FORCEPOINT
POWERED BY Raytheon

Installation Guide

Forcepoint Web Security
Forcepoint DLP
Forcepoint Email Security

v8.5.x, v8.6.x, v8.7.x

Published 2020

Last modified 08-Jun-2020

Contents

1 Preparing for Forcepoint Deployment

Applies to:
• Forcepoint Web Security and Forcepoint URL Filtering, v8.5.x • Forcepoint DLP, v8.5.1, v8.6.x, v8.7.x • Forcepoint Email Security, v8.5.x • Forcepoint appliances, v8.5.x

Note

- Forcepoint DLP v8.7.1 is supported with Forcepoint Web and Email Security v8.5.4.
- Forcepoint DLP v8.6 and v8.7 are supported with Forcepoint Web and Email Security v8.5.3.
- Forcepoint DLP v8.5.1 is supported with Forcepoint Web and Email Security v8.5.0.
- Forcepoint DLP v8.5.0 and v8.5.2 are stand-alone versions of that product and cannot be integrated with other Forcepoint products.

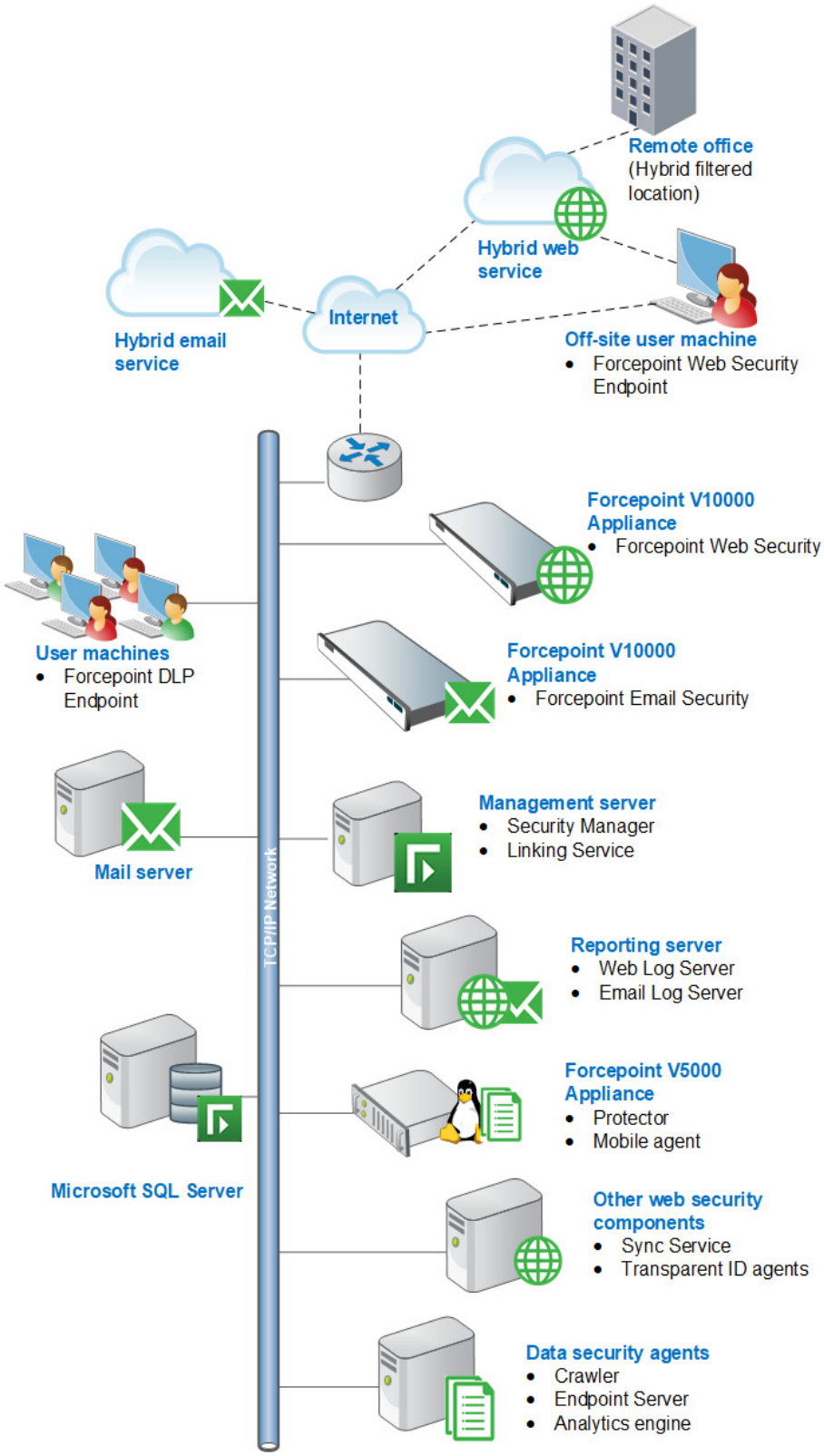
A full Forcepoint deployment includes Forcepoint Web Security with optional Hybrid Module, Forcepoint DLP Network, Forcepoint DLP Endpoint, and Forcepoint Email Security with optional Hybrid Module.

- Forcepoint Security Manager, the management interface for Web, Email, and Data products, resides on a Windows server.
- Forcepoint Web Security may be deployed on Forcepoint appliances, dedicated Windows or Linux servers, or a combination of platforms. This guide covers the following configuration:
  - The policy source (the standalone or primary Policy Broker and central Policy Server) resides separate from the management server, on another Windows or Linux server, or on a Forcepoint appliance.

    While this is not required and Policy Broker and Policy Server can reside on the management server machine, this configuration is recommended for full Forcepoint deployments to ensure optimum performance.

    - Web Log Server resides separate from the management server on a dedicated Windows machine.
- Forcepoint DLP runs on Windows servers, optional protector appliances, and elsewhere in the network.
- Forcepoint Email Security enforcement components reside only on Forcepoint appliances. Management and reporting components reside on Windows servers.

Following is a diagram of a basic appliance-based deployment.



Installation overview

Before beginning the installation process, refer to the Deployment and Installation Center for complete system requirements and required system preparation steps.

The process of installing Forcepoint components is as follows:

1. Ensure that a supported version of Microsoft SQL Server (not Express) is installed and running in your network.
2. The machine with the standalone or primary Policy Broker and its companion Policy Server instance must be configured first. These web components must be running before any other web components can be installed:
   - If Policy Broker will reside on a full policy source appliance, configure that appliance first.
   - If Policy Broker and Policy Server will reside on a Windows or Linux server that is not the management server, install these components **before** the management server installation. Install the software version if you plan to use Policy Broker replication.

