Forcepoint DLP

10.4

Installation Guide

Revision A

Published 07 October 2025

Contents

Chapter 1

Installing the Management Server

Contents

The first step in installing Forcepoint DLP is to install the management server. The management server hosts both the Forcepoint Security Manager (the graphical user interface used to manage Forcepoint security solutions) and core Forcepoint DLP components.

- Installation must be completed on the management server before other Forcepoint DLP components (supplemental servers, protectors, and endpoints, for example) can be installed.
- The management server serves as the primary Forcepoint DLP server.

There are 2 parts to installing Forcepoint DLP components on the management server:

1) *Install the Forcepoint Infrastructure*.
   The management infrastructure includes the Forcepoint Security Manager and its settings database.

2) *Install Forcepoint DLP management components*.
   The Forcepoint DLP management server components include the policy engine, crawler, fingerprint repository, forensics repository, and endpoint server.

Forcepoint DLP may be installed on hardware or virtual machines (VMs).

Starting in Forcepoint DLP v8.9, Forcepoint Security Manager and Forcepoint DLP may be installed in Amazon Web Services (AWS). For more information, see *DLP Installation in Cloud Providers*.

After the management components have been installed, additional Forcepoint DLP agents, servers, and crawlers may be installed to add functionality and for system scaling.

See *Installing Supplemental Forcepoint DLP Servers* and *Installing Forcepoint DLP Agents* for more information.

Note

From Forcepoint Security Manager 9.0, the pgAdmin will no longer be included in the installer.

By default, the pgAdmin is included in the Forcepoint Security Manager 8.6.4 and prior versions.

For more information, see PgAdmin Installation Guide Knowledge Base article.

Related concepts

Installing Supplemental Forcepoint DLP Servers on page 19
Installing Forcepoint DLP Agents on page 25

Related tasks

Install the Forcepoint Infrastructure on page 11
Install Forcepoint DLP management components on page 16

Related information
Appendix A:DLP Installation in Cloud Providers on page 61

Management server system requirements

Find system requirements for the Forcepoint management server in the *Deployment & Installation Center*, as described below:

- For operating system, hardware, virtualization (VM), and database requirements, see System requirements for this version.
- For port requirements, see Forcepoint DLP ports (the “Forcepoint management server” section).

Preparing for management server installation

Before installing Forcepoint DLP, complete all of the preparatory steps in this section.

Windows considerations

1) Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.

2) Make sure that the .NET Framework v3.5 and v4.6-4.8 are installed on the management server.

3) Make sure that at least the Visual C++ version 2022 (or later) Runtime Libraries are installed on the management server. Download the Visual C++ Redistributable for Visual Studio from Microsoft.

Domain considerations

- The servers running Forcepoint DLP software can be set as part of a domain or as a separate workgroup. If there are multiple servers, or if the system will be configured to run commands on file servers in response to discovery, it is best practice to make the servers part of a domain.
  Do not install Forcepoint DLP on a domain controller machine.
- Strict GPOs may interfere with Forcepoint DLP and affect system performance, or even cause the system to halt. To avoid this issue, when adding Forcepoint DLP servers to a domain, make them part of an organizational unit that does not enforce strict GPOs.

- Certain real-time antivirus scanning can downgrade system efficiency. This problem can be reduced by excluding some directories from that scanning (see *Antivirus*). Please contact Forcepoint Technical Support for more information on enhancing performance.

Related concepts
Antivirus on page 7

Synchronizing clocks

If you are distributing Forcepoint components across different machines in your network, synchronize the clocks on all machines where a Forcepoint component is installed. It is a good practice to point the machines to the same Network Time Protocol server.

Note

If the deployment will include one or more Forcepoint V Series appliances, synchronize the management server's system time to the appliance system time.

Antivirus

You must disable any antivirus software (or other security software that can perform active files scanning and process monitoring including `.dll` injections) on the machine prior to installing management server components.

Ensure to re-enable antivirus software after installation. Exclude the following Forcepoint files and folders from antivirus scans to avoid performance issues:

- The product installation folder, which, by default, is one of the following:
  - `*:\Program Files\Websense`
  - `*:\Program Files(x86)\Websense`
- `*:\Program Files\Microsoft SQL Server\*.*`
- `*:\Program Files(x86)\Microsoft SQL Server\*.*`
- `C:\Users\<user>\AppData\Local\Temp\*.*`
- `%WINDIR%\Temp\*.*`
- The forensics repository (configurable; defaults to the Websense folder)

No underscores in FQDN

Do not install Forcepoint components on a machine whose fully-qualified domain name (FQDN) contains an underscore. The use of an underscore character in an FQDN is inconsistent with Internet Engineering Task Force (IETF) standards.

Note

Further details of this limitation can be found in the IETF specifications RFC-952 and RFC-1123.

Disable UAC and DEP

Before beginning the installation process, disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation. The UAC settings can be re-enabled following installation.

Microsoft SQL Server Standard or Enterprise

Before you begin

If Forcepoint DLP will be used with Microsoft SQL Server Standard or Enterprise, do the following before running the Forcepoint Security Installer:

Steps

1) Install Microsoft SQL Server according to the product's instructions. Refer to Microsoft for more information. See the Certified Product Matrix for supported versions of SQL Server.

Tip

To install the database in a custom folder, see these instructions. Starting with Microsoft SQL Server 2012, the database engine service must have access permissions for the folder where database files are stored.

2) Make sure that SQL Server is running.

3) Make sure the SQL Server Agent is running.

4) Obtain account information for one of the following:

   - A SQL Server administrator
   - An account that has the db_creator server role, SQLAgent role, and db_datareader in **msdb**, as well as a sysadmin role.

   The account name and password are required during Forcepoint DLP installation. This account can be a Windows system account or a SQL admin account.

   For more information, see Administering Forcepoint Databases.

5) Restart the SQL Server machine after installation.

6) Make sure the management server machine can recognize and communicate with SQL Server.

7) Install the SQL Server client tools on the management server. Run the SQL Server installation program, and select **Connectivity Only** when asked which components to install. See the Microsoft SQL Server documentation for details.

8) Restart the management server machine after installing the connectivity components.

Getting the Forcepoint Security Installer

Download the Windows-only Forcepoint Security Installer from the Forcepoint Support website:

1) Go to support.forcepoint.com.
2) On the Member Login page, enter your Forcepoint Support account credentials, then click **Login**.
3) Select **Downloads**.
4) Select **Data Loss Prevention (DLP)** from Products list, and then select **DLP Core**.
5) On the list of installers, click **Forcepoint Security Manager for DLP v10.4**.
6) On the Product Installer page, click **Download**.
   The Forcepoint Security Installer executable is named **ForcepointDLP1040Setup.exe**.

When extracted, the installation files occupy approximately 4 GB of disk space.

Install the management server

Use the steps below to install Forcepoint DLP management server components.

Launch the installer

Steps

1) Log on to the installation machine with an account that has **local** administrator privileges.

Important

Use a dedicated account, and do not change the account after installation. Installed services use this account (the service account) when interacting with the operating system. If the account must later be changed, contact Forcepoint Technical Support first.

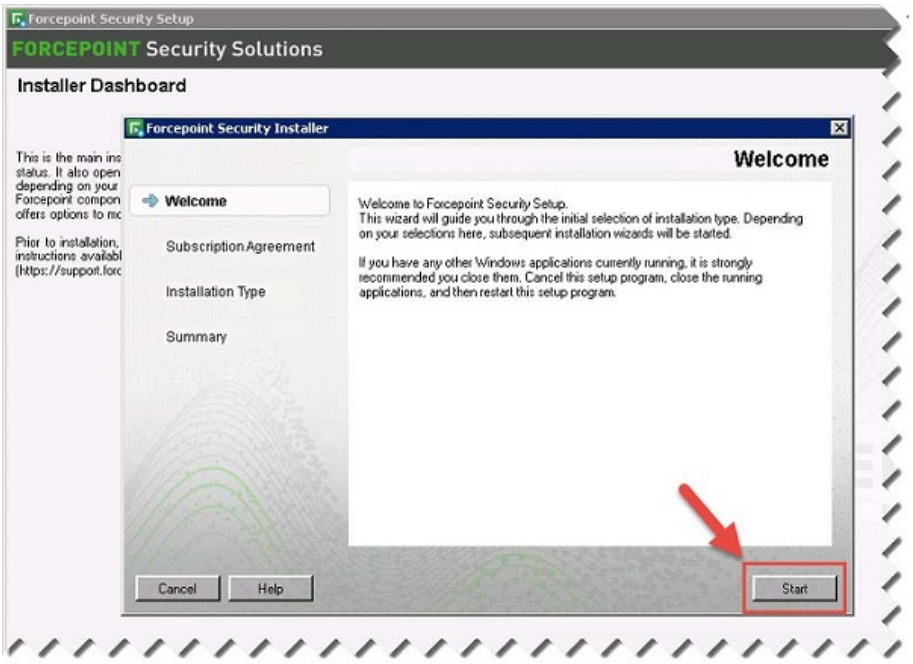
2) Double-click **ForcepointDLP1040Setup.exe** to launch the setup program.
   This process may take several minutes. A progress dialog box appears, as files are extracted.

Tip

Upon exit, the installer offers the option to **Keep installation files**. This greatly reduces the time needed to launch the installer in the future (for example, to add components or otherwise modify the installation).

To launch the installer from saved files, click **Forcepoint Security Setup** on the Start screen, or in the Forcepoint folder in the Start menu.

3) On the Welcome screen, click **Start**.

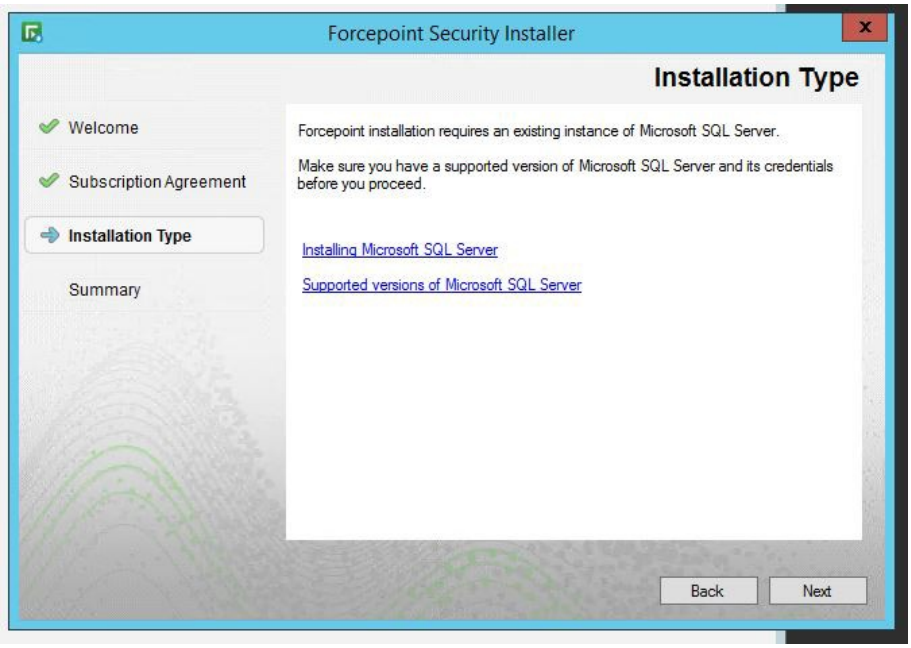


4) On the Subscription Agreement screen, select **I accept this agreement** and then click **Next**.

5) On the first Installation Type screen, select **Forcepoint Security Manager**, then select **Forcepoint DLP**. The following image shows the Installation Type screen:

Click **Next**. The second Installation Type screen displays.

6) Review the second Installation Type screen, as shown in the following image:



- If you do not already have an instance of SQL Server installed, click **Installing Microsoft SQL Server**.
- Click **Supported versions of Microsoft SQL Server** to verify the supported versions before installation.
- Then, click **Next**.

7) On the Pre-installation Summary screen, click **Next** to continue the installation.

8) On the Summary screen, click **Finish**.
The Forcepoint Infrastructure Setup wizard launches.

Note

If using the local SQL Express, it is recommended that you update to the latest cumulative update (CU).

Install the Forcepoint Infrastructure

Steps

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

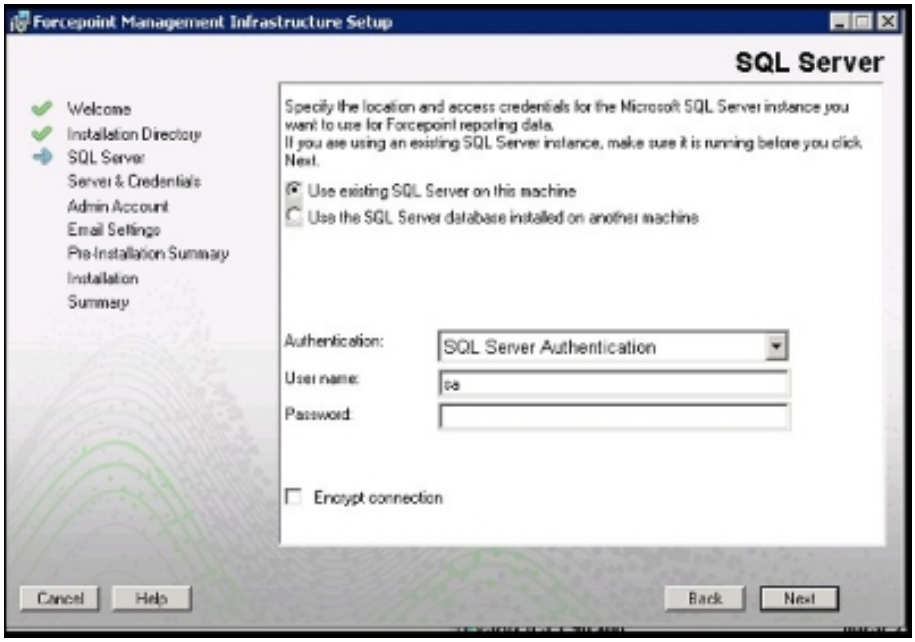
2) On the Installation Directory screen, accept the default installation path (recommended) or browse to a custom installation path, then click **Next**.

