



Installation Guide

Forcepoint DLP

v8.8

©2020 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

Published 2020

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Last modified 27-Sep-2020

Contents

Topic 1	Installing the Management Server	1
	Management server system requirements	1
	Preparing for management server installation	2
	Install the management server	4
Topic 2	Installing Supplemental Forcepoint DLP Servers	15
	Supplemental server system requirements	16
	Supplemental server prerequisites	16
	Supplemental server installation steps	17
	Step 1: Download and launch the installer	17
	Step 2: Configure the installation	17
	Step 3: Install and activate the new server software	19
Topic 3	Installing Forcepoint DLP Agents	21
	Integration agent.	22
	The crawler.	24
	Troubleshooting Forcepoint DLP agent installation	27
Topic 4	Installing the Protector	29
	Protector installation prerequisites	29
	Installation steps for ISO/Appliance Protector.	30
	STEP 1: Accept license agreement	31
	STEP 2: Select the hardware to install and confirm hardware requirements	31
	STEP 3: Set administrator and root passwords	31
	STEP 4: Set the NIC for management server and SSH connections	32
	STEP 5: Define the hostname and domain name	33
	STEP 6: Define the domain name server	34
	STEP 7: Set the date, time and time zone	34
	STEP 8: Register with a Forcepoint DLP Server	35
	Final step: Verify the protector installation.	35
	Installing the Forcepoint DLP Protector software package	36
	Pre-installation requirements.	36
	Installing Forcepoint DLP Protector software package	37
	Uninstalling Forcepoint DLP Protector software package	38
	Configuring the protector	38
Topic 5	Installing Web Content Gateway	39
	Preparing the operating system for Content Gateway	39

Topic 6	Adding, Modifying, or Removing Components	51
	Adding or modifying Forcepoint DLP components	51
	Recreating Forcepoint DLP certificates	51
	Repairing Forcepoint DLP components	52
	Changing the Forcepoint DLP service account	53
	Configuring encrypted connection to SQL Server	53
	Removing Forcepoint DLP components	54

1

Installing the Management Server

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, page 7.](#)

The management infrastructure includes the Forcepoint Security Manager and its settings database.

2. [Install Forcepoint DLP management components, page 12.](#)

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).

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, page 15](#), and [Installing Forcepoint DLP Agents, page 21](#), for more information.

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.

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, page 2](#)). Please contact Forcepoint Technical Support for more information on enhancing performance.

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

Disable any antivirus software on the machine prior to installing management server components. Be sure 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*.*
- C:\Documents and Settings\\Local Settings\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

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

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. 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 and click **Downloads** in the toolbar at the top of the page.
2. On the Member Login page, enter your Forcepoint Support account credentials, then click **Login**.
3. If the Data Security section of the downloads page is not displayed, click **All Downloads**.
4. Under Data Security > Forcepoint DLP, click **8.8**.
5. On the list of installers, click **Forcepoint DLP 8.8**.
6. On the Product Installer page, click **Download**.

The Forcepoint Security Installer executable is named **ForcepointDLP88xSetup.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

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 **ForcepointDLP88xSetup.exe** to launch the setup program.
This process may take several minutes. A progress dialog box appears, as files are extracted.



Tip

On 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).

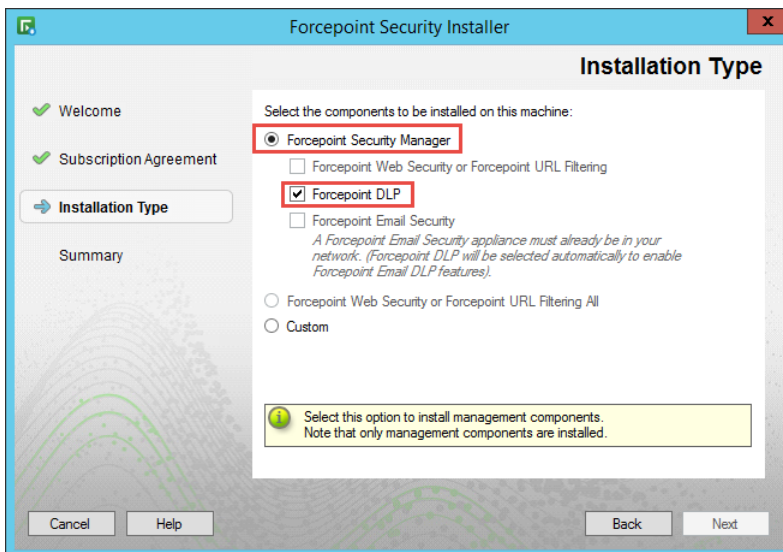
To launch the installer from saved files, click **Forcepoint Security Setup** on the Start screen, or in the Forcepoint folder in the Start menu.