     It is also recommended that you install an instance of Filtering Service on this machine.

   See *Installing the Forcepoint Web Security policy source*, page 5.
3. Install and run the **firstboot** script on your appliances.
4. Install Forcepoint management and core Forcepoint DLP components on a Windows Server machine.

   On the **Installation Type** screen, select all three modules (**Web**, **Data**, and **Email**) under the Security Manager.

   See *Creating the Management Server*, page 6
5. Install Web and Email Log Server.

   In deployments that include the Forcepoint Web Security Hybrid Module, Sync Service is typically installed with Web Log Server.

   See *Install Web Log Server*, page 19, and *Install Email Log Server*, page 32.
6. Install additional components (such as web transparent identification agents or Forcepoint DLP agents) as needed.

   See *Installing web components*, page 19, and *Installing data components*, page 28.

After completing the installation process, follow the initial configuration steps in the Deployment and Installation Center.

2 Installing Forcepoint Management Components

This chapter includes instructions for:

Installing the Forcepoint Web Security policy source

This section describes the steps required to install the primary or standalone Policy Broker and the associated Policy Server instance on a Windows machine. If Policy Broker will reside on a full policy source appliance, see Forcepoint Appliances Getting Started.

As a best practice, install an instance of Filtering Service on the Policy Broker machine (policy source). If no Filtering Service resides on the policy source, the first Filtering Service instance installed must connect to the central Policy Server on the policy source. See *Install an instance of Filtering Service*, page 23.

Other components may optionally reside on the policy source, such as User Service, Usage Monitor, and Directory Agent.

On the machine that will host the policy source:

1. Ensure you have prepared the machine as described in system preparation steps.
2. Log on to the machine with local admin privileges.
3. Download or copy the Forcepoint Security Installer (the Windows installer) to this machine. The installer is available from My Account and the installer file is **Forcepoint85xSetup.exe**.
4. Right-click **Forcepoint85xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
5. On the Welcome screen, click **Start**.

   The Installer Dashboard stays on-screen during installation. Various subinstallers and dialog boxes are displayed over it.
6. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
7. On the Installation Type screen, select **Custom**.

8. On the Custom Installation dashboard, click the Forcepoint Web Security or Web Filter and Security **Install** link.
9. On the Select Components screen, select **Policy Broker**, **Policy Server**, and **Filtering Service**. These components must be installed in the order listed, and before any other web components. (If you select all 3 at the same time, they are installed in the correct order.)
10. On the Policy Broker Replication screen, indicate which Policy Broker mode to use.
    - Select **Standalone** if this will be the only Policy Broker instance in your deployment.
    - Select **Primary**, then create a **Synchronization password** if you will later install additional, replica instances of Policy Broker.

    Important

    Be sure to record the synchronization password. You must provide this password each time you create a Policy Broker replica.

11. On the Integration Option screen, select **Install Forcepoint Web Security to connect to Content Gateway**, then click **Next**.
12. If prompted to install the Microsoft SQL Server Native Client and related tools, follow the on-screen prompts to complete the process.
13. On the Pre-Installation Summary screen, verify the information shown, then click **Next**.

    A progress screen is displayed. Wait for installation to complete.

Creating the Management Server

The installation procedure for the management server includes the following steps:

Ensure you have prepared the machine as described in system preparation steps.

Step 1: Download the Forcepoint Security Installer

1. Log on to the machine with local admin privileges.

2. Download or copy the Forcepoint Security Installer (the Windows installer) to this machine. The installer is available from My Account and the installer file is **Forcepoint85xSetup.exe**.

Continue with *Step 2: Select management components*.

Step 2: Select management components

1. Right-click **Forcepoint85xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
2. On the Welcome screen, click **Start**.
3. On the Subscription Agreement screen, select **I accept this agreement** and then click **Next**.
4. On the Installation Type screen, select **Forcepoint Security Manager**, then use the check boxes to select management modules for one or more security products (Forcepoint Web Security or Forcepoint URL Filtering, Forcepoint DLP, or Forcepoint Email Security).

   When you select the management module for Forcepoint Email Security, the module for Forcepoint DLP is also selected. This is required to enable the email DLP features included with Forcepoint Email Security.

   Important

   A Forcepoint Email Security appliance must already be running in order to install the email security management components. The appliance C interface IP address must be entered during installation.

   The appliance P1 (and P2, if used) interface must also be configured via command-line interface (CLI) before Forcepoint Email Security management components can be installed.

5. When Forcepoint DLP management components are selected on the Installation Type screen, but Forcepoint Email Security components are not, a second Installation Type screen appears. Do **NOT** mark the check box. Click **Next**.
6. On the Summary screen, click **Next** to continue the installation.

   Forcepoint Infrastructure Setup launches.

Continue with *Step 3: Install the Forcepoint Infrastructure*.

Step 3: Install the Forcepoint Infrastructure

The Forcepoint Infrastructure includes data storage and common components for the management modules of the Security Manager.

1. On the Forcepoint Infrastructure Setup Welcome screen, click **Next**.

2. On the Installation Directory screen, specify the location where you want Forcepoint Infrastructure to be installed and then click **Next**.

   Important
   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   - To accept the default location (recommended), simply click **Next**.
   - To specify a different location, click **Browse**.

3. On the SQL Server screen, specify the location of your database engine and the type of authentication to use for the connection. Also specify whether to encrypt communication with the database.

   The information entered here is also used by the Web, Data, and Email component installers, by default. The Web component installer can be used to specify a different database; the Data and Email component installers cannot.

   Select **Use the SQL Server database installed on another machine** to specify the location and connection credentials for a database server located elsewhere in the network.

   Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any.

   - If you are using a named instance, the instance must already exist.
   - If you are using SQL Server clustering, enter the virtual IP address of the cluster. (Clustering is only supported with Forcepoint Email Security and Forcepoint Web Security.)

   Also provide the **Port** used to connect to the database (1433, by default).

   After entering the above information, specify an authentication method and account information:

   - Select the **Authentication** method to use for database connections: **SQL Server Authentication** (to use a SQL Server account) or **Windows Authentication** (to use a Windows trusted connection).