Important

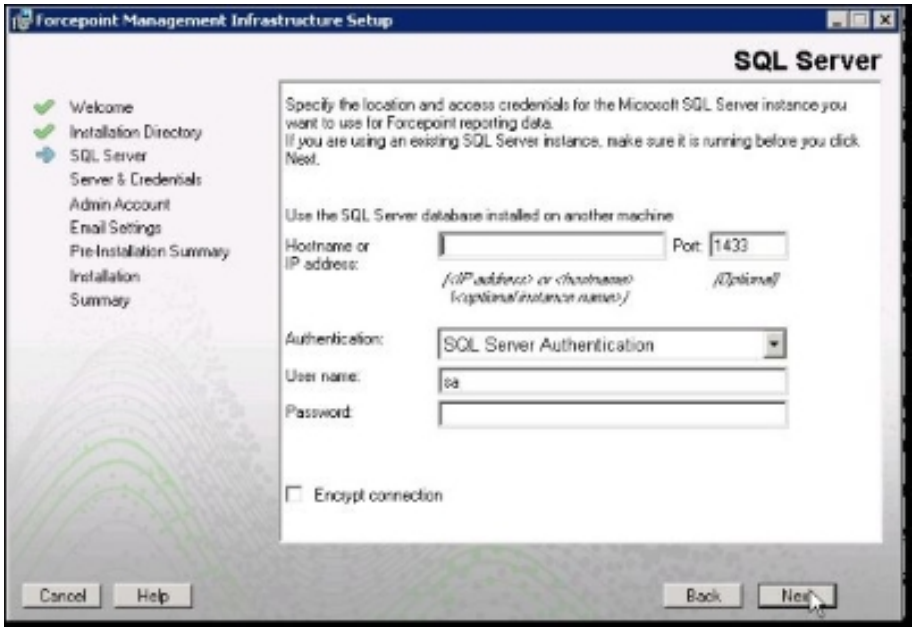
The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

3) On the SQL Server screen, specify the location of the database engine. The following two options are available.

- If Microsoft SQL is installed on your machine:



- If Microsoft SQL was not installed in your machine, or is installed on another machine:



- 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.

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

  See *Management server system requirements*,(mentioned below) to verify your version of SQL Server is supported.

4) Specify an authentication method and account information for connecting to the SQL Server database:

a) Select **SQL Server Authentication** to use a SQL Server account or **Windows Authentication** to use a Windows trusted connection.

b) Enter the **User Name** or **Account** and its **Password**.

For SQL Server Express, **sa** (the default system administrator account) is automatically specified.

If **Windows authentication** is selected for the authentication method, the current admin account's user name and password are automatically specified. These credentials can be edited to other existing Windows accounts, either local or domain. The chosen account must have login permissions on the SQL Server.

Note

The system administrator account password cannot contain the following characters: ;'"=[ ] { } ( ) ? * ! @ ,

c) Forcepoint DLP can use SSL to encrypt communication with the database. If encryption is already configured within Microsoft SQL Server, select **Encrypt connection** to enable SSL encryption.

For more information, see Administering Forcepoint Databases.

d) Click **Next**.

The installer verifies the connection to the database engine. If the connection test is successful, the next installer screen appears.

If the test is unsuccessful, an "Unable to connect" message is displayed. Click **OK** to dismiss the message, verify the connection information, and click **Next** to try again.

5) On the Server & Credentials screen, provide the following information:

a) Select an **IP address** for this machine. If the machine has a single network interface card (NIC), only one address is listed

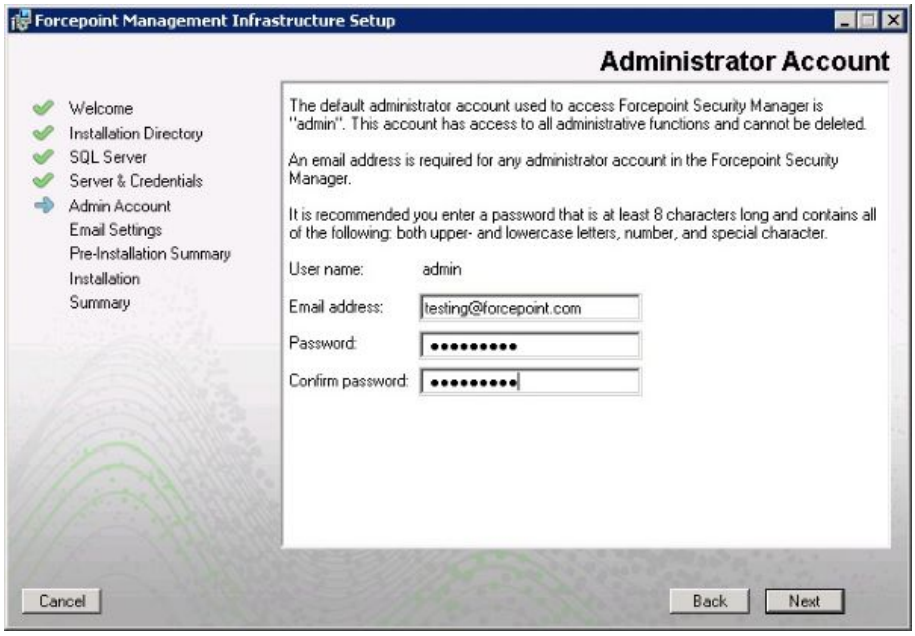
Administrators will use the selected IPv4 address to access the Security Manager via a web browser. This is also the IP address that remote Forcepoint components will use to connect to the management server.

b) Specify the **Server or domain** of the service account to be used by the Forcepoint Infrastructure and Security Manager components. The hostname cannot exceed 15 characters.

c) Specify the **User name** and **Password** for the service account.

d) Click **Next**.

6) On the Administrator Account screen, enter an email address and password for the default Security Manager administrator account: **admin**. This account has full access to all Security Manager features and functions for all products.



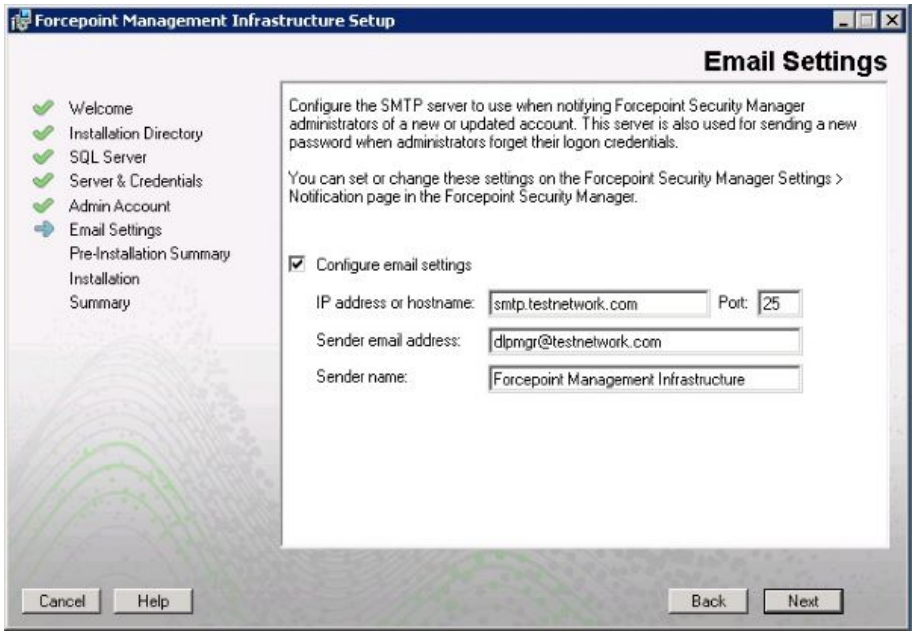
The password must:

- Be at least 8 characters
- Contain upper case characters
- Contain lower case characters
- Contain numbers
- Contain non-alphanumeric characters

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

When you are finished, click **Next**.

7) On the Email Settings screen, configure the SMTP server to use for system notifications, then click **Next**. SMTP settings can also be configured after installation.



Important

SMTP server configuration must be completed before password recovery email messages can be sent.

a) Enter the **IP address or hostname** of the SMTP server through which email alerts should be sent. In most cases, the default **Port** (25) should be used.

b) Enter the **Sender email address** that will appear in notification email messages.

c) Enter a descriptive **Sender name** to use in notification email messages. This can help recipients identify that a message originates from the Security Manager.

8) On the Pre-Installation Summary screen, verify the information, then click **Next** to begin the installation.

a) Forcepoint Security Installer starts again. In the Forcepoint Infrastructure Setup Welcome screen, click **Next**.

b) The Ready to Resume... screen appears. Click **Next**.

Note

When you click **Next**, it may take a couple minutes for the next screen to appear. Wait for the next screen, then continue with the next step.

9) The Installation screen appears. Wait until all files have been installed.

If the following message appears, determine whether port 9443 is in use on the machine:

Error 1920. Server 'Websense TRITON Central Access' (EIPManagerProxy) failed to start. Verify that you have sufficient privileges to start system services.

If port 9443 is in use, release it and then click **Retry** to continue installation.

10) On the Installation Complete screen, click **Finish**.

Result

The Installer Dashboard displays. After a few seconds, the Forcepoint DLP component installer launches. Continue with the next section.

Related reference
Management server system requirements on page 6

Install Forcepoint DLP management components

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

Note

If any prerequisites are missing, the Forcepoint DLP installer attempts to install them.

If prompted, click **OK** to allow services such as SMTP to be enabled and required Windows components to be installed. Access to the operating system installation disc or image may be required.

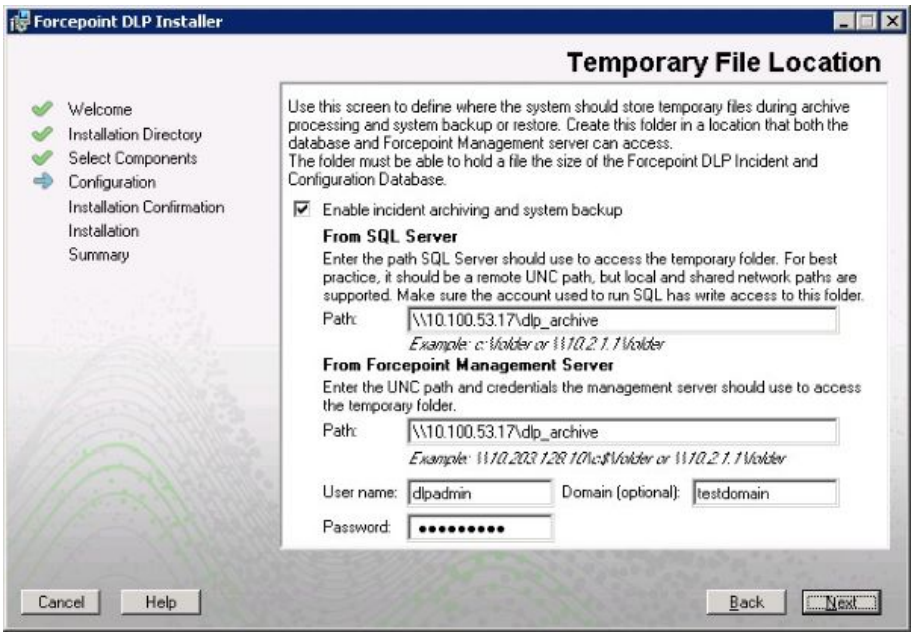
2) On the Destination Folder screen, accept the default installation directory (C:\Program Files (x86)\Websense \Data Security), or click **Browse** to select another location.
To continue, click **Next**.

3) On the Local Administrator screen, specify the **User Name** and **Password** for a local administrator account with complete access to all servers that include Forcepoint DLP components.

- As a best practice, use the same account information for all servers that host Forcepoint DLP components.
- If the local administrator is also a domain account, enter the user name in the "DOMAIN\user_name" format. The domain name must not exceed 15 characters.
- If the local administrator is a local account, use the "hostname\user_name" format. The hostname must not exceed 15 characters.
- The password must:
  - Be at least 8 characters
  - Contain uppercase characters
  - Contain lowercase characters
  - Contain numbers

- Contain non-alphanumeric characters

4) If the SQL Server database is on a remote machine, use the Temporary File Location screen to enable incident archiving and system backups, then specify where the system stores temporary files during archive processing and system backup and restore.
Before proceeding, create a folder in a location that both the database and management server can access. On average, this folder will hold 10 GB of data.