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



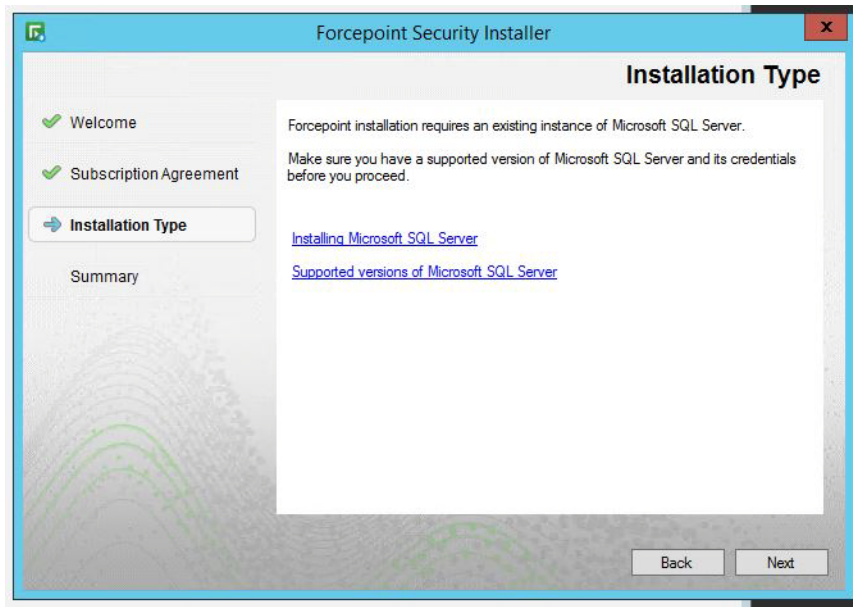
4. On the Subscription Agreement screen, select **I accept this agreement** and then click **Next**.
5. On the first Installation Type screen, select **Forcepoint Security Manager**, then select **Forcepoint DLP**.

The following image shows the Installation Type screen:



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

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

- On the Forcepoint Infrastructure Setup Welcome screen, click **Next**.
- On the Installation Directory screen, accept the default installation path (recommended) or browse to a custom installation path, then click **Next**.

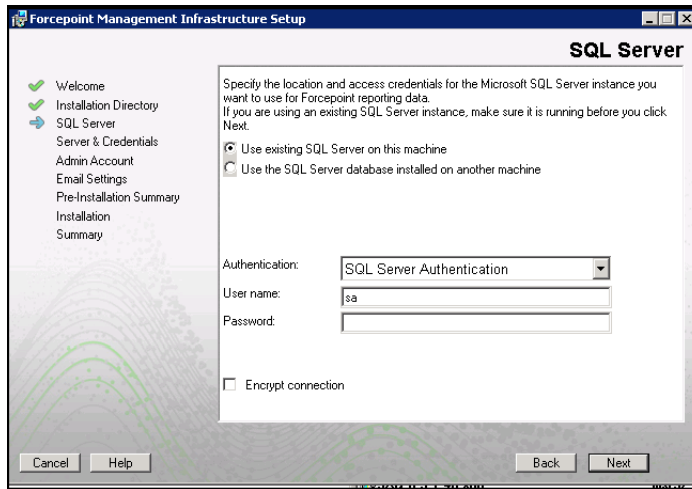


Important

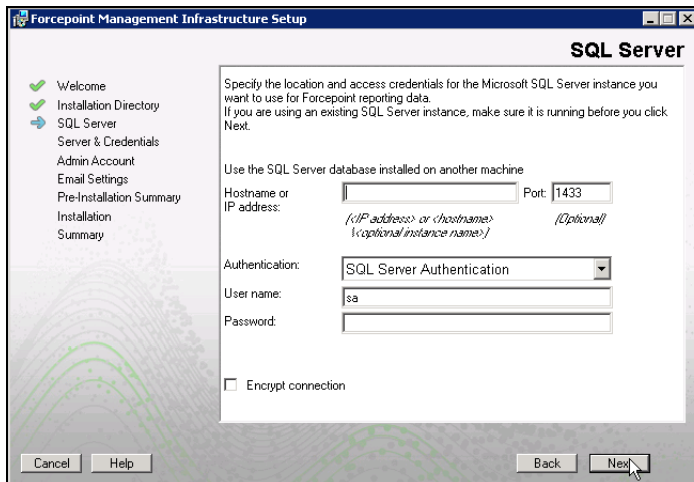
The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

- 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, page 1](#), 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.



Note

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

- 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 screenshot shows the 'Administrator Account' screen in the 'Forcepoint Management Infrastructure Setup' application. The window title is 'Forcepoint Management Infrastructure Setup'. On the left, a navigation pane lists the following steps: Welcome, Installation Directory, SQL Server, Server & Credentials, Admin Account (highlighted with a blue arrow), Email Settings, Pre-Installation Summary, Installation, and Summary. The main content area is titled 'Administrator Account' and contains the following text: 'The default administrator account used to access Forcepoint Security Manager is "admin". This account has access to all administrative functions and cannot be deleted. An email address is required for any administrator account in the Forcepoint Security Manager. It is recommended you enter a password that is at least 8 characters long and contains all of the following: both upper- and lowercase letters, number, and special character.' Below this text are four input fields: 'User name:' with the value 'admin', 'Email address:' with the value 'testing@forcepoint.com', 'Password:' with a masked password of 8 dots, and 'Confirm password:' with a masked password of 8 dots. At the bottom of the window are three buttons: 'Cancel', 'Back', and 'Next'.