     Next, provide the **User Name** or **Account** and its **Password**. This account must be configured to have system administrator rights in SQL Server. If you are using Windows authentication with Forcepoint DLP, Forcepoint Web Security or Forcepoint Email Security, use an account with the sysadmin role. If you are using SQL Server Express, **sa** (the default system administrator account) is automatically specified (this is the default system administrator account).

     Note
     The system administrator account password cannot contain single or double quotes.

     For more information about permissions required for the connection account, see Installing with SQL Server.

If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Web Security module of the Forcepoint Security Manager. See How do I configure services to use a trusted connection?

When you click **Next**, connection to the database engine is verified. If the connection test is successful, the next installer screen appears.

If the test is unsuccessful, the following message appears:

Unable to connect to SQL
Make sure the SQL Server you specified is currently running. If it is running, verify the access credentials you supplied.

Click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

4. On the Server & Credentials screen, select the IP address of this machine and specify network credentials to be used by the Security Manager.
   - Select an **IP address** for this machine. If this machine has a single network interface card (NIC), only one address is listed.

     Use the IP address selected to access the Security Manager (via Web browser). Also specify this IP address to any component that needs to connect to the management server.
   - Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and the Security Manager. The server/host name cannot exceed 15 characters.
   - Specify the **User name** of the account to be used by the Security Manager.
   - Enter the **Password** for the specified account.
5. On the Administrator Account screen, enter an email address and password for the default the Security Manager administration account: **admin**. The password must:
   - Be at least 8 characters
   - Contain upper case characters
   - Contain lower case characters
   - Contain numbers
   - Contain non-alphanumeric characters
6. When you are finished, click **Next**.

   System notification and password reset information is sent to the email address specified (once SMTP configuration is done; see next step).

   You must use a strong password, as described on the screen.

7. On the Email Settings screen, enter information about the SMTP server to be used for system notifications and then click **Next**. You can also configure these settings after installation in Forcepoint Security Manager.

   Important
   If you do not configure an SMTP server now and you lose the **admin** account password (set on previous screen) before the setup is done in the Security Manager, the "Forgot my password" link on the logon page does not provide password recovery information. SMTP server configuration must be completed before password recovery email can be sent.

   - **IP address or hostname**: IP address or host name of the SMTP server through which email alerts should be sent. In most cases, the default **Port** (25) should be used. If the specified SMTP server is configured to use a different port, enter it here.
   - **Sender email address**: Originator email address appearing in notification email.
   - **Sender name**: Optional descriptive name that can appear in notification email. This is can help recipients identify this as a notification email from the Security Manager.

8. On the Pre-Installation Summary screen, verify the information and then click **Next** to begin the installation.
9. The Installation screen appears. Wait until all files have been installed.

   If an "Error 1920" error appears, check whether port 9443 is already in use on this machine.

   If port 9443 is in use, release it and then click **Retry** to continue installation.
10. On the Installation Complete screen, click **Finish**.

After the **Finish** Forcepoint Infrastructure Setup completes, component installers for each selected management module are launched in succession.

Continue with the appropriate next step. If all management modules are selected, their component installers open in the order listed.

- *Step 4: Install Web management components*
- *Step 5: Install Data management components*
- *Step 6: Install Email management components*

Step 4: Install Web management components

In the recommended software installation for Forcepoint web, data, and email deployments, the management server hosts management components while the primary or standalone Policy Broker and central Policy Server may reside on a separate machine (the policy source machine), as described in *Installing the*

Forcepoint Web Security policy source.

Note that if Linking Service will run on the management server, the Filtering Service that connects to the central Policy Server must be installed and running before Linking Service is installed.

Important

If you have a **full policy source** Web appliance, Policy Broker, Policy Server, and Filtering Service, among other components, reside there.

Follow these instructions to install Forcepoint Web Security management components on a management server.

1. In the Select Components screen, select the components you want to install on this machine and then click **Next**.

   The following Forcepoint Web Security components are available for installation on a management server:

   - **Security Manager (Web module)** must be installed. It is selected by default and cannot be deselected. The other components shown are optional for this machine.
   - **Sync Service** typically does not run on the management server. It is a required component if you have the Web Hybrid module, but it typically resides on the Web Log Server machine.

Note

Although Sync Service and the Web Log Server may be installed on the management server, they consume considerable system resources. For Forcepoint Enterprise deployments, it is recommended to install these components on another machine. See *Install Web Log Server*, page 19.

- Select **Linking Service** if your subscription includes both a Web and Data solution.

  Important

  Filtering Service must be installed in your network before you install Linking Service. In an appliance-based deployment, Filtering Service is installed on all Web appliances (full policy source, user directory and filtering, and filtering only). In a software-based deployment, it is recommended that you install Filtering Service with Policy Broker and Policy Server on another separate machine from the management server, as Filtering Service can consume considerable system resources and may have a performance impact on the management server. Large or distributed environments may include multiple Filtering Service instances.

  You can return to the management server at a later time and install Linking Service if required.

- **Real-Time Monitor** is optional. It is typically installed on the management server, but can be located elsewhere. Install no more than one instance of Real-Time Monitor for a Policy Server instance. In most cases, only one instance of Real-Time Monitor is required per deployment.
- **Policy Broker and Policy Server** are typically already installed on a separate machine, and should not be selected again.

Policy Server Connection screen

If Policy Server does not reside on the management server, on the Policy Server Connection screen, enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.

The Policy Broker communication port must be in the range 1024-65535. During installation, Policy Broker may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Broker instances.) To verify the port:

1. Navigate to the **bin** directory on the Policy Server machine (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/, by default).
2. Open the **BrokerService.cfg** file in a text editor.
3. Locate the **listen_port** value.
4. When you are finished, close the file without saving. Do **not** modify the file.

Policy Broker Connection screen

If Policy Broker does not reside on the management server, and you selected Sync Service for installation, the **Policy Broker Connection** screen appears. Enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.

The Policy Broker communication port must be in the range 1024-65535. During installation, Policy Broker may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Broker instances.) To verify the port:

1. Navigate to the **bin** directory on the Policy Server machine (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/, by default).
2. Open the **BrokerService.cfg** file in a text editor.
3. Locate the **listen_port** value.
4. When you are finished, close the file without saving. Do **not** modify the file.

Select Policy Broker Screen

This screen appears if Policy Server is selected for installation, but Policy Broker is not.

Policy Server can be connected to a primary, standalone, or replica Policy Broker.

A list of Policy Broker instances to which this Policy Server can be connected is provided. The list is based on the Policy Broker IP address entered on the Policy Broker Connection screen.