Complete the fields on the Temporary Folder Location screen as follows:

a) Select **Enable incident archiving and system backup** to allow archiving of old or aging incidents, as well as system backup or restore.

b) Under From SQL Server, enter the **Path** that the SQL Server should use to access the temporary folder. A remote UNC path is recommended, but local and shared network paths are supported. Make sure the account used to run SQL has write access to this folder.
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
```

c) Under From Forcepoint Management Server, enter the UNC **Path** themanagement server should use to access the temporary folder, then enter credentials for an account authorized to access the location.

5) On the Fingerprinting Database screen, accept the default database directory (C:\Program Files (x86)\Websense\Data Security\PreciseID DB\), or click **Browse** to select another local path.
To continue, click **Next**.

6) On the Installation Confirmation screen, first verify that the current time and data displayed are correct, then click **Install** to start installing Forcepoint DLP components.

7) The Installation Progress screen is displayed.
During installation, the setup program may display a prompt to:
   - Install required third-party services.
   - Free port 80.
   - Free port 443.

   Click **Yes** to continue the installation (**No** cancels the installation).

8) When the Installation Complete screen appears, click **Finish** to close the Forcepoint DLP installer.

Depending on whether or not other modules have been selected for installation, when the Forcepoint DLP installer completes, either the next module installer or the Modify Installation dashboard is displayed.

For information on installing other Forcepoint DLP components, such as the protector or endpoint client, refer to the below topics.

Also, if the user wants to later add, change, or remove components from a Forcepoint DLP machine, see *Adding or modifying Forcepoint DLP components*.

Note

The version 10.4 Forcepoint DLP installer also installs Forcepoint Security Manager version 10.4, Forcepoint Email Security version 8.5.5, and Forcepoint Web Security version 8.5.7.

Related concepts

Installing Supplemental Forcepoint DLP Servers on page 19
Installing Forcepoint DLP Agents on page 25
Installing Web Content Gateway on page 43

Related tasks

Adding or modifying Forcepoint DLP components on page 55

Related reference

Installing the Protector on page 35

Chapter 2

Installing Supplemental Forcepoint DLP Servers

Contents

After Forcepoint DLP has been installed on the management server (as described in *Installing the Management Server*), supplemental Forcepoint DLP servers can be installed to distribute analysis load.

Important

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

Note

Customers using Email Security Gateway (ESG) and Web Content Gateway (WCG) must not upgrade to the Supplemental Forcepoint DLP Server 10.4 which no longer support Optical Character Recognition (OCR) server, and must use the OCR server from previous version to keep the OCR functionality working. Stay tuned for further announcements regarding general availability of Email Security Gateway and Web Content Gateway with Forcepoint Security Manager 10.4 and Policy engine 10.4 to enable the new Policy Engine's OCR functionality.
Review the following article for possible upgrade paths: Optical Character Recognition (OCR) backward compatibility in DLP and Upgrade path.

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

Medium to large organizations may require more than one Forcepoint DLP server to perform content analysis efficiently. Having multiple Forcepoint DLP servers improves performance and allows for custom load balancing, as well as providing for organizational growth.

The following components are included on supplemental Forcepoint DLP servers:

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

Note

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

Related concepts
Installing the Management Server on page 5

Supplemental server system requirements

Find system requirements for supplemental Forcepoint DLP servers in the *Deployment & Installation Center*, as described below:

- For operating system, hardware, virtualization (VM), and database requirements, see System requirements for this version.
- For port requirements, see Forcepoint DLP ports (the “Supplemental Forcepoint DLP server” section).

Supplemental server prerequisites

Before you begin

Before installing a Forcepoint DLP server, ensure that all of the following prerequisites are met:

Steps

1) Set the installation partition to 1 NTFS Partition.

2) Configure Regional Settings to match the primary location (the location of the management server). If necessary, add supplemental language support and adjust the default language for non-Unicode programs.

3) Configure the network connection to have a static IP address.

4) Make sure that the server hostname does not include an underscore sign.

5) Enable Short Directory Names and Short File Names (see support.microsoft.com/kb/121007).

6) Create a local administrator to be used as a service account.
   If the deployment includes more than one Forcepoint DLP server, use a domain account (preferred), or the use same local user name and password on each machine. Do not change the service account.

7) Be sure to set the system time accurately on the server.

8) Exclude the following directories from antivirus scanning:
   - The folder where Forcepoint DLP was installed. For supplemental servers, this is Program Files (x86)\Websense\, by default.
   - *:\Inetpub\mailroot*.* - (typically at the OS folder)
   - *:\Inetpub\wwwroot*.* - (typically at the OS folder)
   - C:\Users\<user>\AppData\Local\Temp*.*
   - %WINDIR%\Temp*.*
   - The forensics repository (configurable; defaults to the product installation directory)

9) If a Lotus Notes client is installed on the machine (to allow fingerprinting and discovery on a Lotus Domino server), be sure to:
   a) Create at least one user account with **administrator** privileges for the Domino environment. (Read permissions are not sufficient.)
   b) Be sure that the Lotus Notes installation is done for “Anyone who uses this computer.”
   c) Connect to the Lotus Domino server from the Lotus Notes client.

10) Ensure that the Microsoft Visual C++ redistributable version 2022 (or later) is installed before installing the Forcepoint DLP Manager.

Supplemental server installation steps

The installation steps for Supplemental Server is explained in this section.

Step 1: Download and launch the installer

Steps

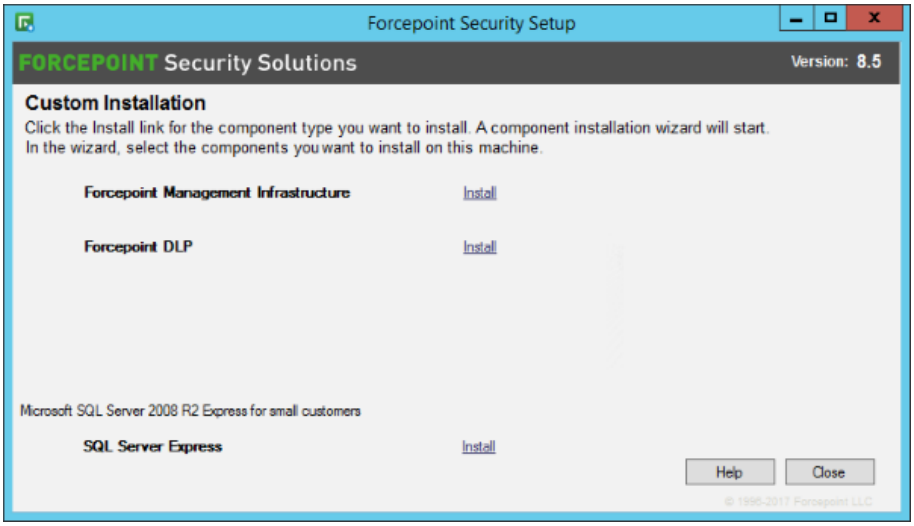
1) Copy the Forcepoint Security Installer (ForcepointDLP1030Setup.exe) from the management server machine to the current server, or download a copy from support.forcepoint.com, and click **Downloads**. (This requires a Forcepoint Support login account.)

2) Launch the installer.

3) Click through the Welcome page and 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.

Step 2: Configure the installation

Steps

1) Use the Destination Folder screen to either accept the default installation folder (C:\Program Files\Websense \Data Security) or specify a custom folder.
   - If the machine has multiple drives, and one is larger than the C drive, the larger drive 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, the machine must have a minimum of 4 GB of free disk space on the Windows partition for the Forcepoint Security Installer.

2) On the Select Components screen, select **Forcepoint DLP Server**.

3) On the Fingerprinting Database screen, accept the default database location, or click **Browse** to select another location.

4) Use the Server Access screen to select the IP address to use to identify this machine to other Forcepoint components.

5) Use the Register with the Forcepoint DLP Server screen to specify the location and logon credentials for the management server.
   - FQDN is the fully-qualified domain name of the management server machine.
   - Provide the credentials of a Forcepoint DLP administrator with System Modules permissions.

6) In the Local Administrator screen, supply an administrator user name and password as instructed. The server/hostname portion of the user name cannot exceed 15 characters.

7) If a Lotus Notes client is installed on this machine (to allow fingerprinting and discovery on a Lotus Domino server), the Lotus Domino Connections screen appears. To enable Lotus Domino fingerprinting and discovery:

   Important

   Before completing the information on this screen, be sure the prerequisites described in *Supplemental server prerequisites*, (mentioned below) have been met.

   a) Select **Use this machine to scan Lotus Domino servers**.

   b) Browse to the **User ID file** (user.id) of an authorized administrator user.

   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) Enter the **Password** for the authorized administrator user.

Related tasks

Supplemental server prerequisites on page 20

Step 3: Install and activate the new server software

Steps

1) Verify the information on the Installation Confirmation screen, then click **Install**to begin installation.

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

   During installation, the setup program may display a prompt to:

   - Install required third-party services.
   - Free port 80.
   - Free port 443.

   Click **Yes** to continue the installation (**No** cancels the installation).

2) When the Installation Complete page displays, click **Finish**.

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

Chapter 3

Installing Forcepoint DLP Agents

Contents

Forcepoint DLP agents enable the system to access the data necessary to analyze specific types of traffic, or the traffic from specific servers.

Important

Before installing an agent, 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.

Click the links below to learn more about each agent, including where to deploy it, installation prerequisites, installation steps, special considerations, and best practices.

- Connect to **Data Protection Service** to work with the Forcepoint DLP integrations with Forcepoint CASB, Forcepoint Web Security Cloud, and Forcepoint Cloud Email for enforcement of DLP policies on the cloud. No installation steps are required, only connection and activation of DLP Cloud Applications, as appropriate according to the licenses you have. See *Data Protection Service*, for more information.
- The on-premises **crawler** performs discovery and fingerprinting scans. The crawler is installed automatically on the management server and other Forcepoint DLP servers. To improve scanning performance in high transaction volume environments, additional, standalone instances can be used. (See *The crawler*)
- **Forcepoint DLP Endpoint** client software resides on and monitors data activity on endpoint machines. It also reports on data at rest. The endpoint agent can monitor application operations such as cut, copy, paste, and print screen, and block users from copying files, or even parts of files, to devices such as thumb drives, CD/DVD burners, and Android phones. The endpoint agent can also monitor or block print operations as well as outbound web posts and email messages. (See Installing and Deploying Forcepoint DLP Endpoint Clients.)

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 management server. When deployed in a DMZ or behind a firewall, the relevant ports must be allowed.

Related concepts

Data Protection Service on page 29

The crawler on page 31

Installing the Analytics Engine

The Analytics Engine is used to calculate the risk of user activity, correlate it with other risky activity to create a case, and assign the case with a risk score. Risk scores appear in the Forcepoint Security Manager in both the Incident Risk Ranking report and on the dashboard.

This feature requires installing the on-premises Analytics Engine on a 64-bit Linux machine as described in this section. The Analytics Engine is also available as a virtual appliance. For more information, see *Installing the Analytics Engine virtual appliance*.

For more information about clean installation of Analytics Engine, see Clean installation of Analytics Engine in Forcepoint Security Manager 10.3 knowledge base article

.

Analytics Engine system requirements

Find the system requirements for the Analytics Engine in the *Deployment and Installation Center* document, as described below:

- For operating system and hardware requirements, see System requirements for this version.
- For port requirements, see Forcepoint DLP ports (the “Analytics Engine” section).

Before installing the Analytics Engine

You must follow the preparation steps before installing Analytics Engine (AE) on the machines.

Before starting the installation, make sure the following Linux packages are installed on the machine that will host the Analytics Engine (AE):

- apr
- apr-util
- perl-Switch
- unixODBC
- freetds

Note

AE installation is no longer supported on CentOS systems. If you are still interested in installing Analytic Engine on CentOS, see Clean Installation of Analytics Engine on CentOS in Forcepoint Security Manager 10.3 for a workaround.

For Red Hat Enterprise Linux 8.10 supported AE installation, you can use the following commands to install the packages:

```
yum update
```

You can run one of the following:

```
dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

```
subscription-manager repos --enable codeready-builder-for-rhel-8-$(arch)-rpms
```

or

```
subscription-manager repos --enable codeready-builder-for-rhel-8-$(arch)-rpms && yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

And then run,

```
yum install apr apr-util perl-Switch libtool-ltdl unixODBC-devel freetds gcc gcc-c++ python2
 python2-devel libgsf libnsl python3-msal
```

The EPEL repository must be configured on the machine in order to install freetds.

The Forcepoint DLP components must already be installed and running on the management server to install the Analytics Engine.

Analytics Engine installation steps

Complete the Analytics Setup Wizard to configure user behavior analytics for Forcepoint DLP. Enter information as prompted. For help, enter “?”. To quit, press “Quit” or “Ctrl-C”.

Launch the Analytics Setup Wizard

To download the Analytics Engine installer (AnalyticsEngine86), complete the below steps:

Steps

1) Complete the steps below to download the Analytics Engine installer.
   a) Go to support.forcepoint.com and log in.
   b) Click the **Downloads** link in the menu bar at the top of the page.
   c) Select the product **Data Loss Prevention (DLP)**, and select **DLP Core**.
   d) To download the installer file, click the **Forcepoint DLP Analytics Engine software package**.
2) Log in to the installation machine as **root** and copy the installation file to the current working directory. Make sure the installation file has execution privileges.

3) To run the installer, enter:

```
./AnalyticsEngine86
```

- If a “permission denied” error appears, run the following command:

  ```
  chmod +x AnalyticsEngine86
  ```

- If a “missing packages” error appears, follow the instructions in the message to install the required packages using yum.

  After installing the required packages, run the command