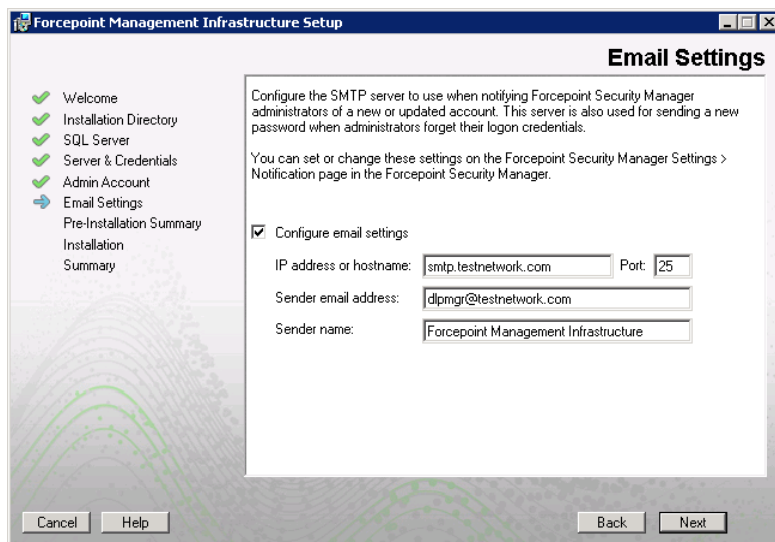
The password must:

- 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**.

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

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.

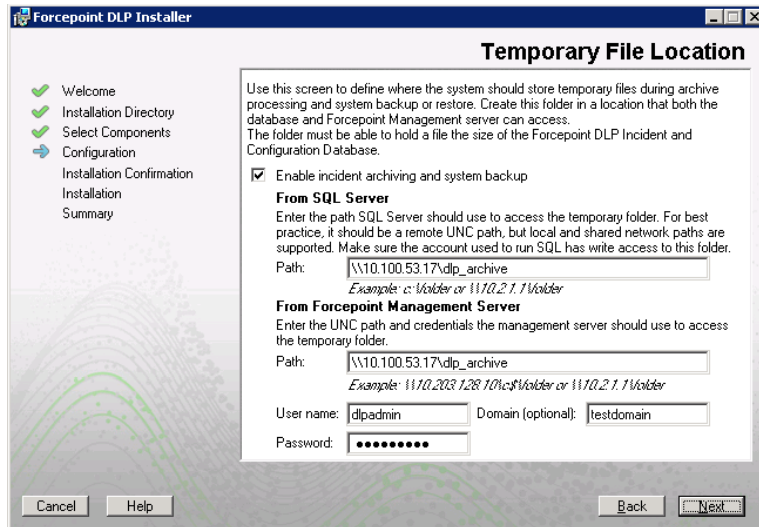
To continue, click **Next**.