- Select the Policy Broker instance that the Policy Server being installed should connect to.
- The primary or standalone Policy Broker is selected by default.

If Policy Broker is not installed anywhere in your network, you must install it before **any other** web protection component.

Filtering Service Communication screen

If you select Linking Service for installation, the **Filtering Service Communication** screen appears.

Enter the IP address of the Filtering Service machine and the port Filtering Service uses to communicate with Network Agent, Content Gateway, or third-party integration products (default is 15868).

- In an appliance-based deployment, Filtering Service is installed on all Web appliances (full policy source, user directory and filtering, and filtering only).
  - Enter the IP address of the appliance's C interface and use the default port (15868).

- If you have multiple appliances, be sure to select the one you want Network Agent, the filtering plug-in, or Linking Service to use.

- The Filtering Service communication port must be in the range 1024-65535. During installation, Filtering Service may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Filtering Service instances.) To verify the port:

  a. Navigate to the **bin** directory on the Policy Server machine (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/, by default).

  b. Open the **eimserver.ini** file in a text editor.

  c. Locate the **WebsenseServerPort** value.

  d. When you are finished, close the file without saving. Do **not** modify the file.

If Filtering Service is not installed anywhere in your network, you must install it before installing Network Agent, a filtering plug-in, or Linking Service.

Completing the installation

1. On the **Pre-Installation Summary** screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.

2. Click **Next** to start the installation. The **Installing Forcepoint** progress screen is displayed. Wait for installation to complete.

3. On the **Installation Complete** screen, click **Next**.

4. If you have not selected any other Security Manager module, you are returned to the Modify Installation dashboard. Installation is complete.

   If you have chosen to install other Security Manager modules, you are returned to the Installer Dashboard and the next component installer is launched.

Step 5: Install Data management components

Follow these instructions to install Forcepoint DLP management components on the management server. This includes:

- A Forcepoint DLP policy engine
- Primary fingerprint repository
- Forensics repository
- Endpoint server

After installing the Forcepoint Infrastructure and (if needed) the Web Security management components, install the

1. When the Forcepoint DLP installer is launched, a Welcome screen appears. Click **Next** to begin Forcepoint DLP installation.

   Note

   Both .NET 3.5 and 4.5 are required for the Forcepoint Infrastructure.

   - For Windows Server 2008 R2 SP1, you can add .NET 3.5 from Server Manager\Features. Usually this feature is **On** by default. You must download .NET 4.5 from the Microsoft site, https://msdn.microsoft.com/en-us/library/5a4x27ek%28v=vs.110%29.aspx?f=255&MSPPError=-2147217396.
   - For Windows server 2012/2012 R2, you can both .NET 3.5 and .NET 4.5 from Server Manager\Features. Usually v3.5 is **Off** by default and v4.5 is **On** by default. Turn them both on.

2. In the Select Components screen, click **Next** to accept the default selections.

   Note

   If there is insufficient RAM on this machine for Management Server components, a message appears. Click **OK** to dismiss the message. You are allowed to proceed with the installation. However, it is a best practice to install only if you have sufficient RAM.

3. If prompted, click **OK** to indicate that services such as ASP.NET and SMTP will be enabled.

   Required Windows components will be installed. You may need access to the operating system installation disc or image.

4. On the Fingerprinting Database screen, accept the default location or use the **Browse** button to specify a different location.

   Note that you can install the Fingerprinting database to a local path only.

5. If your SQL Server database is on a remote machine, you are prompted for the name of a temporary folder. This screen defines where Forcepoint DLP should store temporary files during archive processing as well as system backup and restore.

   Archiving lets you manage the size of your incident database and optimize performance. Backup lets you safeguard your policies, forensics, configuration, data, fingerprints, encryption keys, and more.

   If you do not plan to archive incidents or perform system backup and restore, you do not need to fill out this screen.

Before proceeding, create a folder in a location that both the database and management server can access. (The folder must exist before you click **Next**.) On average, this folder will hold 10 GB of data, so choose a location that can accommodate this.

On the **Temporary Folder Location** screen, complete the fields as follows:

- **Enable incident archiving and system backup**: Check this box if you plan to archive old or aging incidents and perform system backup or restore. This box does not appear when you run the installer in Modify mode and perform a disaster recovery restore operation.
- **From SQL Server**: Enter the path that the SQL Server should use to access the temporary folder. For best practice, it should be a remote UNC path, but local and shared network paths are supported. For example: c:\folder or \\10.2.1.1.\folder. Make sure the account used to run SQL has write access to this folder.
- **From Management Server**: Enter the UNC path the management server should use to access the temporary folder. For example: \\10.2.1.1.\folder. Enter a user name and password for a user who is authorized to access this location.

To grant this permission, issue the following T-SQL commands on the SQL Server instance:

```
USE master
GRANT BACKUP DATABASE TO <user>
GO
```

After installation of Forcepoint DLP components, you can revoke this permission:

```
USE master
REVOKE BACKUP DATABASE TO <user>
GO
```

6. In the Installation Confirmation screen, click **Install** to begin installation of Forcepoint DLP components.
7. If a message about port 80 or port 443 is displayed, click **Yes** to continue the installation.

   Clicking **No** cancels the installation.
8. The Installation progress screen appears. Wait for the installation to complete.
9. When the Installation Complete screen appears, click **Finish** to close the Forcepoint DLP installer.
10. If no other Security Manager module is chosen for installation, you are returned to the Modify Installation dashboard. Installation is complete.

    Otherwise, you are returned to the Installer Dashboard and the next component installer is launched.

For information on installing a supplemental Forcepoint DLP server, see *Installing data components*, page 28. For information on installing other Forcepoint DLP

components, such as the protector, mobile agent, or endpoint client, see the Forcepoint DLP Installation Guide.

Step 6: Install Email management components

Follow these instructions to install the Email Security module of the Security Manager. In addition to the Email Security module, you will be given the option to install Email Log Server on this machine. As Log Server consumes considerable system resources, for when multiple Forcepoint security solutions are installed, it is recommended to run it on another machine. See *Install Email Log Server*, page 32.

1. Once the Forcepoint Email Security Installer is launched, the Introduction screen appears; click **Next** to begin Email Security installation.
2. On the Select Components screen, deselect the Email Log Server option if you are installing the Log Server on a separate Windows machine, then click **Next**.

   If you are deploying Email Log Server and Forcepoint Email Security on separate machines, it is recommended to install Email Log Server first.