  ```
  ./AnalyticsEngine86
  ```

Forcepoint Security Manager connection for Analytics Engine

Steps

1) When prompted, enter the IP address of the management server.

2) Enter a user name for a Security Manager administrator account with System Modules permissions.

3) Enter the account password.

4) The Analytics Engine verifies that it can connect to the management server.

   The Setup Wizard is complete.

   Administrators can now use the Security Manager to configure the Analytics Engine. See the Getting Started Guide for initial configuration details.

Installing the Analytics Engine virtual appliance

Once you acquire an Analytics Engine OVA, you will need to deploy it to a virtual machine and initiate the machine. The first time you power on (boot) the virtual appliance, a firstboot wizard displays with prompts to guide you through the installation.

Steps

1) From the firstboot wizard, enter **yes** to install the Analytics Engine image, then read and accept the subscription agreement.

2) At the first prompt, select the security mode. The only available option is **1**, for Forcepoint DLP Analytics Engine. Enter **yes** to continue.

3) Enter the hostname for the appliance.
Example: appliance.domain.com

4) You have the option to configure an NTP server; select yes to enable NTP and enter the NTP server, separating URLs with commas.

5) Select the relevant time zone.

6) Enter the administrator password for logging into the appliance.

7) The selected configuration displays for review. If you are satisfied with the current configuration, enter yes to continue with configuring the appliance network.

8) You have the option to configure the appliance network using a DHCP server or manually. Select **no** for manual configuration; **DHCP is not supported**.

9) If you selected manual configuration, enter the subnet mask, default gateway, and DNS when prompted.

10) The selected configuration displays for review. If you are satisfied with the current configuration, enter **yes** to continue with configuring the appliance engine.

11) Enter the IP address of the Forcepoint Security Manager.

12) Enter the username and password for the Forcepoint Security Manager.

13) The selected configuration displays for review. If you are satisfied with the current configuration, enter **yes**.

14) The full configuration settings for the Analytics Engine display for review. If you are satisfied with the finished configuration, enter **yes**.
If you enter **no**, the configuration wizard restarts and you will need to re-enter all of the information.

15) After you have completed the wizard, the Analytics Engine virtual appliance is installed and displays on the page **Settings > Deployment > System Modules**. To deploy the Analytics Engine, click **Deploy**.

Data Protection Service

To integrate Forcepoint DLP with Forcepoint CASB, Forcepoint Web Security Cloud, and Forcepoint Email Security Cloud for enforcement of DLP policies in the cloud, it is necessary to connect to Data Protection Service and activate DLP Cloud Applications, as appropriate according to the licenses you have. For full details, see the Forcepoint DLP Administrator Help and the Cloud Security Gateway Integration Guide.

To connect to Data Protection Service, you must have a JSON configuration file. This file should be part of your fulfillment package, or can be obtained from Forcepoint Technical Support.

Configuring Data Protection Service

Use the **Data Protection Service** tab of the **Settings** > **General** > **Services** page to connect to Data Protection Service. This is done by uploading tenant information from the JSON file you received from Forcepoint. Each time a file is uploaded, the system resets as if this is the first connection:

1) Click **Select File**, and in the dialog box that appears, click **Choose File**. Browse to the JSON file you received from Forcepoint, and then click **OK**.
   The file is uploaded to the server, and the information begins to appear in the Connection area of the Data Protection Service tab.

2) Click **Connect** to establish the connection with Data Protection Service:

3) Click **Deploy** to begin enforcing policies in cloud channels.

4) Click **OK** at the bottom of the screen to complete the process.

When the connection is active, the **Connect** button turns into a **Disconnect** button, enabling disconnection of Data Protection Service from Forcepoint DLP.

In the Data Protection Service Status area, upon successful connection, the status is marked as **Connected successfully**, the time and date of the connection is displayed, and the **Recheck connection** link is enabled. This link is used to check the connection status in the event of problems. If an error is returned upon checking the connection, the status is listed as **Failed to connect**.

After a successful connection to Data Protection Service is established, do the following to ensure the service is working properly:

1) Deploy a policy to Data Protection Service.

2) Check the incident report to make sure incidents are analyzed by Data Protection Service.

Note

As part of the integration with the Forcepoint Web Security Cloud, URL categories can now be imported from the Forcepoint Web Security Cloud Portal. See Forcepoint DLP Administrator Help for more information.

Error handling

- If Data Protection Service shows the status “Failed to connect”, the module is temporarily unavailable. Click **Connect** or **Recheck Connection** to try to connect again. If the problem continues, contact Forcepoint Technical Support.
- If the JSON file is uploaded for the first time, and when you click **Connect** the connection fails, the status shown is “Never connected”. This is because the Forcepoint Security Manager has never successfully connected to the Data Protection Service. Contact Forcepoint Technical Support for assistance.
- If you receive the following message in the Data Protection Service Status area:
  This service is not connected to Forcepoint CASB. Incident reporting and policy enforcement will be affected for cloud channels. See “Explain this page” for more information.

This means that there is a connection issue, and DLP Cloud API and Cloud Data Discovery channels will not enforce DLP policies, and the DLP Cloud Proxy channel might not report incidents to the Forcepoint Security Manager. See Forcepoint DLP Administrator Help, “Error handling”, for more information.

The crawler

The crawler is the name of the discovery and fingerprinting agent. It is selected by default when you install the management server or supplemental Forcepoint DLP servers.

Multiple crawlers may be deployed. During creating of a discovery or fingerprinting task, administrators select which crawler should perform the scan. Forcepoint recommends using the crawler that is located closest to the data you are scanning.

To view crawler status in the Security Manager, go to the **Settings** > **Deployment** > **System Modules** page, select the crawler, and click **Edit**.

Refer to the following topics:

Related concepts

Crawler system requirements on page 31

Related tasks

Special considerations for IBM Notes and Domino on page 31
Installing the crawler agent on page 32

Crawler system requirements

Find system requirements for the crawler in the *Deployment & Installation Center*, as described below:

- For operating system requirements, see System requirements for this version.
- For port requirements, see Forcepoint DLP ports (the “Crawler agent” section).

Special considerations for IBM Notes and Domino

Before installing a crawler that will be used for Domino fingerprinting and discovery:

Steps

1) Install IBM Notes on the machine that will host the Forcepoint DLP crawler.
   - After IBM Notes is installed, either Forcepoint DLP server or a standalone crawler instance can be installed on the machine.
   - Forcepoint DLP supports IBM Notes versions 8.5.1, 8.5.2 FP4, and 8.5.3.

   Important

   The crawler used for Domino fingerprinting and discovery must be on the same machine as Notes.

   Be sure that the installation is done for “Anyone who uses this computer.”

2) Log on to Notes and supply a user.id file and password.

3) Connect to the Domino server from the Notes client with the user account that will be used to install the crawler.

   For best practice, do not run Notes on this machine again after the crawler is installed.

Installing the crawler agent

Steps

1) Download the Forcepoint Security Installer (ForcepointDLP1030Setup.exe) from the **Downloads** page of support.forcepoint.com.

2) Launch the installer.

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 folder into which to install the agent.

   The default destination is C:\Program Files *or* Program Files (x86)\Websense\Data Security. If you have a larger drive, 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, the machine must have a minimum of 0.5 GB of free disk space on the C: drive.

8) On the **Select Components** screen, select **Crawler agent** and then **Entire feature will be installed on local hard drive**. If this is a stand-alone installation, deselect all other options, including Forcepoint DLP Server.

9) In the **Server Access** screen, select the IP address to identify this machine to other Forcepoint components.

The following message may appear:
Forcepoint Data Discovery Agent works with a specific version of WinPcap. The installation has detected that your WinPcap version is <version> In order to proceed with this installation, WinPcap version 4.0.0.1040 needs to be installed and will replace yours. Click Yes to proceed or Click No to preserve your WinPcap version and deselect the Discovery Agent Feature to continue with the installation.

"Discovery Agent" refers to the crawler agent. The particular version of WinPcap mentioned in this message must be in place to install Crawler Agent. Note that after installation of the crawler agent you can install a different version of WinPcap. The crawler agent should continue to work properly.

10) In the **Register with the Forcepoint DLP Server** screen specify the path and log on credentials for the Forcepoint DLP server to which this agent will connect. This could be the management server or a secondary Forcepoint DLP server.

FQDN is the fully-qualified domain name of a machine.

11) In the **Local Administrator** screen, enter a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters.

12) If you installed a Lotus Notes client on this machine so you can perform fingerprinting and discovery on a Lotus Domino server, the **Lotus Domino Connections** screen appears.

If you plan to perform fingerprinting or discovery on your Domino server, complete the information on this page.

Important

Before you complete the information on this screen, make sure that you:

- 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 the check box labeled **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.

13) In 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 the following message appears, click **Yes** to continue the installation:

Forcepoint DLP needs port 80 free.

In order to proceed with this installation, DSS will free up this port. Click Yes to proceed OR click No to preserve your settings.

Clicking **No** cancels the installation.

A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.

14) Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.

15) Once installation is complete, the **Installation Successful** screen appears to inform you that your installation is complete.

For information on configure the crawler, see “Configuring the crawler” in the Data Security Manager Help system.

Chapter 4

Installing the Protector

Contents

Protector installations include all of the following:

- A policy engine
- ICAP client (for integration with third-party solutions that support ICAP, such as some web proxies)
- Secondary fingerprint repository (the primary is on the management server)

There are 3 basic steps to installing the Forcepoint DLP protector(refer to the below topics for information regarding theses steps):

1) Make sure all prerequisites are met. See *Protector installation prerequisites*.

2) Perform the installation. See *Before you begin:*(topic under "Protector installation prerequisites").

3) Configure the protector in the Data Security module of the Security Manager. See *Final step: Verify the protector installation*.

Related concepts
Protector installation prerequisites on page 35
Before you begin: on page 36

Related information
Final step: Verify the protector installation

Protector installation prerequisites

This section lists the prerequisites for installing the protector.

Before installing the protector:

- Make sure the hardware that will host the protector soft appliance meets the requirements specified in System requirements for this version.
- Make sure that firewalls and other access control devices on the network do not block ports used by the protector to communicate with the Forcepoint DLP server.
  For port requirements, see Forcepoint DLP ports (the “Protector” section).
- The protector device must have visibility into both incoming and outgoing traffic in the monitored segment.

If incoming and outgoing traffic are on separate links, the mirror port must be configured to send traffic from both links to the protector.

- Make sure the protector machine can communicate with the management server, and vice-versa.

Related information
Installing the Forcepoint DLP Protector software package on page 36

Before you begin:

- If the protector will reside on a Forcepoint DLP Appliance, follow the instructions on the quick start poster to rack, cable, and power on the appliance.
  Note that at least one of the P1, P2, and N interfaces must be configured for monitor mode (it doesn't matter which one).
- If the protector will reside on other hardware:
  1) Connect to the command line via a direct terminal or serial port. For serial port connection, configure the terminal application (for example, HyperTerminal or TeraTerm) as follows:
     - 19200 baud
     - 8 data bits
     - no parity
     - 1 stop bit
     - no flow control
  2) Restart the machine.
  3) An installer page appears. Press **Enter** and the machine is automatically restarted a second time.

  For installation, see *Installation steps for ISO/Appliance Protector*.
- If the protector is deployed in public cloud and is provided as a self-extractor package that can be installed on any Red Hat Enterprise Linux 8.x or Oracle Linux 8.x based system and provides the protector application part (ICAP server and MTA), see *Installing the Forcepoint DLP Protector software package*.

Installing the Forcepoint DLP Protector software package

Pre-installation requirements

Before installing the Forcepoint DLP Protector software, you have to ensure the requirements are met.

- Forcepoint DLP Protector software package is supported on Red Hat Enterprise Linux versions 7.x and 8.x and Oracle Linux 8.x. It is recommended that you upgrade to the latest version.

Note

- Use of Red Hat Enterprise Linux 8.x requires a license key upon installation. Subscriber must separately purchase a license key to Red Hat Enterprise Linux 8 through Red Hat's official channels.

- For software package deployment, verify that the outputs of the two commands match:

  `"hostname -f": --fqdn, --long long host name (FQDN)`

  `"hostname -s": --short short host name`

  If the outputs match, you can continue the installation.

  If the outputs do not match, the fully-qualified domain name (FQDN) (long) should be changed to match the short hostname. To change the FQDN you must open the hosts file located in `/etc/hosts` as root and add the following entry to the hosts file:

  `<Protector IP address> <New Hostname> (match to the short hostname, hostname -s)`

  ```
  127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
  10.139.0.7  ohadpro_onprem
  ::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
  ```

- At least two network interface cards are required.
- For hardware requirements, see Protector Hardware Requirements.
- The file system where /opt directory resides must have a minimum of 45GB disk space.
- SELinux must be disabled before the software protector installation.
- The installation will check whether firewall or NetworkManager are running and disable them if they are running.

Installing Forcepoint DLP Protector software package on Red Hat Enterprise Linux 8.x

When the protector is deployed in public cloud and is provided as a self-extractor package, it can be installed on supported systems.

Steps

1) Download Forcepoint DLP Protector software package, from the **Downloads** page in **My Account** in Forcepoint Customer Hub.

2) Log on as root user to run this installer.

3) Verify that the installation file has executable permissions. If not, run:

   `sudo chmod +x <installation file>`

4) In **Command Prompt**, run the following command:

   `sudo ./<installation file>`

5) Accept the license agreement.
Read the license agreement. At the prompt, select **y** to continue, **n** to exit installation.

```
Do you accept the license agreement [y/n]? y
```

6) Installation begins after file extraction is complete.

7) Register with a Forcepoint DLP server.
In this step, a secure channel will be created connecting the protector to a Forcepoint DLP Server. This can be either the management server or a supplemental server.

   a) Enter the IP address or FQDN of the Forcepoint DLP Server.

   Note

   This must be the IP address identified when you installed the server machine. It cannot be a secondary IP address.

   b) Enter the user name and password for a Forcepoint DLP administrator that has privileges to manage system modules.

8) Verify the protector installation.
In the Data Security module of the Security Manager, verify that the protector status is no longer pending and that the icon displays its active status.

9) Refresh the browser, and then click **Deploy**.

Uninstalling Forcepoint DLP Protector software package

Steps

1) Run the following file as root user: **sudo uninstall.sh**, located at **/opt/websense/** with the next command:

```
sudo./uninstall.sh
```

2) At the prompt, select **y** to uninstall, **n** to exit.

```
Do you want to uninstall this product [y/n]? y
```

3) Press **Enter** to remove the product.

   Important

   After choosing to proceed, do **not** attempt to quit the product removal by pressing Ctrl-C.

4) When product removal is completed, reboot the protector. At the prompt, select **y**to reboot, **n** to exit installation.