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
```

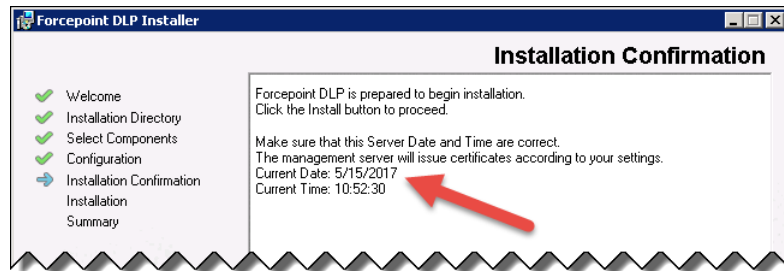
After installation of Forcepoint DLP components, you can revoke this permission:

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

- c. Under From Forcepoint Management Server, enter the UNC **Path** the management 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, see:

- [Installing Supplemental Forcepoint DLP Servers, page 15](#)
- [Installing Forcepoint DLP Agents, page 21](#)
- [Installing the Protector, page 29](#)
- [Installing Web Content Gateway, page 39](#)

To later add, change, or remove components from a Forcepoint DLP machine, see [Adding or modifying Forcepoint DLP components, page 51](#).

2

Installing Supplemental Forcepoint DLP Servers

After Forcepoint DLP has been installed on the management server (as described in [Installing the Management Server, page 1](#)), 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.

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.

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

1. For optimized performance, verify that the operating system is set to use a 4096 byte cluster size.

For more information, refer to the knowledge base article “File System Performance Optimization” at support.forcepoint.com.

2. Set the installation partition to 1 NTFS Partition.
3. 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.
4. Configure the network connection to have a static IP address.
5. Make sure that the server hostname does not include an underscore sign.
6. Enable Short Directory Names and Short File Names (see support.microsoft.com/kb/121007).
7. 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.

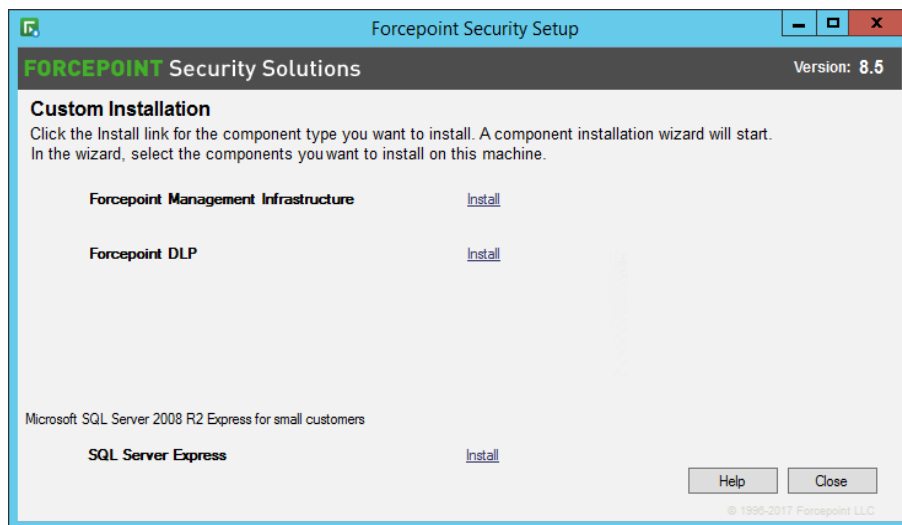
8. Be sure to set the system time accurately on the server.
9. Exclude the following directories from antivirus scanning:
 - The folder where Forcepoint DLP was installed. For supplemental servers, this is Program Files (x86)\Websense\, by default.
 - *:\Inetpub\mailroot*.* - (typically at the OS folder)
 - *:\Inetpub\wwwroot*.* - (typically at the OS folder)
 - C:\Documents and Settings\\Local Settings\Temp*.*
 - %WINDIR%\Temp*.*
 - The forensics repository (configurable; defaults to the product installation directory)

10. 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.

Supplemental server installation steps

Step 1: Download and launch the installer

1. Copy the Forcepoint Security Installer (ForcepointDLP880Setup.exe) from the management server machine to the current server, or download a copy from support.forcepoint.com/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

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*, page 16, 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.

Step 3: Install and activate the new server software

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.

3

Installing Forcepoint DLP Agents

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.



Note

For the Forcepoint DLP integrations with Forcepoint CASB and Forcepoint Web Security Cloud for enforcement of DLP policies on the cloud, no installation steps are required, only connection with Data Protection Service and activation of DLP Cloud Applications, as appropriate according to the licenses you have. The details are sent via email.

For more information, see the [Forcepoint DLP Administrator Guide](#) and the [DLP-CASB Integration Guide](#).

[Test](#)

- 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](#), page 24.)
- **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.

Integration agent

In this topic:

- [Installing the integration agent, page 22](#)
 - [Registering the integration agent, page 23](#)
 - [Using the Forcepoint DLP API, page 23](#)
-

The integration agent allows third-party products to send data to Forcepoint DLP for analysis.

Installing the integration agent

When you embed the integration agent in the product installer, 3 Forcepoint DLP components are installed on the end-user machine:

- **PEInterface.dll** interacts with the Forcepoint DLP policy engine on the management server.
- **ConnectorsAPIClient.exe** connects the API in the third-party product with Forcepoint DLP.
- **registerAgent.bat** (or .vbs) performs registration with the management server.

On Windows, the installation package for the integration agent is provided as an MSI file. The MSI installation wizard presents 4 interactive dialogs:

- **Installation-dir** to select the installation directory
- **Registered Channels** to select the DLP channels to use: HTTP, SMTP, Printer, Discovery
- **Local IP Address** to select which of the static IP addresses currently assigned to the machine should be used for registration

- **management server details** to specify the management server IP address or hostname, user name, and password

Registering the integration agent

Every instance of the integration agent needs to be registered after being installed. In other words, every time the third-party product is installed on an end-user machine, that instance of the agent needs to be registered.

The registration operation can be done during the installation by the installer, or using a command-line utility provided with the agent.

The command-line utility receives the following input arguments:

- **Protocols** - a non-empty list of supported protocols (out of HTTP, SMTP, Printer, Discovery).
- **management server details** - IP address or host name, user name, password.
- **Local IP Address (optional)** - In case this is not supplied, use any of the static addresses of the machine, and print it to the standard output.
- **Search IP Address (optional)** - used for re-registration after IP change. In case this is not supplied, use the address in the “registerAgent.conf” file. If that file does not exist, use the given local IP address.

A successful operation registers the machine with the management server and identifies it as having the appropriate protocols. It also generates certificate files in the same directory that the tool is located. The tool also stored a configuration file (registerAgent.conf) with the IP address used for registration.

On failure, the script returns a meaningful exit code and prints an error message to standard output

Using the Forcepoint DLP API

Third parties that subscribe to the integration agent use a C-based API to send data to Forcepoint DLP for analysis and receive dispositions in return.

The API can be used to configure analysis operations on a transaction-by-transaction basis on the following variables:

- **Channel/Protocol** - Upon installation the third-party product can declare its ability to intercept various protocols, and assign each transaction to a protocol.
- **Blocking/Monitoring mode** - each transaction can work in a different mode.
- **Timeout** - can be different per transaction.

For documentation on the Forcepoint DLP API, consult with a Forcepoint Sales representative.

The crawler

In this topic:

- [Crawler system requirements](#), page 24
 - [Special considerations for IBM Notes and Domino](#), page 24
 - [Installing the crawler agent](#), page 25
-

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**.

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:

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

1. Download the Forcepoint Security Installer (ForcepointDLP880Setup.exe) from the [My Account](#) > Downloads page at 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, you 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.

Troubleshooting Forcepoint DLP agent installation

In this topic:

- [Initial registration fails, page 27](#)
- [Deploy settings fails, page 28](#)
- [Subscription errors, page 28](#)

Though the installation and deployment of agents is normally a series of clear-cut steps, occasionally, some problems can arise. Below are how to resolve common problem scenarios.

Initial registration fails

- Make sure you can ping the Forcepoint DLP agents by IP address and hostname from the management server.
- On Windows, run the following command (in a Command Prompt) to check for block ports:


```
netstat 1 -na | find "SYN"
```

Each line displayed in response to the command is a blocked port. This command is one-way. Run it on both the agent machine and the management server.
- Check logs on the management server and remote policy engines.
 - %dss_home%/logs/mgmt.d.log
 - %dss_home%/tomcat/logs/dlp/dlp-all.log
- Check logs on the protector. These reside in the /opt/websense/neti/log directory. In particular, check the /opt/websense/neti/log/**registration.log** file.
- Make sure no duplicate certificates are installed on the agents’ servers; if there are duplications, delete all of them and re-register the agent. Also, make sure the system date/time of the agent machine and the management server are the same. The following certificates are expected:

Certificate > My User Account > Trusted Root Certification Authorities > Certificates > **ws-ilp-ca**

Certificates > Computer > Personal Certificates ><servername> (issued by ws-ilp-ca)

Certificates > Computer > Trusted Root Certification Authorities > Certificates > **ws-ilp-ca**

- Make sure the FQDN value of the agent states the full server name for the agent's server.
 - For the protector, if a domain name is configured, the FQDN is:
`protectorname.domain.name`
 - For agents and Forcepoint DLP server, copy the computer name value from "My Computer" > Properties.

Deploy settings fails

- Make sure you can ping the agents by IP address and by hostname from the management server.
- Check logs on the management server and remote policy engines.
 - `%dss_home%/tomcat/logs/dlp/dlp-all.log`
 - `%dss_home%/tomcat/logs/dlp/deployment-trace.log`
- Check the **plat.log** file on the protector.

Subscription errors

- Restart the "Websense Data Security Manager" service on the management server.
- Check `%dss_home%/tomcat/logs/dlp/dlp-all.log`.

4

Installing the Protector

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:

1. Make sure all prerequisites are met. See [Protector installation prerequisites](#), page 29.
2. Perform the installation. See [Before you begin.](#), page 30.
3. Configure the protector in the Data Security module of the Security Manager. See [Final step: Verify the protector installation](#), page 35.

Protector installation prerequisites

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.

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. The protector software is provided on an ISO image. Download the image, **DataProtector88.iso**, from support.forcepoint.com/Downloads and burn it to a CD or bootable USB. (Accessing the Downloads page requires a Forcepoint Support login.)
 3. Place the media in the protector's CD drive or USB port and restart the machine.
 4. An installer page appears. Press **Enter** and the machine is automatically restarted a second time.

For installation, see *Installation steps for ISO/Appliance Protector*, page 30.

- If the protector is deployed in public cloud and is provided as a self-extractor package that can be installed on any CentOS 7.x and RedHat 7.x based system and provides the protector application part (ICAP server and MTA), see *Installing the Forcepoint DLP Protector software package*, page 36.

Installation steps for ISO/Appliance Protector

To begin the installation process:

1. When prompted for a user name and password, enter **admin** for both.

When the protector CLI opens for the first time, logging in as admin automatically opens the installation wizard. On subsequent attempts, type "wizard" at the command prompt to access the wizard.
2. Follow the instructions given by the wizard to configure basic settings.

In some cases, the wizard provides a default setting (shown within brackets []). To accept the default setting, press **Enter**.

STEP 1: Accept license agreement

Each time the installation wizard opens, the end-user license agreement appears. Use the page-down, scroll, or space keys to read to the end of the agreement. Carefully read the license agreement, and when prompted, type **yes** to accept it.

STEP 2: Select the hardware to install and confirm hardware requirements

The system checks to see if your hardware meets the following requirements:

- 2 GB RAM
- 4 CPU
- CPU with more than 2MB of cache
- CPU speed of 8000 bogomips
- Partition “/opt/websense/data” should have at least 45 GB
- 2 NICs

If the machine does not meet the requirements, the wizard asks whether or not to continue.

```
Step 2/8: Hardware requirements
WARNING: Total amount of physical memory is not enough
Minimum required: 2000 MB, found: 1010 MB.
WARNING: Not enough CPU/cores.
Minimum required: 4 processors, found: 1
WARNING: CPU speed is too low.
Minimum required: 8000 BogoMIPS, found: 4000 BogoMIPS
Hardware requirements are not satisfactory. Do you want to continue? [yes/No]: _
```

STEP 3: Set administrator and root passwords

1. Type in and confirm a new password for the “admin” account. For security reasons, it is best practice to change the default password.