   The Security Manager (Email Security module) will be installed automatically. You cannot deselect it.

   Note
   If you do not see the Email Security module on this screen, Forcepoint Infrastructure was not detected by the Forcepoint Email Security Installer. Forcepoint Infrastructure must be installed already to be able to install Email management components.

3. On the Email Log Database screen, specify the IP address or IP address and instance name (format: IP address\instance) and port for the email Log Database.

   You may specify whether the connection to the database should be encrypted.

   Please note the following issues associated with using this encryption feature:

   - By default, Email Log Server uses NTLMv2 to encrypt the connection.

     If you want to use SSL encryption, you must have imported a trusted certificate to the Log Server machine. See your database documentation for information about importing a trusted certificate.
   - The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
   - The connection from the Forcepoint appliance to the Log Database cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.

   Designate the login type for the database, either Windows authentication or **sa** account.

4. On the Email System Credentials screen, specify the server name or domain name of the management server, along with the user credentials to be used by Forcepoint Security Manager components when running services. Specify the **User name** and **Password** of the account to be used by the Security Manager.
5. On the Email Appliance screen, specify the Email appliance to be managed by this installation of the Security Manager and then click **Next**.

   Enter the IP address of the **C** interface of the Email appliance. You must specify an IP address only. Do not use a fully-qualified domain name (FQDN).

   When you click **Next**, communication with the specified appliance will be verified. Communication may be unsuccessful if:

   - Subscription key has already been applied to the appliance (typically meaning another installation of the Security Manager has been used to manage the appliance). The subscription key must be reset on the appliance.
   - Version of software to be installed does not match the version of the appliance. Verify whether the versions match.
   - Specified appliance is a secondary appliance in a cluster. Specify the primary appliance in the cluster or a non-clustered appliance.
   - The appliance cannot connect to the specified database server (specified during product installation).
   - Firewall is blocking communication to the appliance on port 6671. Make sure any local firewall allows outbound communication on port 6671.
   - Appliance P1 interface has not been correctly configured via the appliance CLI.
6. On the Installation Folder screen, specify the location to which you want to install Email Security module components and then click **Next**.

   To select a location different than the default, use the **Browse** button.

   Each component (Email Security module and/or Email Log Server) will be installed in its own folder under the parent folder you specify here.
7. On the Pre-Installation Summary screen, review the components to be installed. If they are correct, click **Install**.

   Click **Previous** to return to any screen on which you want to modify settings.

   The Installing Forcepoint Email Protection Solutions screen appears, as components are being installed.
8. Wait until the **Installation Complete** screen appears, and then click **Done**.
9. The installer program closes. Installation is complete.

3 Installing Additional Components

This chapter includes instructions for:

Installing web components

The steps is this section describe the installation of web protection components if you have not already installed them on the management server. If you are distributing components across multiple machines, run the installer and complete the installation steps on each machine.

These instructions assume that you have already launched the installer and selected **Custom**.

Install Web Log Server

Log Server is a Windows-only component that logs Internet request data, including:

- Source of request
- Category or protocol associated with the request
- Whether the request was permitted or blocked
- Whether keyword blocking, file type blocking, quota allocations, bandwidth levels, or password protection were applied

Each Log Server instance can log to only one Log Database at a time, and only one Log Server can be installed for each Policy Server.

Log Server processing can consume considerable system resources.

In a software-based deployment, do not install Log Server on the same machine as Filtering Service or Network Agent—policy enforcement or logging performance may be affected if they are on the same machine.

In an appliance-based deployment, Log Server must be installed on a separate Windows machine.

> **Note**
> Log Server must be installed before you can see charts on the **Status > Dashboard** page, or run presentation or investigative reports in the Web module of the Security Manager.

Installation steps

To be able to install Log Server, a supported database engine must be running.

1. On the Select Components screen in the Forcepoint Security Installer, select **Log Server**.

   If the deployment includes the Forcepoint Web Security Hybrid Module, also select **Sync Service**.
2. On the Policy Server Connection screen, enter the IP address of the Policy Server for this Log Server, and the Policy Server communication port (55806, by default).
3. On the Policy Broker Connection screen, enter the management server IP address and the Policy Broker communication port (55880, by default), and then click Next.

   In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.
4. If the Log Server server machine does not include a supported version of the Microsoft SQL Server Native Client and related tools, you are prompted to install the required components.

   Depending on your current configuration, the Native Client installer may run silently in the background, or prompt you for input.

   - When the Native Client installer runs in the background, you will know the process is complete when the Forcepoint installer continues to the next screen. This may take a few minutes.
   - When the Native Client installer runs in the foreground, follow the prompts to complete the installation. Note that if you are prompted to reboot the machine, do not reboot at this point. Instead, complete the Forcepoint software installation first, then reboot.
5. On the **Database Information** screen, enter the hostname or IP address of the machine on which a supported database engine is running. If a supported database engine is detected on this machine, its IP address is already entered by default. To use a database engine on a different machine, enter its IP address instead.

   If you are using SQL Server clustering, enter the virtual IP address of the cluster. (Clustering is only supported with Forcepoint Email Security and Forcepoint Web Security.)

After entering the IP address of the database engine machine, choose how to connect to the database:

- Select **Trusted connection** to use a Windows account to connect to the database. Enter the user name and password of a trusted account with local administration privileges on the database machine. The trusted account you specify here should be the same as that with which you logged onto this machine before starting the Forcepoint Security Installer.

  If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Web module of the Security Manager. See How do I configure services to use a trusted connection?

- Select **SQL Server Authentication** to use a SQL Server account to connect to the database. Enter the user name and password for a SQL Server account that has administrative access to the database. The SQL Server password cannot be blank, or begin or end with a hyphen (-).

> **Note**
> The database engine must be running to install Forcepoint reporting components. The installer will test for a connection to the specified database engine when you click **Next** on the **Database Information** screen. The installer cannot proceed unless a successful connection can be made.

6. On the Log Database Location screen, accept the default location for the Log Database files, or select a different location. Then click **Next**.

   The default database location information is taken from the Management Infrastructure configuration.

   - If the database engine is on another machine, the default location is C:\Program Files\Microsoft SQL Server on that machine.
   - If the database engine is on this machine (not recommended), the default location is C:\Program Files \Websense.

> **Important**
> The directory you specify for the Log Database files must already exist. The installer cannot create a new directory.