```
Do you want to reboot now [y/n]? y
```

Installing Forcepoint DLP Protector on Oracle Linux 8.x

This section outlines the Protector installation procedure on Oracle Linux 8 systems.

The Forcepoint DLP Protector software package can be installed on the following Oracle Linux options:

- Minimal Linux
- Workstation Edition
- Server Edition

Steps

1) Download the Forcepoint DLP Protector software package for Oracle Linux, from the **Downloads** page in **My Account** in Forcepoint Customer Hub.

2) Log on as root user to run this installer.

3) Verify that the installation file has executable permissions. If not, run `chmod +x <installation file>`.

4) Run the installer file by entering `<installation file>`.
   The prerequisites are checked for all types of installation.

5) Disable SELinux in the Server Edition and Minimal Linux.
   a) Enter the command, `vi /etc/selinux/config`.
   b) Edit the file by replacing `SELINUX=enforcing` with `SELinux=disabled`.
   c) Save the file and enter `reboot` to reboot the machine.

   Note

   In the Workstation Edition, SELinux is disabled by default.

6) Run the installer file again to proceed with the installation.

7) To disable the firewall connectivity, enter `y`.

8) To install the network-scripts, enter `y`.
   Network scripts gets successfully installed.

9) To disable the NetworkManager connectivity, enter `y`.
   The user agreement message displays. You can press space to continue reading the agreement.

10) To accept the license agreement, enter `y`.
    The installation prerequisite check will complete and prompt you to add the missing package files.

11) To install the missing packages for the Server Edition installation, enter the command, `yum install java-17-openjdk-headless perl libnsl stunnel rpm-libs`.

12) To install the missing packages for the Workstation Edition installation, enter the command, `yum install java-17-openjdk-headless postfix perl libnsl stunnel rpm-libs`.

13) To install the missing packages for the Minimal Linux installation, enter the command, `yum install cyrus-sasl java-17-openjdk-headless cyrus-sasl-plain postfix perl stunnel python3 rpm-libs libX11 libnsl python3-idna python3-requests libXft libgsf chrony`.

14) To confirm the installation, enter `y`.
The status appears as Complete.

15) Run the installer file again to proceed with the installation.
User agreement message displays. You can press space to continue reading the agreement.

16) To accept the license agreement, enter `y`.
Installation begins after file extraction is complete.

17) Register with a Forcepoint DLP server.
In this step, a secure channel will be created connecting the protector to a Forcepoint DLP Server. This can be either the management server or a supplemental server.

    a) Enter the IP address or FQDN of the Forcepoint DLP Server.

    Note

    This must be the IP address identified when you installed the server machine. It cannot be a secondary IP address.

    b) Enter the user name and password for a Forcepoint DLP administrator that has privileges to manage system modules.

18) Verify the protector installation.
In the Data Security module of the Security Manager, verify that the protector status is no longer pending and that the icon displays its active status.

19) Refresh the browser, and then click **Deploy**.
The Protector is successfully connected to the DLP Manager.

Configuring the protector

To begin monitoring the network for sensitive information loss, configure the protector in the Data Security module of the Forcepoint Security Manager, on the **Settings** > **Deployment** > **System Modules** page.

The basic steps are:

1) Select the protector instance.

2) Define the channels for the protector to monitor.

3) Supply additional configuration parameters needed by the Forcepoint DLP server to define policies for unauthorized traffic.

4) Click **Deploy**.

After making configuration changes, make sure the protector does not have the status

Disabled or **Pending**. (The status is displayed on the **System Modules** page.) For detailed configuration information, see:

- Configuring the Protector in the Forcepoint DLP Administrator Help
- "Configuring the Protector for Use with SMTP" in the Forcepoint DLP Getting Started Guide.

Chapter 5

Installing Web Content Gateway

Contents

The Web Content Gateway is included with Forcepoint DLP Network. It provides DLP policy enforcement for the web channel, including decryption of SSL traffic, user authentication, and content inspection using the DLP policy engine.

This core Forcepoint DLP component permits the use of custom policies, fingerprinting, and more. It is available as Linux software that does not require Forcepoint Web Security.

Note that Web Content Gateway is inactive until registered with a management server.

Note

Make sure the server hosting the Content Gateway has external connectivity allowed and can reach the domains listed below.

- download.forcepoint.com
- ddsdom.forcepoint.com
- ddsint.forcepoint.com
- download.websense.co

A constant access to these domains is recommended as various product services, including (but not limited to) URL database, AV definitions and licensing, need open connection with Forcepoint for the purpose of maintenance, update or validation. DNS queries can narrow down the relevant servers for your location. Prolonged periods without connectivity of more than two weeks may result in license invalidation and policy enforcement may no longer occur.

Preparing the operating system for Content Gateway

1) See the Certified Product Matrix for a list of supported operating systems.

2) Make sure that the server you intend to use meets or exceeds the requirements listed in the “Content Gateway” section of “Requirements for web protection solutions” in System requirements for this version. See *Installing on Red Hat Enterprise Linux 6, update 9 and higher* for additional details on installing on Red Hat Linux 6.

3) Configure a hostname for the Content Gateway machine and also configure DNS name resolution. Complete these steps on the machine on which you will install Content Gateway.

   a) Configure a hostname for the machine that is 15 characters or less:

   ```
   hostname <hostname>
   ```

b) Update the HOSTNAME entry in the **/etc/sysconfig/network** file to include the new hostname assigned in the previous step:

```
HOSTNAME=<hostname>
```

c) Specify the IP address to associate with the hostname in the **/etc/hosts** file. This should be static and not served by DHCP.
The proxy uses this IP address in features such as transparent authentication and hierarchical caching. This must be the first line in the file.

Do not delete the second and third lines (the ones that begin with “127.0.0.1” and “::1”, respectively). Also, do not add the hostname to the second or third line.

```
xxx.xxx.xxx.xxx <FQDN> <hostname>
```

```
127.0.0.1 localhost.localdomain localhost
```

```
::1 localhost6.localdomain6 localhost6
```

<*FQDN*> is the fully-qualified domain name of this machine (for example: myhost.example.com). <*hostname*> is the same name specified in Step a.

Do **not** reverse the order of the FQDN and hostname.

d) Configure DNS in the **/etc/resolv.conf** file.

```
search <subdomain1>.<top-level domain>
```

```
<subdomain2>.<top-level domain> <subdomain3>.<top- level domain>
```

```
nameserver xxx.xxx.xxx.xxx nameserver xxx.xxx.xxx.xxx
```

This example demonstrates that more than one domain can be listed on the search line. Listing several domains may have an impact on performance, because each domain is searched until a match is found. Also, this example shows a primary and secondary nameserver being specified.

e) Gather this information:

- Default gateway (or other routing information)
- List of your company’s DNS servers and their IP addresses
- DNS domains to search, such as internal domain names. Include any legacy domain names that your company might have.
- List of additional firewall ports to open beyond SSH(22) and the proxy ports (8080-8090).

4) For Content Gateway to operate as a caching proxy, it must have access to at least one raw disk. Otherwise, Content Gateway will function as a proxy only.
To create a raw disk for the proxy cache when all disks have a mounted file system:

Note

This procedure is necessary only if you want to use a disk already mounted to a file system as a cache disk for Content Gateway. Perform this procedure **before** installing Content Gateway.

Warning

Do not use an LVM (Logical Volume Manager) volume as a cache disk.

Warning

The Content Gateway installer will irretrievably clear the contents of cache disks.

a) Enter the following command to examine which file systems are mounted on the disk you want to use for the proxy cache:

```
df -k
```

b) Open the file /etc/fstab and comment out or delete the file system entries for the disk.

c) Save and close the file.

d) Enter the following command for each file system you want to unmount:

```
umount <file_system>
```

When the Content Gateway installer prompts you for a cache disk, select the raw disk you created.

Note

It is possible to add cache disks after Content Gateway is installed. For instructions, see the Content Gateway Manager Help.

5) If you plan to deploy multiple, clustered instances of Content Gateway:

- Find the name of the network interface you want to use for cluster communication. This must be a dedicated interface.
- Find or define a multicast group IP address.
  If a multicast group IP address has not already been defined, enter the following at a command line to define the multicast route:

  ```
  route add <multicast.group address>/32 dev <interface_name>
  ```

  Here, <*interface_name*> is the name of the interface used for cluster communication. For example:

  ```
  route add 224.0.1.37/32 dev eth1
  ```

6) It is recommended that the Content Gateway host machine have Internet connectivity before starting the installation procedure. The software will install without Internet connectivity, but analytic database updates cannot be performed until Internet connectivity is available.

7) Use the Download tab of the My Account page at support.forcepoint.com to download the **ContentGateway853Setup_Lnx.tar.gz** installer tar archive to a temporary directory on the machine that will host Content Gateway.
To unpack the tar archive, use the command:

```
tar -xvzf ContentGateway853Setup_Lnx.tar.gz
```

8) Consider the following security issues prior to installing Content Gateway:

- Physical access to the system can be a security risk. Unauthorized users could gain access to the file system, and under more extreme circumstances, examine traffic passing through Content Gateway. It is strongly recommended that the Content Gateway server be locked in an IT closet and that a BIOS password be enabled.
- Ensure that root permissions are restricted to a select few persons. This important restriction helps preclude unauthorized access to the Content Gateway file system.

- For a list of default ports, see the Web tab of the Forcepoint Ports spreadsheet. They must be open to support the full set of Forcepoint DLP features.

  Note

  If you customized any ports that your web protection software uses for communication, replace the default port with the custom port you implemented.

  Restrict inbound traffic to as few other ports as possible on the Content Gateway server. In addition, if your subscription does not include certain features, you can restrict inbound traffic to the unneeded ports. For example, if your subscription does not include the Forcepoint Web Security DLP Module, you may choose to restrict inbound traffic to those ports related to Forcepoint DLP.
- If your server is running the Linux IPTables firewall, you must configure the rules in a way that enables Content Gateway to operate effectively. See IP Tables for Content Gateway.

9) Content Gateway can be used as an explicit or transparent proxy. For setup considerations for each option, see the Content Gateway explicit and transparent proxy deployments.

Installing on Red Hat Enterprise Linux 6, update 9 and higher

biosdevname

Red Hat Enterprise Linux 6, update 1 introduced **biosdevname**:

... optional convention for naming network interfaces. biosdevname assigns names to network interfaces based on their physical location. biosdevname is disabled by default, except for a limited set of Dell systems.

The biosdevname convention is designed to replace the older, inconsistent “eth#” naming scheme. The new standard will be very helpful when it is fully adopted, but that is still in the future.

In this release, biosdevname is not supported by Content Gateway.

Disabling biosdevname

If while installing Content Gateway the installer finds non-eth# interface names, the installer quits and provides a link to instructions for modifying system startup files.

There are 2 ways to disable biosdevname:

1) During operating system installation.

2) Post-operating system installation through modification of several system files and other activities.

The easiest way to disable biosdevname is to do it during operating system installation. This is the recommend method.

Disabling biosdevname during operating system installation:

When the installer starts, press Tab and alter the boot line to add **biosdevname=0** and, when installing on Red Hat Enterprise Linux 7.x, **net.ifnames=0** as follows:

Proceed through the rest of the installer as usual.

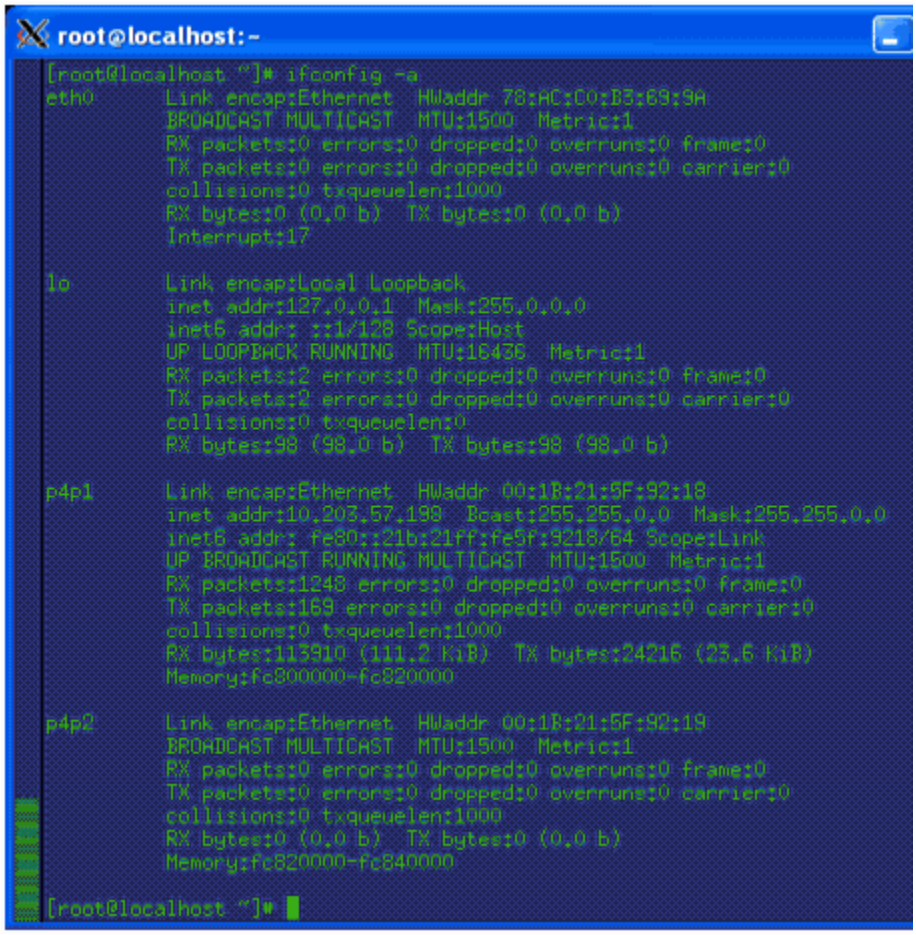
Disabling biosdevname after operating system installation:

Log on to the operating system and verify that non-eth# names are present.

```
ifconfig -a
```

If only “eth#” and “lo” names are present, you are done. No other actions are required.

If there are names like “emb#” or “p#p#” perform the following steps.



1) Log in as **root**.

2) Navigate to the **network-scripts** directory:
`cd /etc/sysconfig/network-scripts`

3) Rename all “ifcfg-<ifname>” files except “ifcfg-lo” so that they are named **ifcfg-eth#**.

   a) Start by renaming **ifcfg-em1** to **ifcfg-eth0** and continue with the rest of the “ifcfg-em#” files.

   b) When the above are done, rename the “ifcfg-p#p#” files.
   If there are multiple **ifcfg-p#p1** interfaces, rename all of them in the order of the lowest **ifcfg-p#** first.

   For example, if the initial set of interfaces presented by **ifconfig -a** is:

   `em1 em2 em3 em4 p1p1 p1p2 p2p1 p2p2`

   Then:

   `em1 -> eth0`

   `em2 -> eth1`

   `em3 -> eth2`

   `em4 -> eth3`

   `p1p1 -> eth4`

   `p1p2 -> eth5`

   `p2p1 -> eth6`

```
p2p2 -> eth7
```

c) Make the **ifcfg-eth#** files linear so that if you have 6 interfaces you have eth0 through eth5.

4) Edit all the **ifcfg-eth#** files.
   a) Update the **DEVICE=** sections to refer to the new name: “**eth#**”
   b) Update the **NAME=** sections to refer to the new name: “**System eth#**”

5) Remove the old udev device mapping file if it exists:
```
rm -f /etc/udev/rules.d/70-persistent-net.rules
```

6) Modify the **grub.conf** file to disable **biosdevname** for the kernel you boot:
   a) Edit the **/boot/grub/grub.conf** file.
   b) Add the following to the end of the “kernel /vmlinuz” line:
```
biosdevname=0
```

7) Reboot the machine.

8) Reconfigure the interfaces as required.

Installer gives NetworkManager or avahi-daemon error

When Red Hat Enterprise Linux 6 is installed with a graphical user interface (GUI), the Content Gateway installer recognizes systems running NetworkManager or avahi- daemon processes and emits an error similar to the following:

```
Error: The avahi-daemon service is enabled on this system and must be disabled before Content Gateway v8.5.x can be installed.
```