```
Step 3/8: Administrator Password
Choose a new password or passphrase for the "admin" user.
A valid password should be at least 8 characters in length.
It should contain at least 4 of the following classes:
One digit
One capital letter
One lowercase letter
One symbol
Enter a new "admin" password:
Re-enter the password: _
```

2. Type in and confirm a new Root Password (mandatory). The root account provides full access to the device and should be used carefully.

STEP 4: Set the NIC for management server and SSH connections

A list of available network interfaces (NICs) appears. In this step, choose the NIC for use by the management server, SSH connections, and logging onto the protector (eth0 by default). All other NICs will be used for intercepting traffic.

To help identify which NIC to use, the wizard can simulate traffic for 0-60 seconds and cause LEDs to blink on the selected interface. This does not work for all hardware and drivers.

1. When prompted, choose the NIC index number of the management NIC, or accept the default interface.
2. Enter a number 0-60 to indicate how long (in seconds) to simulate traffic, or press **Enter** to skip this step.

```
Step 4/8: NIC for Management Server and SSH Connections

The protector has a set of NICs for intercepting traffic and one NIC for
use by the management server and SSH connections.
This NIC is also used to log onto the protector.

*NOTE* During an upgrade the network port used for management might be
        assigned differently than previous Protector versions. Please make
        sure that your Management Interface is connected properly.

Available network interfaces:
(* - current Management Interface, BR - bridge member interface)
(0) * eth0 (driver: pnet32  mac: 00:0C:29:59:56:2B  inet: 192.168.1.1/24)
(1)  eth1 (driver: pnet32  mac: 00:0C:29:59:56:35  inet: 0.0.0.0/0)
(2)  eth2 (driver: pnet32  mac: 00:0C:29:59:56:3F  inet: 0.0.0.0/0)

Please choose a management interface number (0-2)[0]: _
```

3. Enter the IP address of the NIC to use. The default is 192.168.1.1.
4. Enter the IP prefix of this NIC. This is the subnet mask in abbreviated format (number of bits in the subnet mask). The default is 24 (255.255.255.0).
5. Enter a broadcast address for the NIC. The installation wizard will provide a calculated value, which is normally correct.

- Enter the IP address of the default gateway to be used to access the network. If the IP address of the Forcepoint DLP server is not on the same subnet as the protector, a default gateway is required to tell the protector how to communicate with the Forcepoint DLP server.

```

Vendor:      Advanced Micro Devices [AMD]
Model:      79c978 [PCnet32 LANCE]

This wizard can assist you in identifying the Management Interface by initiating
simulated traffic for a number of seconds, causing some LEDs to blink on that p
ort. (Note that this feature depends on the hardware/driver and may not work.)

How many seconds would you like the traffic simulated?
(0-60, press [Enter] to skip this step)

The eth0 network interface has now been configured as the management interface.
You are asked below to confirm the configuration setting. Answering "Yes" confir
ms the configuration, "No" will delete the settings and restart this step of the
wizard.
Do you want to continue? [Yes/no]: yes
Enter the Management Interface IP address [192.168.1.1]: 10.0.34.101

Prefix denotes the network mask, i.e 255.255.255.0 is the same as prefix 24.
Enter the Management Interface IP prefix [24]:

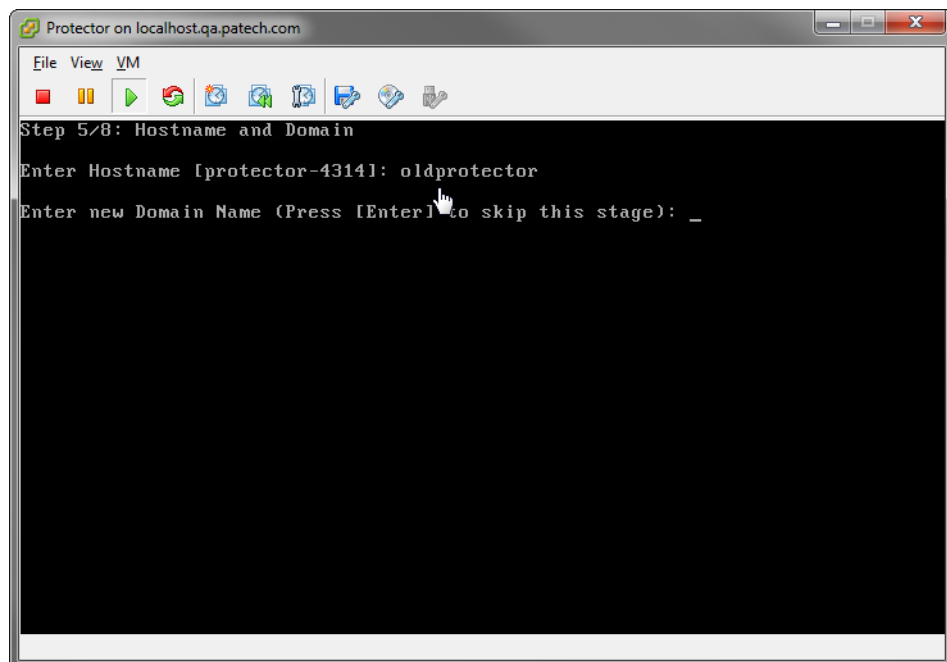
Enter a broadcast address [10.0.34.255]:

Enter a new default gateway IP address
(Type 'Delete' to remove the default gateway) [192.168.1.254]: _

```

STEP 5: Define the hostname and domain name

- Enter a unique hostname for the protector appliance.