7. On the Optimize Log Database Size screen, select either or both of the following options and then click **Next**.

   - **Log web page visits**: Enable this option to log one record (or a few records) with combined hits and bandwidth data for each web page requested rather than a record for each separate file included in the web page request. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities. Deselect this

option to log a record of each separate file that is part of a web page request, including images and advertisements. This results in more precise reports, but creates a much larger database and causes reports to generate more slowly.

- **Consolidate requests**: Enable this option to combine Internet requests that share the same value for all of the following elements, within a certain interval of time (1 minute, by default):
  - Domain name (for example: www.forcepoint.com)
  - Category
  - Keyword
  - Action (for example: Category Blocked)
  - User/workstation

8. On the Installation Directory screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.

   The installation path must be absolute (not relative). The default installation path is:

   C:\Program Files\Websense\Web Security

   The installer creates this directory if it does not exist.

   Important
   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   The installer compares the installation's system requirements with the machine's resources.

   - Insufficient disk space prompts an error message. The installer closes when you click **OK**.
   - Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.

9. On the Pre-Installation Summary screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.

10. Click **Next** to start the installation. An Installing progress screen is displayed. Wait for the installation to complete.
11. On the Installation Complete screen, click **Done**.

12. After installing Log Server, restart the management server machine.

Important
When Log Server is not installed on the management server, be sure to restart the management server before creating scheduled jobs in presentation reports. Any scheduled jobs you create before restarting the server cannot be saved properly and will be lost, even if they appear to work for a period of time.

Install an instance of Filtering Service

When the standalone or primary Policy Broker and the central Policy Server reside on the management server, you must install at least one instance of Filtering Service that connects to the central Policy Server.

This instance of Filtering Service may reside:

- On a supported Linux server
- On a supported Windows server
- On a **filtering only** appliance

  Note that using a software installation for this instance of Filtering Service may make for a more convenient deployment. A software deployment allows you to also install components like User Service and Usage Monitor for the central Policy Server. (These components don't reside on a filtering only appliance.)

Best practice is to install Filtering Service on a different machine from the management server. This is because Filtering Service can consume considerable system resources and may have a performance impact on the server.

Although other components (like Network Agent or a transparent identification agent) may be installed with Filtering Service, a second instance of Policy Server may **not** reside on this machine. This Filtering Service instance **must** connect to the central Policy Server on the management server machine.

Using a filtering-only appliance

Follow the setup, firstboot, and initial configuration instructions in the Forcepoint Appliances Getting Started Guide.

Installing Filtering Service on Windows

Ensure you have prepared the machine as described in Preparing for installation.

To install Filtering Service on a supported Windows platform:

1. Log on to the machine with domain admin privileges.
2. Download the Forcepoint Security Installer (**Forcepoint85xSetup.exe**) from My Account.

3. Right-click **Forcepoint85xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
4. On the Welcome screen, click **Start**.
5. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
6. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that Forcepoint Security Solutions components should use for communication, then click **Next**.
7. On the Installation Type screen, select **Custom** and then click **Next**.
8. On the Select Components screen, select the following components, then click **Next**:
   - Filtering Service
   - User Service
   - Usage Monitor

   Optionally, you may also select:
   - Network Agent
   - State Server
   - DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent
   - Directory Agent (*used by the Forcepoint Web Security Hybrid Module*)
9. On the Policy Server Connection screen, enter the IP address of the central Policy Server machine and the Policy Server communication port (55806, by default), then click **Next**.
10. If you are installing Directory Agent, on the Policy Broker Connection screen, enter the IP address of the primary or standalone Policy Broker and its communication port (55880, by default), then click **Next**.
11. On the Active Directory screen, indicate whether you are using Windows Active Directory to authenticate users in your network, then click **Next**.
12. On the Computer Browser screen, indicate that the installer should attempt to start the service, then click **Next**.
13. On the Integration Option screen, select **Install Web Security to connect to Content Gateway**, then click **Next**.
14. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other Forcepoint Security Solutions components, then click **Next**.
15. On the Filtering Feedback screen, indicate whether you want your software to send feedback to Forcepoint LLC, then click **Next**.
16. On the Directory Service Access screen, enter the domain, user name, and password of an account that is a member of the Domain Admins group on the domain controller, then click **Next**.

    User Service, DC Agent, and Logon Agent use this information to query the domain controller for user and group information.

17. On the Installation Directory screen, accept the default installation path, or click or select **Choose** to specify another path, and then click **Next**.

    The installation path must be absolute (not relative). The default installation path is C:\Program Files (x86)\Websense\Web Security\.

    The installer creates this directory if it does not exist.

    Important
    The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

18. On the Pre-Installation Summary screen, verify the information shown, then click **Next**.

    The summary shows the installation path and size, and the components to be installed.

19. A progress screen is displayed. Wait for the installation to complete.
20. On the Installation Complete screen, click **Finish**.

Installing Filtering Service on Linux

Ensure you have prepared the machine as described in Preparing for installation.

1. Log on to the installation machine with full administrative privileges (typically, **root**).
2. Create a setup directory for the installer files. For example:

   ```
   /root/Forcepoint_setup
   ```

3. Download the Web Security Linux installer package from My Account. The installer package is called **Web85xSetup_Lnx.tar.gz**.

   Place the installer archive in the setup directory you created.

4. In the setup directory, enter the following commands to uncompress and extract files:

   ```
   tar -xvzf Web85xSetup_Lnx.tar.gz
   ```

5. Launch the installer using the following command (from the setup directory):

   ```
   ./install.sh -g
   ```

   This launches a GUI-based installer and is available on English versions of Linux only. A text-only, command-line version can be launched by omitting the -g switch:

   ```
   ./install.sh
   ```

Perform the Filtering Service installation

1. On the Introduction screen, click or select **Next**.
2. On the Subscription Agreement screen, choose to accept the terms of the agreement and then click **Next**.

3. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that Web Security components should use for communication, then click **Next**.
4. On the Installation Type screen, select **Custom** and then click or select **Next**.
5. On the Select Components screen, select the following components, then click or select **Next**:
   - Filtering Service
   - User Service
   - Usage Monitor

   Optionally, you may also select:
   - Network Agent
   - State Server
   - Logon Agent, eDirectory Agent, or RADIUS Agent
   - Directory Agent (*used by the Web Security Hybrid Module*)
6. On the Policy Server Connection screen, enter the central Policy Server IP address and communication port (55806, by default).
7. If you are installing Directory Agent, on the Policy Broker Connection screen, enter the IP address of the primary or standalone Policy Broker machine, and the Policy Broker communication port (55880, by default).
8. On the Integration Option screen, select **Install Web Security to connect to Content Gateway**, then click or select **Next**.