```
Please disable the avahi-daemon service with the following commands and restart the Content Gateway installation.
```

```
chkconfig --levels 2345 avahi-daemon off
```

```
service avahi-daemon stop
```

Warning

Content Gateway is supported on Red Hat Enterprise Linux 6, Basic Server (no GUI) and is **not** supported on Red Hat Enterprise Linux 6 with a GUI.

To continue, the conflicting NetworkManager and avahi-daemon processes must be stopped.

1) To disable the avahi-daemon service, enter the following commands:
```
chkconfig --levels 2345 avahi-daemon off
```

```
service avahi-daemon stop
```

2) Restart the installer:
```
./wcg_install.sh
```

Install Content Gateway

Steps

1) Disable any currently running firewall on this machine for the duration of Content Gateway installation. Bring the firewall back up after installation is complete, opening ports used by Content Gateway.

Important

If SELinux is enabled, set it to permissive or disable it before installing Content Gateway. Do not install or run Content Gateway with SELinux enabled.

Important

Forcepoint Web Security customers using Red Hat Enterprise Linux or CentOS 7.x must disable firewall prior to installing Content Gateway.

On the machine where Content Gateway will be installed, execute the following:

```
systemctl stop firewalld
```

```
systemctl disable firewalld
```

2) Make sure you have root permissions:
```
su root
```

3) In the directory where you unpacked the tar archive, begin the installation, and respond to the prompts to configure the application.
```
./wcg_install.sh
```
The installer installs Content Gateway in /opt/WCG. It is installed as **root**.

Note

Up to the configuration summary, you can quit the installer by pressing Ctrl-C. If you choose to continue the installation past the configuration summary and you want to quit, do **not** use Ctrl-C. Instead, allow the installation to complete and then uninstall it.

If you want to change your answer to any of the installer prompts, you will be given a chance to start over at the first prompt once you reach the configuration summary; you do not have to quit the installer.

4) If your server does not meet the minimum hardware requirements or is missing required operating system packages, you will receive error or warning messages.

   Install the missing packages and again start the Content Gateway installer.
   Here is an example of a system resource warning:

   ```
   Warning: Content Gateway requires at least 6 gigabytes of RAM.
   Do you wish to continue [y/n]?
   ```

   Enter **n** to end the installation and return to the system prompt.

   Enter **y** to continue the installation. If you choose to run Content Gateway after receiving this warning, performance may be affected.

5) Read the subscription agreement. At the prompt, enter **y** to continue installation or**n** to cancel installation.

   ```
   Do you accept the above agreement [y/n]? y
   ```

Completing the installation wizard

Steps

1) Enter and confirm a password for the Content Gateway Manager administrator account:

   ```
   Enter the administrator password for the Forcepoint Content Gateway management interface.
   Username: admin
   Password:> (note: cursor will not move as you type)
   Confirm password:>
   ```

   This account enables access to the management interface for Content Gateway (the Content Gateway manager). The default user name is **admin**.

   To create a strong password (required), use 8 to 15 characters, with at least 1 each of the following: upper case letter, lower case letter, number, special character.

   Important

   The password cannot contain the following characters:

   - space
   - $ (dollar symbol)
   - : (colon)
   - ‘ (backtick; typically shares a key with tilde, ~)
   - \ (backslash)
   - “ (double-quote)

   Note

   As you type a password, it may seem that nothing is happening—the cursor will not move nor will masked characters be shown—but the characters are being accepted. After typing a password, press Enter. Then repeat to confirm it.

2) Enter an email address where Content Gateway can send alarm messages:

```
Forcepoint Content Gateway requires an email address for alarm notification.
Enter an email address using @ notation: [] >
```

Be sure to use @ notation (for example, user@example.com). Do not enter more than 64 characters for this address.

3) When prompted, select **2** to configure the Content Gateway as a component of Forcepoint DLP Network (without Forcepoint Web Security).

4) When prompted, enter the IPv4 address of the management server. Use dot notation (i.e., xxx.xxx.xxx.xxx).

5) Review default Content Gateway ports.

- Change a port assignment if it will conflict with another application or process on the machine. Otherwise, leave the default assignments in place.
- Any new port numbers must be between 1025 and 65535, inclusive.

6) For clustering, at least two network interfaces are required. If the machine has only one, the following prompt appears:

```
Content Gateway requires at least 2 interfaces to support clustering. Only one active network interface is detected on this system
```

Press **Enter** to continue installation and skip to Step 13.

7) If two or more network interfaces are found on the machine, a prompt asks whether Content Gateway should be part of a cluster:

- If this instance of Content Gateway will not be to be part of a cluster, enter 2.
- If 1 is selected, provide information about the cluster as follows:

  a) The name of the Content Gateway cluster.
  All members of a cluster must use the same cluster name.

  b) The network interface for cluster communication.

  c) A multicast group address for the cluster.

8) For Content Gateway to act as a web cache, a raw disk must be present on this machine. If no raw disk is detected, the following prompt appears:

```
No disks are detected for cache.
Forcepoint Content Gateway will operate in PROXY_ONLY mode.
```

Content Gateway will operate as a proxy only and will not cache web pages. Press Enter to continue the installation and skip Step 15.

9) If a raw disk is detected, optionally enable the web cache feature:

> **Note**
>
> Cache disks may also be added after Content Gateway has been installed. For instructions, see the Content Gateway Manager Help.

a) Select available disks from the list. Selected disks become dedicated cache disks and cannot be used for any other purpose. Cache disks must be raw. Aggregate disk cache size should not exceed 147 GB.

> **Warning**
>
> Although it might be listed as available, do **not** use an LVM (Logical Volume Manager) volume as a cache disk.

b) Indicate whether to add or remove disks individually or as a group.

c) Specify which disk or disks to use for the cache.

d) The selections are confirmed. Note the “x” before the name of the disk.

```
Here is the current selection
[X] (1) /dev/sdb 146778685440 0x0
```

e) Continue based on the choice in Step b, pressing **X** when you have finished configuring cache disks.

10) A configuration summary appears, showing your answers to the installer prompts.

- To make changes, enter **n** to restart the installation process at the first prompt.
- To continue and install Content Gateway configured as shown, enter **y**.

> **Important**
>
> After choosing to proceed, do **not** attempt to quit the installer by pressing Ctrl-C. Allow the installation to complete. Then uninstall it.

Finishing the installation process

Steps

1) Wait for the installation to complete.

2) When installation is complete, reboot the Content Gateway server.

3) When the reboot is complete, use the following command to check Content Gateway status:

```
/opt/WCG/WCGAdmin status
```

All services should be running. These include Content Cop, Content Gateway, and Content Gateway Manager.

Initial configuration steps for the Web Content Gateway can be found in the Forcepoint DLP Getting Started Guide.

Chapter 6

Adding, Modifying, or Removing Components

Contents

The topics in this chapter provide instructions for:

Related tasks

Adding or modifying Forcepoint DLP components on page 55
Recreating Forcepoint DLP certificates on page 56
Repairing Forcepoint DLP components on page 56
Changing the Forcepoint DLP service account on page 57
Configuring encrypted connection to SQL Server on page 58
Removing Forcepoint DLP components on page 59

Adding or modifying Forcepoint DLP components

1) To start the Forcepoint Security Installer:
   - If the extracted installation files were saved after the initial installation, select **Forcepoint Security Setup** from the Windows Start screen (or from the Forcepoint folder in the Start menu) to start the installer without having to re- extract files.
   - Otherwise, double-click the installer ForcepointDLP1030Setup.exe.

2) On the Modify Installation screen, click **Modify** next to Forcepoint DLP.

3) In the installation wizard, select **Modify**.
   To add components, select them on the Select Components screen.

Refer to the following sections for the most common Forcepoint DLP modify procedures:

Related tasks
Recreating Forcepoint DLP certificates on page 56

Recreating Forcepoint DLP certificates

The Modify menu includes an option to re-certify the server. This is not recommended except in extreme security breaches. When security certificates are recreated:

- All agents and servers must re-register (see Re-registering Forcepoint DLP components for instructions).
- All agents and servers must repeat the Reestablish Connection process.
- All endpoint clients must be reinstalled. This requires the following steps:
  1) Uninstall the existing endpoint software.
  2) Create a new endpoint package (the existing package cannot be reused).
  3) Use SMS or a similar mechanism to install the new package on the endpoints.
     See Installing and Deploying Endpoint Clients for more information on uninstalling endpoints.

When it first authenticates, the management server trades certificates with the other servers and endpoints in the network.

To re-run the security communication between Forcepoint DLP components:

1) Start the Forcepoint Security Installer:
   - If extracted installation files were saved, select **Forcepoint Security Setup**from the Windows Start screen or the Forcepoint folder in the Start menu.
   - If the shortcut does not exist, double-click the installer executable.
2) In Modify Installation dashboard, click the **Modify** link for Forcepoint DLP.
3) In the installation wizard, select **Modify**.
4) On the Recreate Certificate Authority screen, select **Recreate Certificate Authority**.
5) Complete the installation wizard as prompted.

Repairing Forcepoint DLP components

To initiate the repair process:

1) Start the Forcepoint Security Installer:
   - If extracted installation files were saved, select **Forcepoint Security Setup**from the Windows Start screen or the Forcepoint folder in the Start menu.

- If the shortcut does not exist, double-click the installer executable.

2) In Modify Installation dashboard, click the **Modify** link for Forcepoint DLP.

3) In the installation wizard, select **Repair**.

4) Complete the installation wizard as prompted.

This restores the installed configuration to its last successful state. This can be used to recover from various corruption scenarios, such as binary files getting deleted, registries getting corrupted, and so on.

Changing the Forcepoint DLP service account

The Forcepoint DLP service account user name cannot be changed. Doing so can cause the system to behave in unexpected ways. For example, services may not be able to start and encryption keys may not work.

To change the password for the service account:

Steps

1) Modify the service account password from the domain's Active Directory or use Windows. From Windows:
   a) Log onto the management server with the service user account.
   b) Press **Ctrl +Alt +Delete** to access the Windows lock screen, then select **Change Password**.

2) Modify the Forcepoint Management Infrastructure.
   a) Log on to the management server with the service user account.
   b) Run Forcepoint Security Installer (**ForcepointDLP1040Setup.exe**).
   c) Select **Modify**.
   d) During Forcepoint Management Infrastructure setup, change the password on the following screen. These are the credentials that the management server uses when running services or logging on to other machines. The password must:
      - Be at least 8 characters
      - Contain upper case characters
      - Contain lower case characters
      - Contain numbers
      - Contain non-alphanumeric characters
   e) Complete the Forcepoint Management Infrastructure wizard using the defaults.

3) Modify the Forcepoint DLP installation.
   a) Continue the wizard to access the Forcepoint DLP installer.
   b) Change the password on the Local Administrator screen. Use the same password as in the Forcepoint Management Infrastructure. This is the password used to access this server during component installation and operation.
   c) Finish the wizard.
4) Log on to the Data Security module of the Security Manager, then click **Deploy**.

Configuring encrypted connection to SQL Server

Forcepoint Security Manager communicates with your organization's SQL Server database. It is recommended to implement SSL encryption for these communications to increase the level of security in the SQL database. If you did not enable an encrypted connection to SQL Server during installation, use the following steps after installation to enable the encrypted connection.

Steps

1) From the Windows Start menu, click **Forcepoint Security Setup**.
   The Forcepoint Security Setup Installer Dashboard displays. The Installer Dashboard stays on-screen during installation. Various subinstallers and dialog boxes are displayed over it.
2) From Forcepoint Management Infrastructure, click **Modify**.
   The Forcepoint Management Infrastructure Setup wizard displays.
3) Click **Next** on the Welcome and Installation Directory screens.
4) On the SQL Server screen, mark the check box **Encrypt connection** and click **Next**.
5) Complete the Forcepoint Management Infrastructure Setup wizard and click **Finish**.
   If you have additional Forcepoint products installed, they must also be modified. All installed products display on the Forcepoint Security Setup Installer Dashboard.
6) From Forcepoint Web Security, Forcepoint DLP, or Forcepoint Email Security, click **Modify**.
   The relevant setup wizard displays.
7) Repeat steps 3–5 for each Forcepoint product.
8) On the Forcepoint Security Installer Dashboard, click **Close**.

Removing Forcepoint DLP components

Forcepoint DLP components must be removed all at once. Individual components cannot be selected for removal.

Warning

Forcepoint Email Security requires Forcepoint DLP to be installed. If you are using Forcepoint Email Security, do not uninstall Forcepoint DLP or Forcepoint Email Security will quit working.

Do not uninstall the Forcepoint Management Infrastructure before removing Forcepoint DLP.

For instructions on removing a Forcepoint DLP Endpoint, see Uninstalling endpoint software .

To remove Forcepoint DLP components:

Steps

1) To start the Forcepoint Security Installer:
   - If the extracted installation files were saved after the initial installation, select **Forcepoint Security Setup** from the Windows Start screen (or from the Forcepoint folder in the Start menu) to start the installer without having to re- extract files.
   - Otherwise, double-click the installer executable.
2) In the Modify Installation dashboard, click the **Modify** link for Forcepoint DLP.
3) At the Welcome screen, click **Remove**.
4) At the Forcepoint DLP Uninstall screen, click **Uninstall**.

   Important

   This removes all Forcepoint DLP components from this machine.

   The Installation screen appears, showing removal progress.
5) At the Uninstallation Complete screen, click **Finish**.
   The Modify Installation dashboard is displayed.

   Note

   The Secondary Forcepoint DLP server must be uninstalled from the Windows Control Panel and not from the Forcepoint Security Installer.

Chapter 7

Appendix A:DLP Installation in Cloud Providers

Contents

Installing Forcepoint DLP in AWS

This section provides the necessary information to complete the deployment process of Forcepoint DLP in AWS.

Starting in Forcepoint DLP v8.9, customers can install Forcepoint Security Manager and a supplemental Forcepoint DLP server as an endpoint server in Amazon Web Services (AWS).

Note

Forcepoint recommends that Very Large Enterprises (VLE) use AWS's high-performance Solid State Drives (SSDs) for SQL to significantly improve performance, making long processes, such as large Active Directory (AD) imports much faster.

Important

This chapter provides the information needed to install Forcepoint Security Manager and Forcepoint DLP in AWS, but does not cover the procedures specific to AWS. For more information about configuring AWS, see the AWS Documentation.

Prerequisites

- Provision EC2s with a supported version of Windows and Linux, according to Forcepoint hardware requirements available in the System requirements for this version document. Also, use a supported SQL server to host the Forcepoint Security Manager data. See the Certified Product Matrix for supported versions of SQL Server.
- Configure the virtual private cloud (VPC) and security groups according to your company policy and AWS best practices.
- Open the relevant ports for the security group, including RDP port, located in the Forcepoint DLP ports document. The Forcepoint Security Manager itself and its components will use the same security group, so ports should be added in both inbound and outbound. In **Source**, specify the range of desired IP addresses or the desired security group.

- Forcepoint DLP requires a static IP, so allocate a static IP for the Forcepoint Security Manager. You may want to use an elastic IP if you would like to connect to the Forcepoint Security Manager user interface from an external network.

Installing Forcepoint Security Manager and Forcepoint DLP

Steps

1) Launch the Forcepoint Security Manager EC2 instance.
2) Connect to the EC2 Windows instance where you want to install Forcepoint Security Manager.
3) Install .NET 3.5 and Telnet client features on the Forcepoint Security Manager server.
4) Copy the installation file to the server where the Forcepoint Security Manager server will be located. This can be done through any available cloud storage, such as AWS S3, OneDrive, Dropbox, and SharePoint.
5) Run the installation file on the Forcepoint Security Manager server according to the standard Forcepoint procedure. Restart the machine (if needed), apply the subscription provided by Forcepoint, then click **Deploy**.

Installing the supplemental server to be used as an endpoint server

Steps

1) Launch the Windows EC2 where you want to install the Forcepoint DLP supplemental server.
2) Configure the VCP and security groups according to your company policies and AWS best practices.
3) Choose an instance type according to the hardware requirements and your company preferences.
4) Install .NET 3.5 and Telnet client features on the supplemental server.
5) Copy the installation file to the server where the supplemental server will be located.
6) Set up network settings on the supplemental server, which requires a static IP.
7) Run the installation file on the supplemental server machine according to the standard Forcepoint procedure. Restart the machine if needed.
8) Go to the main Forcepoint Security Manager server, deploy, then check that the supplemental server appears in the system modules.

Installing Forcepoint DLP in Azure

This section provides the necessary information to complete the deployment process of Forcepoint DLP in Azure.

This covers the deployment of the Forcepoint Security Manager, Forcepoint DLP Manager, and the Forcepoint DLP supplemental server on Azure cloud.

Note

Forcepoint recommends that Very Large Enterprises (VLE) use Azure's high-performance Solid State Drives (SSDs) for SQL to significantly improve performance, making long processes, such as large Active Directory (AD) imports much faster.

Refer to the below tasks to perform instructions for:

Related tasks

Installing Forcepoint Security Manager and Forcepoint DLP on page 63
Installing the Supplemental Server to be used as an Endpoint Server on page 64
Setting up the public IP address or DNS name for the Endpoint Server on page 64