```

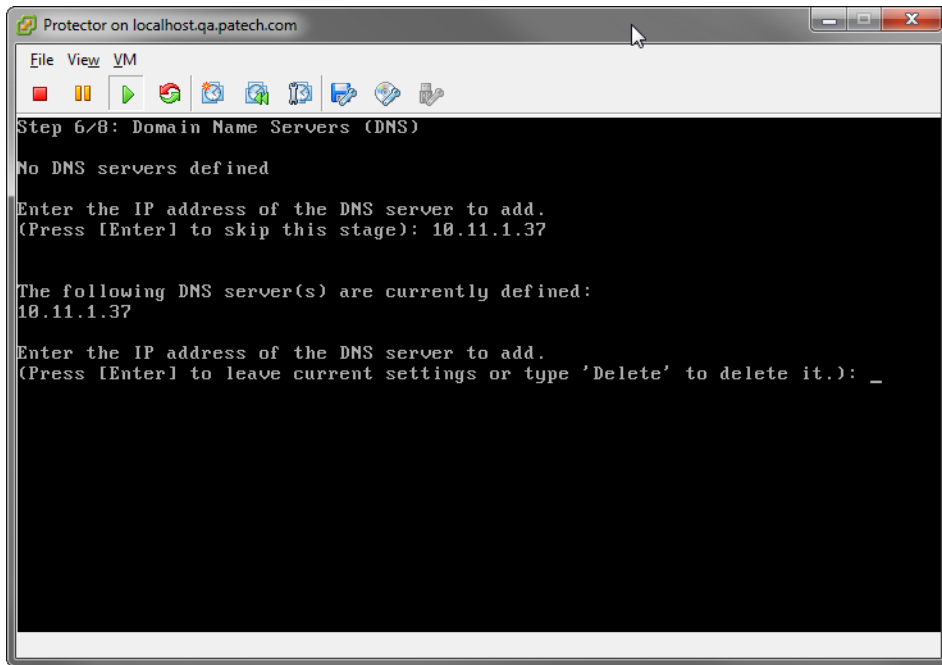
Protector on localhost.qa.patech.com
File View VM
Step 5/8: Hostname and Domain
Enter Hostname [protector-4314]: oldprotector
Enter new Domain Name (Press [Enter] to skip this stage): _

```

- Optionally, enter the domain name of the network into which the protector was added. The domain name set here will be used by the Forcepoint DLP server when defining the protector's parameters.

STEP 6: Define the domain name server

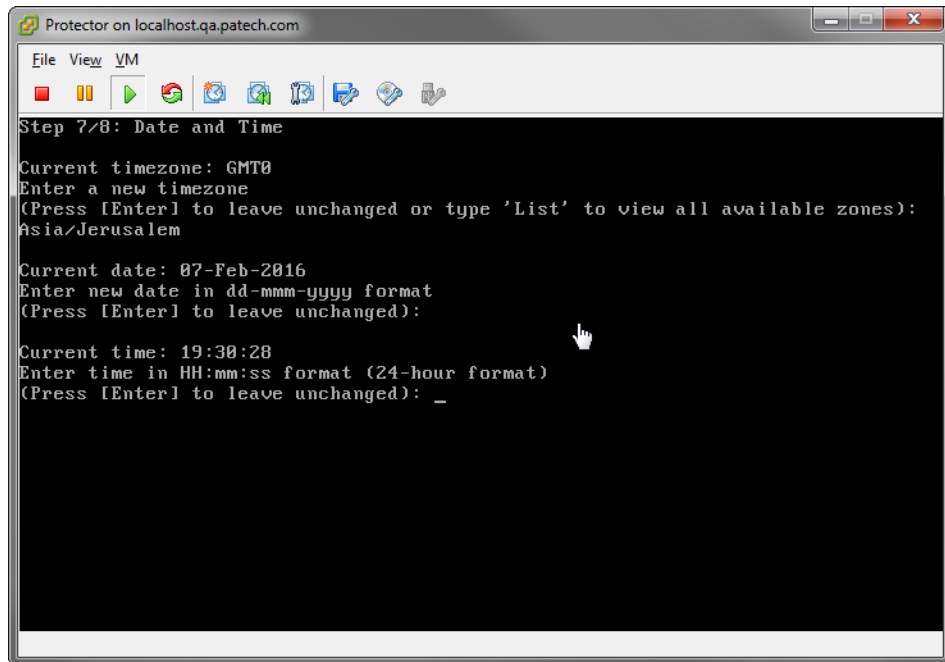
Optionally, enter the IP address of the domain name server (DNS) for this protector. DNS allows access to other network resources using their names instead of their IP addresses.



STEP 7: Set the date, time and time zone

1. Enter the current time zone.
To view a list of all timezones, enter **list**.
2. Enter the current date in the following format: dd-mmm-yyyy.

3. Enter the current time in 24-hour, HH:MM:SS format.



STEP 8: 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.

1. Enter the IP address or FQDN of the Forcepoint DLP Server. Note that this must be the IP address identified when you installed the server machine. It cannot be a secondary IP address.
2. Enter the user name and password for a Forcepoint DLP administrator that has privileges to manage system modules.

Final step: 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. Refresh the browser.

Click **Deploy**.

In the protector command-line interface, the following appears:

```

Done
Generating initial network configuration ...Done

The configuration wizard has completed successfully.