   When you install Content Gateway, you will be prompted for the Filtering Service IP address.
9. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other Web Security components, then click or select **Next**.
10. On the Feedback screen, indicate whether you want your software to send feedback to Forcepoint, then click or select **Next**.
11. On the Installation Directory screen, accept the default installation path, or click or select **Choose** to specify another path, and then click or select **Next**.

    The installation path must be absolute (not relative). The default installation path is: /opt/Websense/

    The installer creates this directory if it does not exist.

    Important

    The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

    The installer compares the installation's system requirements with the machine's resources.
    - Insufficient disk space prompts an error message. The installer closes when you click or select **OK**.

- Insufficient RAM prompts a warning message. The installation continues when you click or select **OK**. To ensure optimal performance, increase your memory to the recommended amount.

12. On the Pre-Installation Summary screen, verify the information shown, then click or select **Next**.

    The summary shows the installation path and size, and the components to be installed.

13. An Installing progress screen is displayed. Wait for the installation to complete.

> **Note**
> If you are using the command-line Linux installer, do **not** cancel (Ctrl-C) the installer after the Pre-Installation Summary screen, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

14. On the Installation Complete screen, click or select **Done**.

Install Content Gateway

Content Gateway is a Linux-based, high-performance web proxy and cache that provides real-time content analysis and website classification to protect clients from malicious content while enabling access to safe content.

Content Gateway offers:

- Categorization of dynamic websites
- Categorization of new and unclassified websites
- Optionally, HTTPS and FTP content analysis, in addition to HTTP
- Enterprise Web proxy caching capabilities
- Prevention of data loss over web channels

Content Gateway is a required component of Forcepoint Security Solutions. In a software-based deployment, Content Gateway must be installed on a Linux machine. The machine should be dedicated to running Content Gateway.

> **Important**
> In an appliance-based deployment, when Forcepoint Security Solutions is configured, Content Gateway is already installed. Forcepoint Security Solutions and Forcepoint Email Security cannot be installed on the same appliance.

For full instructions on preparing a Linux machine and installing Content Gateway, see Installation Guide: Forcepoint Web Security.

Installing other web components

For information about installing other web protection components, see the section "Install additional web protection components" in the installation instructions for Forcepoint Security Solutions.

Installing data components

After Forcepoint DLP components are installed on the management server, additional Forcepoint DLP components may be added as needed. In larger deployments, these might include supplemental Forcepoint DLP servers, crawlers, or policy engines. Other components, such as the Forcepoint DLP protector and any number of Forcepoint DLP agents, may also be installed.

Important

Before installing additional Forcepoint DLP components, make sure that the Forcepoint Management Infrastructure and Forcepoint DLP management components are already installed.

Do not install any Forcepoint DLP component on a domain controller.

Installing supplemental Forcepoint DLP servers

Medium to large enterprises may require more than one Forcepoint DLP server to perform content analysis efficiently. Having multiple Forcepoint DLP servers allows your organization to grow, improves performance, and allows for custom load balancing.

Supplemental Forcepoint DLP server installations include:

- A policy engine
- Secondary fingerprint repository (the primary is on the management server)
- Endpoint server
- Optical Character Recognition (OCR) server
- Crawler

Notes:

In production environments, do not install a Forcepoint DLP server on a Microsoft Exchange, Forefront TMG, or print server. These systems require abundant resources.

To install a supplemental server:

1. Download the Forcepoint Security Installer (**Forcepoint85xSetup.exe**) from My Account.
2. Launch the installer on a supported Windows server.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for Forcepoint DLP.
6. On the Welcome screen, click **Next** to begin the installation.
7. In the Destination Folder screen, specify the installation folder for the software.

   The default destination is C:\Program Files (x86)\Websense\Data Security. If another drive is larger than drive C, it is used instead. Large removable drives may be detected by the system as a local drive and used as the default. Do not install on removable media.

   Important
   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   Note
   Regardless of what drive you specify, it must have a minimum of 4 GB of free disk space for the Forcepoint Security Installer.

8. On the Select Components screen, select **Forcepoint DLP Server**.
9. On the Fingerprinting Database screen, accept the default database location, or to choose a location other than the default shown, use the **Browse** button.
10. On the Server Access screen, select the IP address to identify this machine to other components.
11. On the Register with the Forcepoint DLP Server screen, enter:
    - The fully-qualified domain name (FQDN) of the management server
    - The credentials for a Forcepoint DLP administrator with System Modules permissions
12. On the Local Administrator screen, supply a user name and password as instructed on-screen. The server/hostname portion of the user name cannot exceed 15 characters.
13. If a Lotus Notes client is installed on this machine, the **Lotus Domino Connections** screen appears.

To enable fingerprinting or discovery on the Domino server, complete the information on this page.

Important

Before completing the information on this screen:

- Create at least one user account with administrator privileges for the Domino environment. (Read permissions are not sufficient.)
- Be sure that the Lotus Notes installation is done for "Anyone who uses this computer."
- Connect to the Lotus Domino server from the Lotus Notes client.

a. On the Lotus Domino Connections page, select **Use this machine to scan Lotus Domino servers**.

b. In the User ID file field, browse to one of the authorized administrator users, then navigate to the user's **user.id** file.

Note

Select a user that has permission to access all folders and Notes Storage Format (NSF) files of interest, otherwise certain items may not be scanned.

c. In the Password field, enter the password for the authorized administrator user.

14. On the Installation Confirmation screen, if all the information entered is correct, click the **Install** button to begin installation.

    Installation may seem to take a long time. Unless a specific error or failure message appears, allow the installer to proceed.

    If a message about needing port 80 or port 443 appears, click **Yes** to continue the installation.

    Clicking **No** cancels the installation.

15. Once installation is complete, the Installation Complete screen appears. Click **Finish**.

16. Log onto the Data Security module of Forcepoint Security Manager and click **Deploy** to fully connect the supplemental server with the management server.

Installing Forcepoint DLP agents

The following Forcepoint DLP agents can be installed. With the exception of the protector, mobile agent, and Forcepoint DLP Network, agents are installed using the Custom option of the standard Forcepoint Security Installer.

Note that agents become available only when the installation performed on a server that meets the agent's requirements. For example, the FCI agent is only shown as an option on machines with Microsoft FSRM installed.