Prerequisites:

- Provision VM with a supported version of Windows server, according to Forcepoint hardware requirements available in the System requirements for this version document. Also, use a supported SQL server to host the Forcepoint Security Manager data. See the Certified Product Matrix for supported versions of SQL Server.
- Open the relevant ports for the network security group (if any network security group already exists), including the RDP port, mentioned in the Forcepoint DLP ports document.
- Forcepoint DLP requires a static IP, so allocate a private static IP for the Forcepoint Security Manager.
- Install the .NET Framework 3.5.
- Check that the Microsoft Visual C++ Redistributable is installed according to the Forcepoint software requirements.
- To get an Endpoint (on-prem) connected to the Endpoint server, you need to set up the public IP address or DNS name of the Endpoint server VM.

Note

Underscore characters are not permitted in domain names.

Installing Forcepoint Security Manager and Forcepoint DLP

Steps

1) Copy the installation file to the dedicated VM.

2) Run the installation file on the Forcepoint Security Manager server according to the standard Forcepoint procedure. Restart the machine if needed.

Installing the Supplemental Server to be used as an Endpoint Server

Steps

1) Copy the installation file to the dedicated VM.

2) Run the installation file on the supplemental server according to the standard Forcepoint procedure. Restart the machine if needed.

3) Go to the Forcepoint Security Manager server, click on the **Deploy** button and check that the supplemental server appears in the system modules.

Setting up the public IP address or DNS name for the Endpoint Server

Steps

1) Go to the **Settings** > **Deployment** > **System Modules** page in the **Data Security**module of the Forcepoint Security Manager

2) Click a module.

3) Enter the IP address or DNS name into the Fully Qualified Domain Name (FQDN) field.

4) Deploy the settings.

Installing Forcepoint DLP in Google Cloud Platform

This section provides the necessary information to complete the deployment process of Forcepoint DLP in (GCP).

Starting with Forcepoint DLP 9.0, customers can install Forcepoint Security Manager and its components on the Google Cloud Platform (GCP).

Note

Forcepoint recommends that Very Large Enterprises (VLE) use GCP's high-performance Solid State Drives (SSDs) for SQL to significantly improve performance, making long processes, such as large Active Directory (AD) imports much faster.

Prerequisites

- Provision of the VM instances on GCP as per Forcepoint supported hardware requirements available in the System requirements.
- Configure the networking as per need and open relevant ports, including RDP port, listed in the Forcepoint DLP ports document for both inbound/outbound communication in GCP Firewall.
- Forcepoint DLP requires a static IP, so allocate a private static IP for the Forcepoint Security Manager, SQL server and Supplemental server.
- Install MS SQL Server, use the supported SQL to host Forcepoint Security Manager data as listed in the Certified Product Matrix for supported versions and run the scripts provided by Forcepoint support to configure it for FSM installation.
- Enable an External IP for the instance. It is mandatory for the server, which will contain the Endpoint Server (main FSM or Supplemental Server, or both). Note that for functioning of FSM system, the External IP address should be reserved as static one.

Installing Forcepoint Security Manager and Forcepoint DLP

Steps

1) In the menu of instance, click **Connect** and set the windows password. Next, download the RDP file and then connect via RDP to the instance.

2) Install .NET 3.5, Telnet Client and other needed software on the server that will run the Forcepoint Security Manager.

3) Copy to the server, where FSM will be located, the installation file. This can be done through any available cloud storage (Google Cloud Storage, AWS S3, OneDrive, Dropbox, SharePoint etc.).

4) Run installation file on FSM machine according to standard Forcepoint procedure. Reboot the machine if needed, apply the subscription provided by Forcepoint, then click **Deploy**.

5) If you want to have the Endpoint Server on Forcepoint Security Manager, you need to assign a static External IP for this machine. After getting the External IP, you must add it to properties of the Endpoint Server: **DLP manager** > **Deployment** > **System Modules** > **Forcepoint DLP Server** > **Endpoint Server** > **FDQN**, and then enter the External IP. However, if you want the main FSM DLP server to be the primary Endpoint Server, then you do not need to do anything else on this machine.

Installing the Supplemental Server to be used as an Endpoint Server

Steps

1) In the menu of instance, click **Connect** and set the windows password. Next, download the RDP file and then connect via RDP to the instance.

2) Install .NET 3.5 and other needed software on the server that will run the Supplemental Server.

3) Copy to the server the installation file. This can be done through any available cloud storage (Google Cloud Storage, AWS S3, OneDrive, Dropbox, SharePoint etc.).

4) Run installation file according to standard Forcepoint procedure. Reboot the machine if needed.

5) If you want to have the Endpoint Server on the Supplemental Server, you need to assign a static External IP for this machine. After getting the External IP, you must add it to the properties of Endpoint Server: **DLP manager** > **Deployment** > **System Modules** > **Supplemental Server** > **Endpoint Server** > **FDQN**, and then enter the External IP. If you want Secondary server to be the primary Endpoint Server, navigate to Endpoint Profiles, and create/select a profile and in Servers, make the Secondary server as the primary Endpoint Server.

6) On FSM instance, copy the endpoint package builder, received from Forcepoint. Place all files from the package to %DSS_HOME%client and run the package builder. Enter the External IP of FSM GCP instance, from where the endpoint will get settings updates.

7) Copy the endpoint installer to the endpoint and run the installer. Reboot if needed and check the status on the endpoint interface when done. It must show connection status and a time of policy update.

8) On the FSM interface, check for the newly added endpoint.

Chapter 8

Appendix B: Maintenance Release Installation

Contents

Maintenance installers are delivered for a specific DLP version. There are two maintenance installers:

1) Forcepoint Management Infrastructure Maintenance Release Installer - Includes fixes for the Forcepoint Security Manager's global setting interface.

2) Forcepoint DLP Maintenance Release Installer - Includes fixes for a specific Forcepoint DLP version.

Forcepoint DLP Maintenance packages are supported on the DLP Manager.

For information on the maintenance upgrade, see Forcepoint DLP Upgrade Guide v10.4.

For details on specific maintenance releases, refer to the corresponding release notes in the table.

Forcepoint DLP Maintenance Release Version	Release Note
10.3.1	Forcepoint DLP Release Notes v10.3.1

About the Maintenance Release

This section provides information on the maintenance release installation.

Maintenance installers can be applied directly to the corresponding Forcepoint DLP version, and multiple maintenance releases may be available for a given DLP version. You can install a maintenance release version on top of the base version, even if previous maintenance releases have not been installed.

To install the Forcepoint DLP 10.3.X maintenance release package, you must install the 10.3 base version on your system. A maintenance release can only be applied to the top of its corresponding base version. When you install a new maintenance release, the existing files from the previous version will be replaced with the updated files from the new release.

Each maintenance version is available for download on the Forcepoint support site. In **Products**, you must select **Data Loss Prevention (DLP)**, and then download and install the following package files from the **DLP Core** section:

- Forcepoint DLP Maintenance release (`Forcepoint_DLP_Maintenance_Release_10.3.X.YYY.exe`)

- Forcepoint Management Infrastructure Maintenance release (`Forcepoint_EIP_Maintenance_Release_10.3.X.YYY.exe`)

Note

Forcepoint DLP 10.3.X maintenance package is the maintenance release for the DLP Security Manager, and not for Secondary/Supplemental DLP Servers.

The maintenance release installers must be executed using the same service user that was used to install the product.

Installing the Maintenance Release

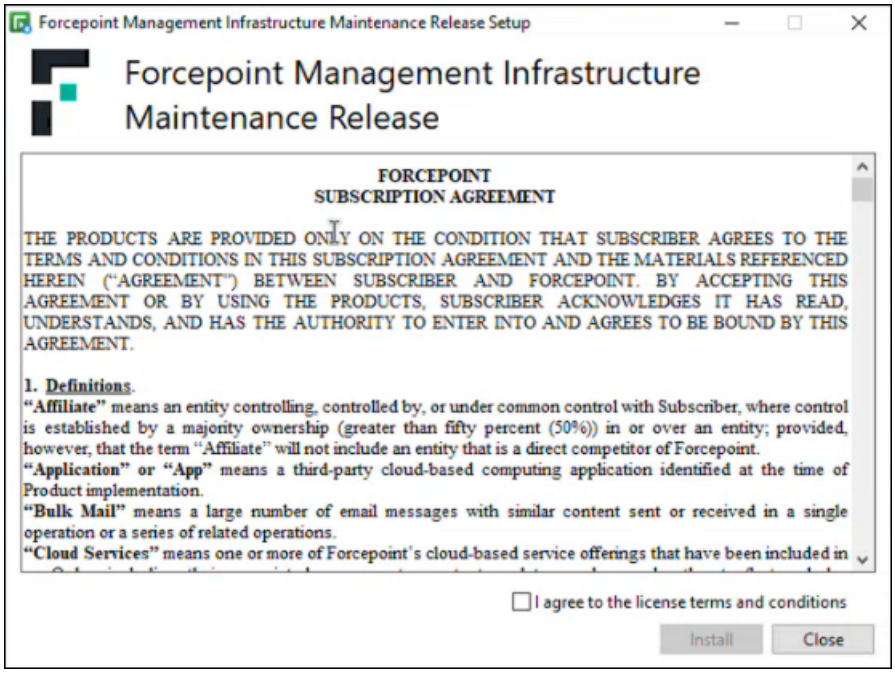
This section outlines the steps to install the Forcepoint Management Infrastructure maintenance and Forcepoint DLP maintenance files on your system.

Before you begin

Ensure that you have downloaded the Forcepoint Management Infrastructure Maintenance release (`Forcepoint_EIP_Maintenance_Release_10.3.X.YYY.exe`) file and the Forcepoint DLP Maintenance release (`Forcepoint_DLP_Maintenance_Release_10.3.X.YYY.exe`) file from the Forcepoint support site.

Steps

1) To install the maintenance release for Forcepoint Management Infrastructure, do the following:
   a) Double-click the `Forcepoint_EIP_Maintenance_Release_10.3.X.YYY.exe` file.
   The **Forcepoint Management Infrastructure Maintenance Release Setup** dialog opens.



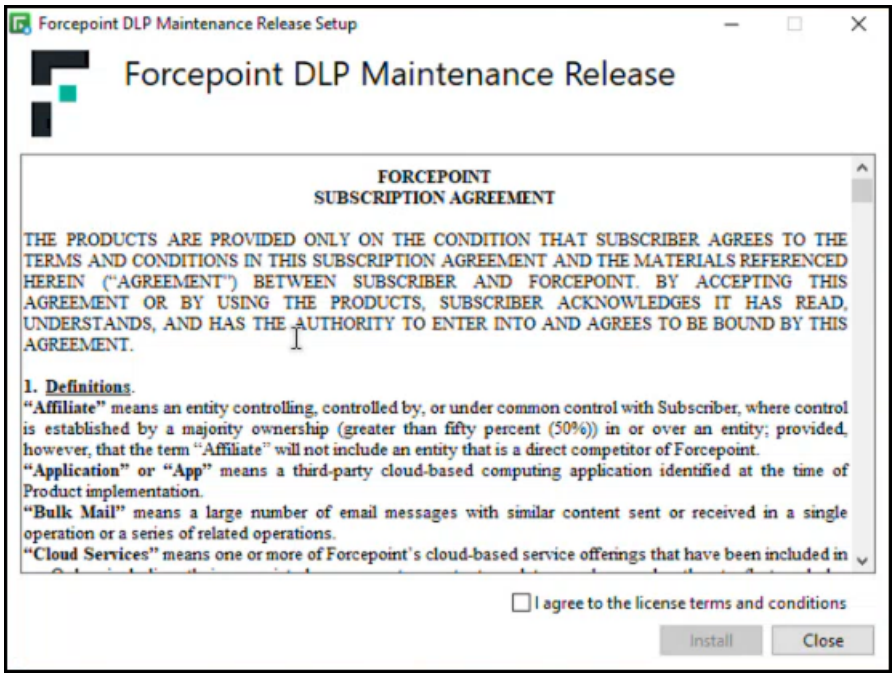
b) Select **I agree to the license terms and conditions**, and then click **Install**.

The **Setup Progress** runs, and the installation completes successfully. The Forcepoint Security Manager build number is then updated to reflect the new maintenance build version.

2) To install the maintenance release for Forcepoint DLP, do the following:

a) Double-click the `Forcepoint_DLP_Maintenance_Release_10.3.X.YYY.exe` file.

The **Forcepoint DLP Maintenance Release Setup** dialog opens.



b) Select **I agree to the license terms and conditions**, and then click **Install**.

The **Setup Progress** runs, and the installation completes successfully. The Forcepoint DLP build number is then updated to reflect the new maintenance build version.

Note

For fixes related to the Forcepoint Security Manager's global settings interface, use only the Forcepoint Management Infrastructure Maintenance Release installer (apply Step 1 only).

For fixes related to Forcepoint DLP, you need both the Forcepoint Management Infrastructure Maintenance Release and Forcepoint DLP Maintenance Release installers (apply Step 1 and Step 2).

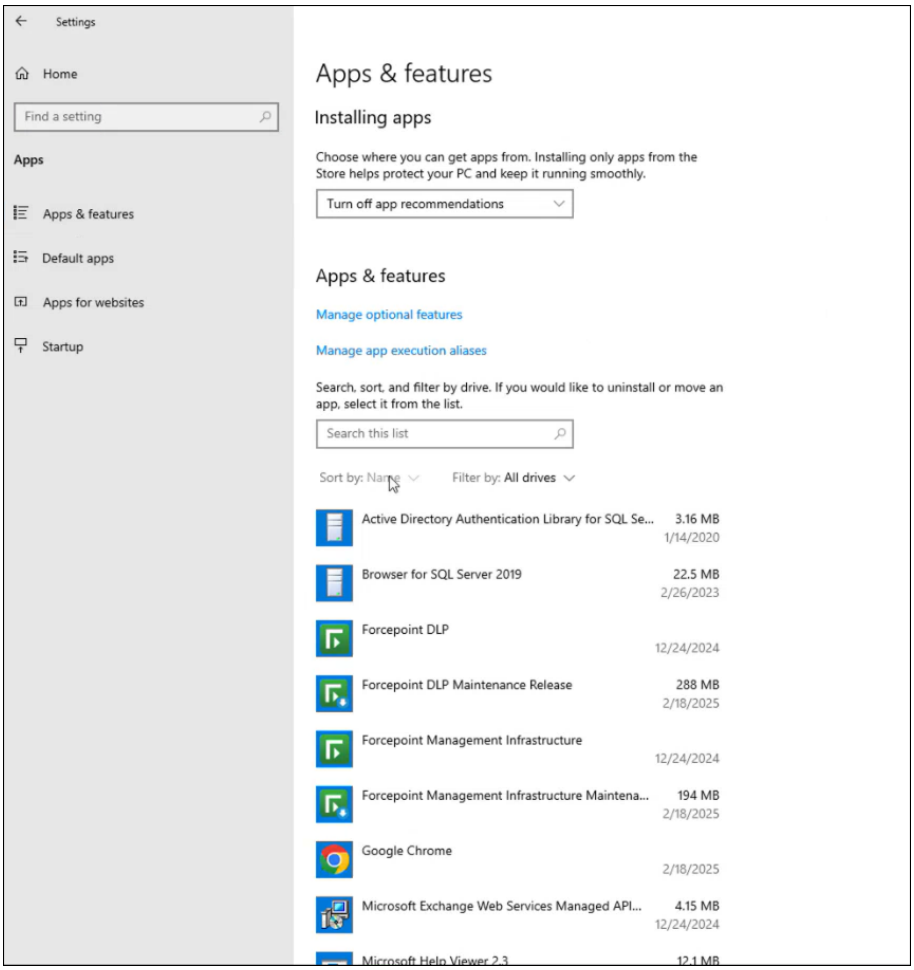
Removing the Maintenance Release

This section outlines the steps to uninstall a maintenance release from your system.

You can uninstall the maintenance release and revert to the base version. For example, if the base version is 10.3.0, and you install 10.3.X, followed by 10.3.Y, removing 10.3.Y will revert the system back to 10.3.0, not 10.3.X.

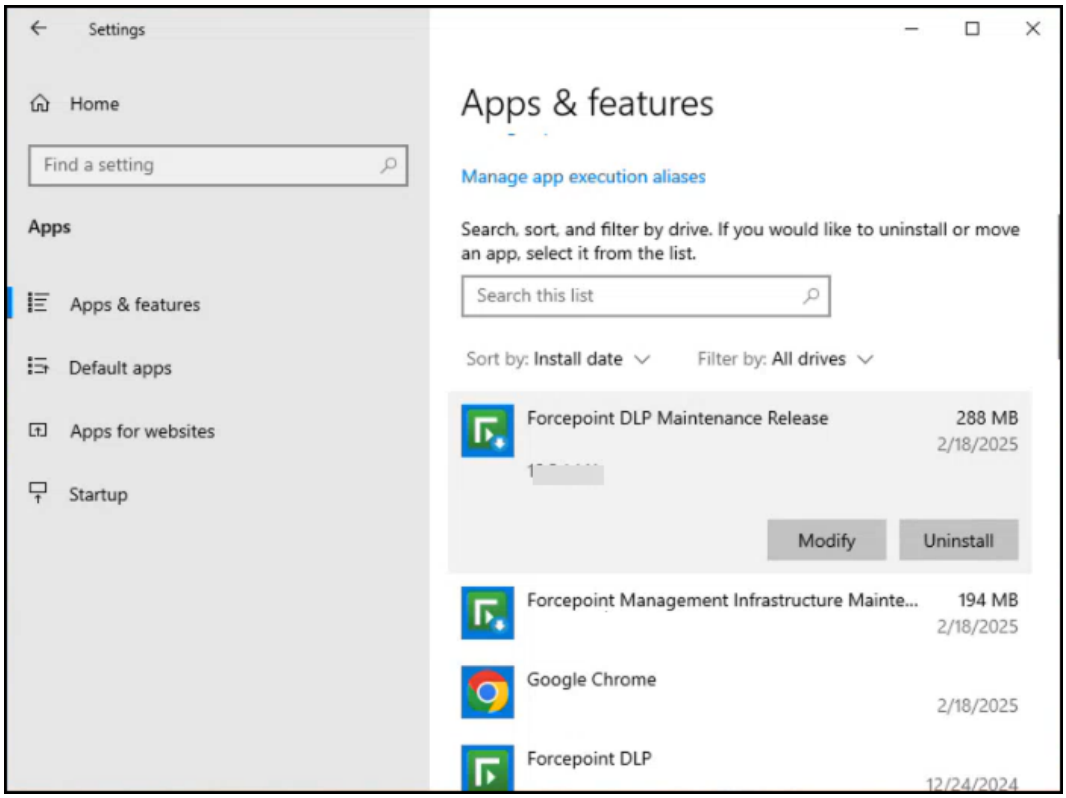
Steps

1) Go to **Settings** > **Apps** > **Apps & features**.



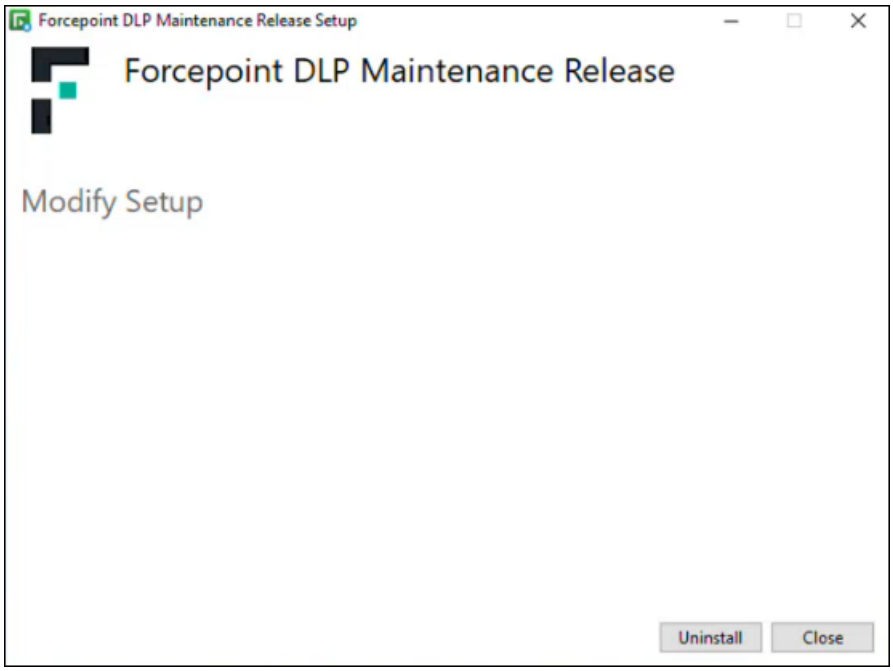
2) To uninstall the Forcepoint DLP Maintenance package, do the following:

a) Select the desired Forcepoint DLP Maintenance Release version.



b) Click **Uninstall**.

The **Forcepoint DLP Maintenance Release Setup** dialog opens.

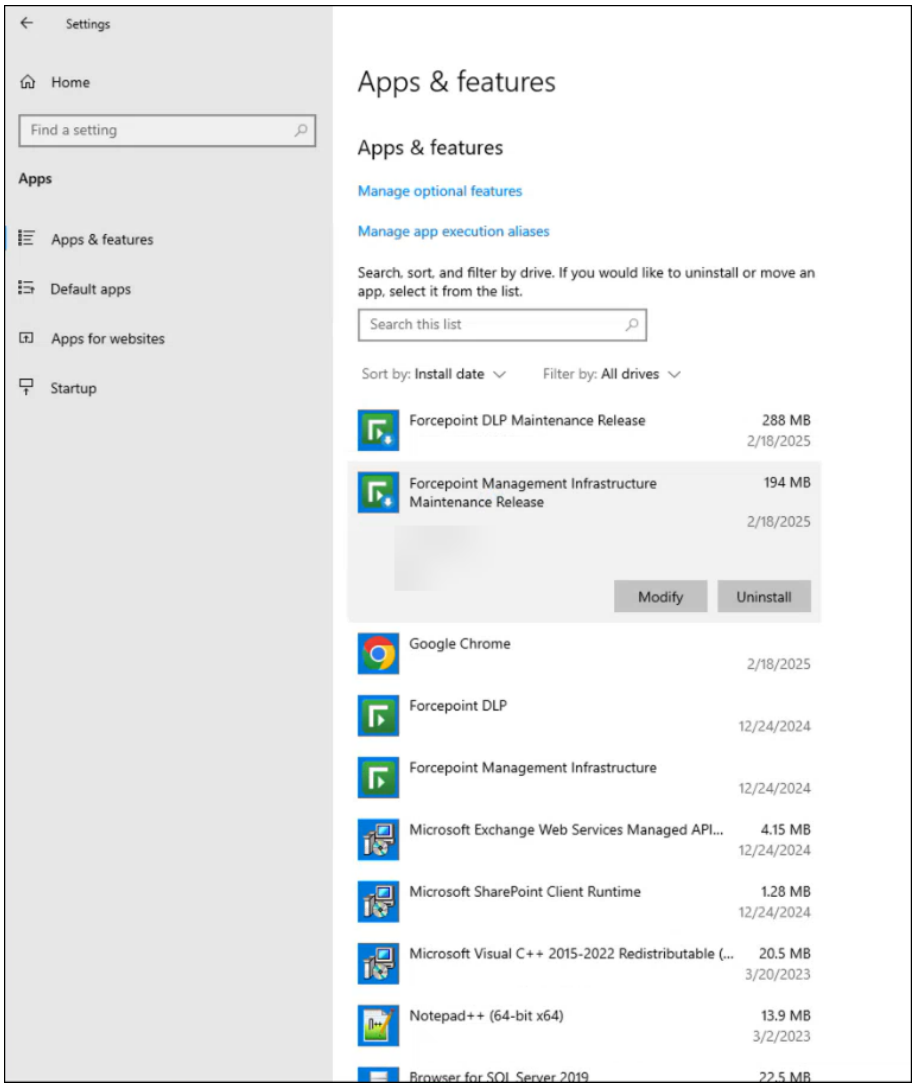


c) Click **Uninstall**.

The **Setup Progress** runs and uninstalls the selected version.

3) To uninstall the Forcepoint Management Infrastructure Maintenance package, do the following:

a) Select the desired Forcepoint Management Infrastructure Maintenance Release version.



b) Click **Uninstall**.
The **Forcepoint Management Infrastructure Maintenance Release Setup** dialog opens.

c) Click **Uninstall**.
The **Setup Progress** runs and uninstalls the selected version.

Note

To remove the Forcepoint Management Infrastructure Maintenance Release installer, apply only Steps 1 and 3.

To remove the Forcepoint DLP Maintenance Release installer, apply all steps (1-3).

Error Handling

Provides solutions for errors that may occur during maintenance installation.

Common errors

Error	Workaround
Issue encountered during the 'Stop and Disable Websense Data Security Manager' service step while installing the DLP maintenance release.	User should rerun the DLP maintenance release.

Maintenance Installation logs

Provides the maintenance installation log file information.

The installer log files are located under the `…\AppData\Local\Temp\` folder.

Log file name for Forcepoint Management Infrastructure:
`Forcepoint_Management_Infrastructure_Maintenance_Release_XXXXXXX.log`

Log file name for Forcepoint DLP: `Forcepoint_DLP_Maintenance_Release_XXXXXXX.log`