Database that matches the Common Name (CN) field on the certificate that SQL Server is using.

4) Use a supported browser (see System requirements for this version) to launch the Forcepoint Security Manager and log on using the default account:

   a) Navigate to the following URL:
   `https://<IP_address>:9443`

   Here, <IP_address> is the IP address of the Forcepoint management server.

   b) Log on as the default admin account, using the password set during installation.

   c) (Version 8.5.4 and v8.5.5 only) During the initial configuration wizard, ensure that you use a hostname or FQDN for your Email Log Database that matches the CN field on the certificate that SQL Server is using.

5) Enter your subscription key or keys. At first startup:

   - The Web Security module of the Security Manager prompts for a subscription key in the Initial Setup Checklist. If you have a solution that includes Content Gateway, the key you enter is automatically applied to Content Gateway, as well.
   - The Data Security module of the Security Manager displays the subscription key page. See the “Initial Setup” section of the Forcepoint DLP Administrator Help for more information.
   - The Email Security module of the Security Manager prompts for a subscription key. Enter the subscription key when prompted, or enter later on the **Settings** > **General** > **Subscription** page.

6) If you did not provide SMTP server details during installation, use the **Global Settings** > **General** > **Notifications** page to specify the SMTP server used to enable administrator password reset functionality and account change notifications.

   To access the **Global Settings** page, click the gear-shaped icon in the **Security Manager** toolbar. See the *Forcepoint Security Manager Help* for more information.

7) If SQL Server Express was installed, verify that SQL Server Browser service is running and that TCP/IP is enabled.

   a) Launch **SQL Server Configuration Manager**.

   b) In the tree pane, select **SQL Server Service**.

   c) In the **properties** pane, make sure **SQL Server Browser** is running and **start mode** is **automatic**. Right-click to start the service or change its start mode.

   d) In the tree pane, select **SQL Server Network Configuration** > **Protocols for** <instance name>, where <instance name> is the default instance or TRITONSQL2K8R2X (or other instance name you specified).

   e) In the **properties** pane, make sure **TCP/IP** is enabled. If not, right-click **TCP/IP** and enable it.

Initial configuration for Forcepoint Email Security

The first time you access the Email Security module of Forcepoint Security Manager, you are prompted for your subscription key. Then, you are asked if you want to use the First-Time Configuration Wizard. This wizard guides you through the process of entering some essential configuration settings. It is strongly recommended you use this wizard. See the Forcepoint Email Security Administrator Help for more information about the wizard.

Important

The configuration wizard is offered only once, at initial Email Security module startup. If you choose not to use the wizard, it will no longer be available. All settings configured in the wizard can be configured in the Email Security module individually. The wizard simply offers a more convenient way to enter some initial settings.

See the Getting started section in the Forcepoint Email Security Administrator Help for information on initial configuration in the following areas:

- First-time Configuration Wizard, for establishing
  - An initial mail route for a protected domain
  - Trusted IP addresses for which some inbound email analysis is not performed
  - Email Log Server IP address and port
  - System notification email address.
- Forcepoint DLP registration, to allow the use of email data loss prevention (DLP) policy options.
- Forcepoint URL database download scheduling, to manage message analysis database updates.

For help with the following Email Security module settings, see the Configuring system settings section in the Administrator Help:

- Delegated administrator management, to modify administrator roles established in the Forcepoint Security Manager.
- System settings, to establish system preferences like the SMTP greeting and system notification email address.
- Appliance management, for administering all the appliances in your email protection system.

- User directory creation and management.
- Protected domain and trusted IP address lists, to designate all the domains that you want protected and the IP addresses whose mail can bypass some email analysis.
- User authentication and recipient validation options.
- Transport Layer Security (TLS) certificate handling, to provide an extra layer of security for email communications.
- Trusted CA certificate importing.
- Email Security module backup and restore functions, to preserve important configuration files, including your appliances list, administrator settings, and report templates.
- System alerts, to configure delivery methods for distributing various email system health alerts.

If your subscription includes the Forcepoint Email Security Hybrid Module, you need to register with the email hybrid service. See the Registering for the hybrid service topic in the Forcepoint Email Security Administrator Help for descriptions of email hybrid service registration.

After you have registered with the email hybrid service, you can configure Email Hybrid Service Log properties and view the Email Hybrid Service Log. See the Administrator Help for details.

Published 02 November 2022