For instructions on how to install the agents, see the Forcepoint DLP Installation Guide.

Agent	Description	When to Use	Location
Protector	The protector is a standard part of Forcepoint DLP deployments. It is a physical or soft appliance with a policy engine and a fingerprint repository, and it supports analysis of SMTP, HTTP, FTP, plain text, and IM traffic that doesn't use SSL. For blocking HTTPS traffic, the protector can integrate with proxies using ICAP.	Monitor/block: network email Monitor: HTTP, FTP, plain text, IM Monitor/block: HTTP via ICAP	On premises
Web Content Gateway	The Web Content Gateway module is included with Forcepoint DLP Network. It provides DLP policy enforcement for the web channel, and offers SSL traffic decryption. This component permits the use of custom policies, fingerprinting, and more. It also makes use of the Forcepoint URL category database to define DLP policies for the web channel.	Monitor/block: HTTP/S with SSL decryption	On premises
Analytics Engine	The analytics engine is used to calculate the relative risk of user activity, correlate it with similar activity, and assign it a risk score.	High risk incident scoring	On premises Virtual appliance
Forcepoint DLP Cloud Agent	The cloud agent provides cloud activity content inspection for files uploaded into and stored within supported cloud collaboration services.	DLP: Delete file/ permit Discovery OneDrive for Business files	Microsoft Azure cloud On premises
Mobile agent	The mobile agent monitors and blocks data downloaded to mobile devices that perform synchronization operations with the Exchange server. It can reside on a Forcepoint appliance or Linux machine.	Monitor/block: Exchange ActiveSync email	On premises

Agent	Description	When to Use	Location
Crawler	The crawler performs discovery and fingerprinting scans. The crawler is installed automatically on the management server and supplemental Forcepoint DLP servers. To improve scanning performance in high transaction volume environments, it can also run standalone.	Discovery/ Fingerprinting	On premises
Forcepoint DLP Endpoint	The endpoint client software monitors all data activity on endpoint machines and reports on data at rest on those machines. Forcepoint DLP Endpoint can monitor application operations such as cut, copy, paste, and print screen. It can also block users for copying files, or even parts of files, to endpoint devices such as thumb drives, CD/DVD burners, and Android phones, among other features.	Monitor/block: email, printing, application control, LAN control, HTTP/S, removable media Local discovery	Endpoint devices

Important

Forcepoint DLP agents and machines with a policy engine (such as a Forcepoint DLP Server or Web Content Gateway appliance) must have direct connection to the Forcepoint management server. When deployed in a DMZ or behind a firewall, the relevant ports must be allowed.

Install Email Log Server

Forcepoint Email Security is an appliance-based solution. All components run on the appliance except the Email Security module of Forcepoint Security Manager and Email Log Server. These are the only two Forcepoint Email Security components that may be installed using the Forcepoint installer.

- Forcepoint Email Security cannot be run on the same appliance as Forcepoint Security Solutions.
- It is recommended that you install Email Log Server on a different machine from the Forcepoint management server.

To install the Windows-based Forcepoint Email Security components:

1. Download and launch the Forcepoint installer on the Log Server machine.
2. Choose the **Custom** installation type.
3. On the Custom Installation dashboard, click the **Install** link for Forcepoint Email Security.

   The Email component installer is launched.

4. On the Introduction screen, click **Next**.

   The Forcepoint Email Security Installer does not detect Forcepoint Management Infrastructure on the machine, and operates in custom mode.

5. In the Select Components screen, Email Log Server is selected for installation by default. To install Email Log Server, SQL Server must already be installed and running in your network.

   If you choose to install Email Log Server, the Email Log Server Configuration utility is also installed. This utility can be accessed from the Forcepoint folder in the Start menu.

6. On the Email Log Database screen, specify the location of a database engine and how you want to connect to it.

   - **Log Database IP**: Enter the IP address of the database engine machine. If you want to use a named database instance, enter it in the form *<IP address>\<instance name>*. The instance must already exist. See your SQL Server documentation for instructions on creating instances.
   - You may specify whether the connection to the database should be encrypted.

     Please note the following issues associated with using this encryption feature:

     - By default, Email Log Server uses NTLMv2 to encrypt the connection.

       If you want to use SSL encryption, you must have imported a trusted certificate to the Log Server machine. See your database documentation for information about importing a trusted certificate.
     - The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
     - The connection from the Email Security module in Forcepoint Security Manager to the Forcepoint appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.
   - **Database login type**: Select how Email Log Server should connect to the database engine.
     - **Trusted connection**: connect using a Windows trusted connection.
     - **Database account**: connect using a SQL Server account.

     Then enter a user name and password.

     - If using a trusted connection, enter the domain\username of the account to be used. This account must be a trusted local administrator on the database engine machine.
     - If using a database account, enter the name of a SQL Server account. This account must have certain roles assigned; see Installing with SQL Server.

   When you click **Next**, connection to the database engine is verified. If the connection test is successful, the next installer screen appears.

7. On the Email Log Database File Location screen, specify where the email Log Database files should be located and then click **Next**.

It is a best practice to use the default location. However, if you want to create the Log Database in a different location (or if you already have a Log Database in a different location), enter the path to the database files.

The path entered here is understood to refer to the machine on which the database engine is located. The path entered must specify a directory that already exists.

If any email components (e.g., the Email Security module in Forcepoint Security Manager or another instance of Email Log Server) have already been installed in your deployment, the following message appears:

The Email Log database exists, do you want to remove it?

This occurs because the database was created upon installation of the other email components. Click **No** to continue using the existing database. In general, you should keep the database if you are sure the database was created only during the course of installing other components in your current deployment.

Clicking **Yes** removes the database.

Warning

If any Forcepoint Email Security log data has been written to the database it will be lost if you remove the database. If you want to keep this data, back up the esglogdb76 and esglogdb76_*n* databases. See your SQL Server documentation for backup instructions.

Warning

If you remove the database, any currently quarantined email will no longer be accessible.

8. On the Installation Folder screen, specify the location to which you want to install Email Log Server and then click **Next**.

   Important

   The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   To select a location different than the default, use the **Browse** button.

   Email Log Server will be installed in its own folder under the parent folder you specify here.

9. On the Pre-Installation Summary screen, review the components to be installed. If they are correct, click **Install**.

   The Installing Forcepoint Email Protection Solutions screen appears, as components are being installed.

10. Wait until the Installation Complete screen appears, and then click **Done**.