Starting the Protector service...

Starting SMTP Blocking Service...           [ OK ]
Starting PAM Watchdog...                     [ OK ]

Ebttables v2.0 registered
arp_tables: (C) 2002 David S. Miller
type=1700 audit(1411381293.337:2): dev=eth1 prom=256 old_prom=0 auid=4294967295
ses=4294967295
type=1700 audit(1411381293.461:3): dev=bond0 prom=256 old_prom=0 auid=4294967295
ses=4294967295
CM-Protector-Lilach> type=1700 audit(1411381369.169:4): dev=eth1 prom=0 old_prom
=256 auid=4294967295 ses=4294967295
type=1700 audit(1411381369.354:5): dev=eth1 prom=256 old_prom=0 auid=4294967295
ses=4294967295
-

```

The protector is now ready to be configured.

Installing the Forcepoint DLP Protector software package

Pre-installation requirements

- Forcepoint DLP Protector software package is supported on CentOS 7.5 or RHEL 7.5.
- 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, continue the installation.

If the outputs do not match, the FQDN (long) should be changed to match the short hostname.

To change the FQDN:

- Open the hosts file located in `/etc/hosts` as root.
- 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 firewalld or NetworkManager are running and disable them if they are running.

Installing Forcepoint DLP Protector software package

When the protector is deployed in public cloud and is provided as a self-extractor package that can be installed on any CentOS 7.5 or RedHat 7.5 based system, use the following steps to install it:

1. Download Forcepoint DLP Protector software package, from My Account > Downloads page at support.forcepoint.com.

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 a Command Prompt, run the following command:

```
sudo ./<installation file> <version>-<build>
```

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 that 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. Refresh the browser.

Click **Deploy**.

Uninstalling Forcepoint DLP Protector software package

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
```

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](#).

5

Installing Web Content Gateway

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.

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 [IPTables 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:

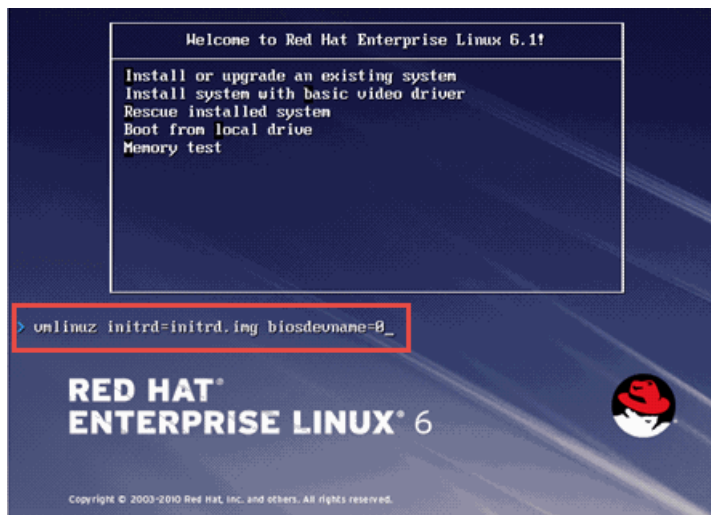
1. During operating system installation.
2. Post-operating system installation through modification of several system files and other activities.

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.

```

root@localhost:~# ifconfig -a
eth0:   Link encap:Ethernet  HWaddr 78:AC:00:09:69:9A
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
        Interrupt:17

lo:     Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1%lo  Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:22 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:98 (98.0 b)  TX bytes:98 (98.0 b)

p4p1:   Link encap:Ethernet  HWaddr 00:1B:21:5F:92:18
        inet addr:10.203.67.130  Bcast:255.255.0.0  Mask:255.255.0.0
        inet6 addr: fe80::21b:21ff:fe5f:9218:64  Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:1248 errors:0 dropped:0 overruns:0 frame:0
        TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:113910 (111.3 kb)  TX bytes:24216 (23.6 kb)
        Memory:f2800000-f2820000

p4p0:   Link encap:Ethernet  HWaddr 00:1B:21:5F:90:19
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
        Memory:fc820000-fc840000

root@localhost:~#

```

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 RHEL 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:

```
./wgc_install.sh
```

## Install Content Gateway

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

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

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](#).



# 6

## Adding, Modifying, or Removing Components

The topics in this chapter provide instructions for:

- [Adding or modifying Forcepoint DLP components, page 51](#)
- [Recreating Forcepoint DLP certificates, page 51](#)
- [Repairing Forcepoint DLP components, page 52](#)
- [Changing the Forcepoint DLP service account, page 53](#)
- [Configuring encrypted connection to SQL Server, page 53](#)
- [Removing Forcepoint DLP components, page 54](#)

### 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 ForcepointDLP880Setup.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:

- [Recreating Forcepoint DLP certificates, page 51](#)
- [Repairing Forcepoint DLP components, page 52](#)
- [Changing the Forcepoint DLP service account, page 53](#)

### 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:

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 (**ForcepointDLP880Setup.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.

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:

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.