FORCEPOINT

POWERED BY Raytheon

Installation Guide

Forcepoint DLP

v8.4.x

Contents

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 all Forcepoint on-premises security solutions) and core Forcepoint DLP components.

- Installation must be complete on the management server before other Forcepoint DLP components (secondary servers, protectors, and agents, 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 Management 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 (VM). (Note that the incident and reporting database is hosted on Microsoft SQL Server, which does not typically run in a virtualized environment.)

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 17, and *Installing Forcepoint DLP Agents*, page 23, for more information.

Management server system requirements

Find system requirements for the Forcepoint management server in the *Deployment & Installation Center*.

- 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 v4.5 are installed on the management server. If the correct versions are not detected, the setup program returns an error.

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 3). 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\<user>\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.

Third-party components

The following third-party components are required to install Microsoft SQL Server 2008 R2 Express. Although the Forcepoint Security Installer installs these components automatically if they are not found, it is a best practice to install the components before running the setup wizard if you plan to use SQL Server Express.

- .NET Framework 3.5 SP1

    Because the installer requires .NET 4.5 as well, both .NET 4.5 and 3.5 SP1 are required if you are installing SQL Server Express.

- Windows Installer 4.5

- Windows PowerShell 1.0 (available from www.microsoft.com)

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.

> **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 **8.4.x**.

5. On the list of installers for Forcepoint DLP version 8.4.x, click the **Forcepoint DLP 8.4** entry.

6. On the Product Installer page, click **Download**.

   The Forcepoint Security Installer executable is named **Forcepoint84xSetup.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 both **domain** and **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 **Forcepoint84xSetup.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**.
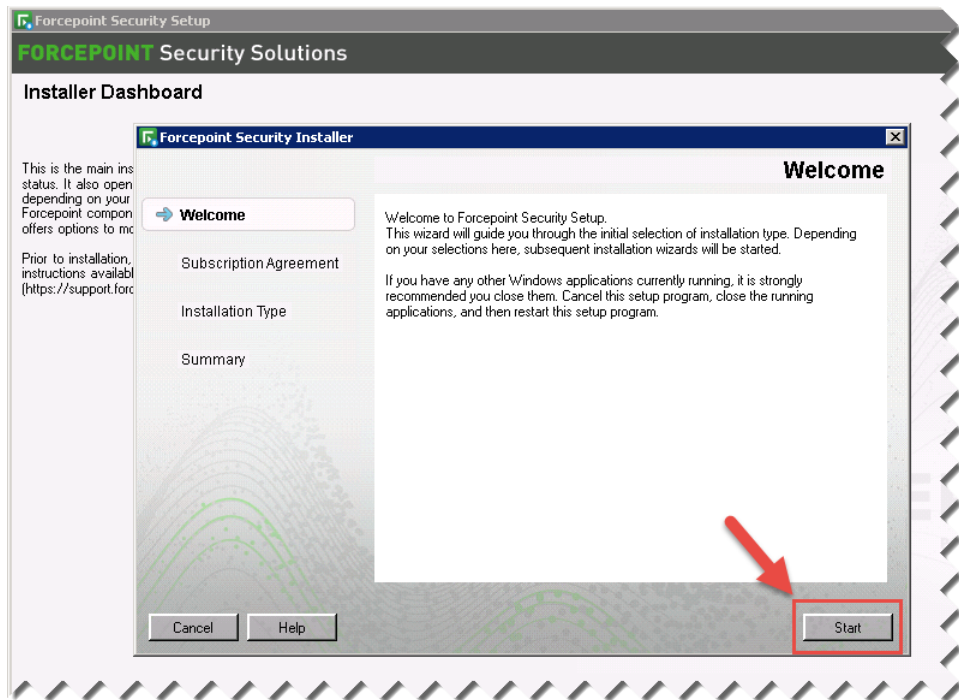
4. On the Subscription Agreement screen, select **I accept this agreement** and then click **Next**.

5. On the Installation Type screen, select **Forcepoint Security Manager**, then select **Forcepoint DLP**.
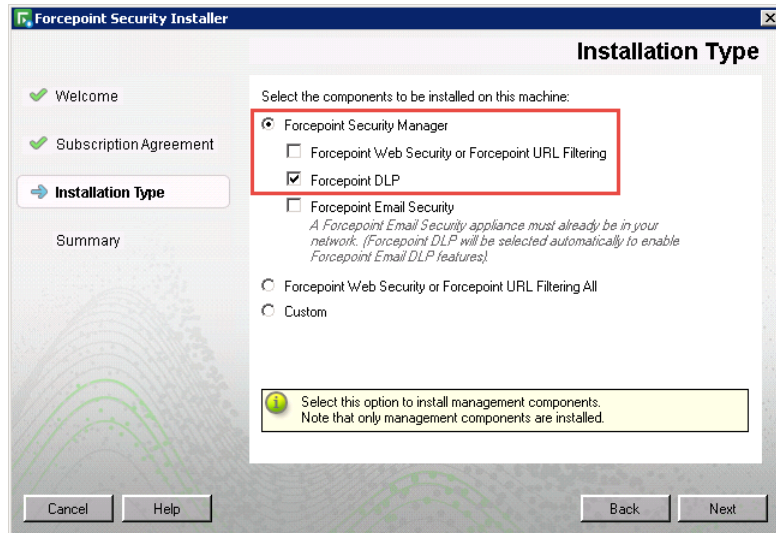
> ⚠️ **Warning**
>
> The Email Gateway for Microsoft Office 365 is not supported in version 8.4. On the next screen, do **not** select the option to install management components for the Forcepoint Email Azure appliance.

6. On the second Installation Type screen, click **Next**.

   DO NOT select the "Install the Forcepoint Email Azure appliance on-premises management component" option.

7. In the **Summary** screen, click **Next** to continue the installation. The Forcepoint Management Infrastructure Setup wizard launches.

Install the Forcepoint Management Infrastructure

1. On the Forcepoint Management 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.
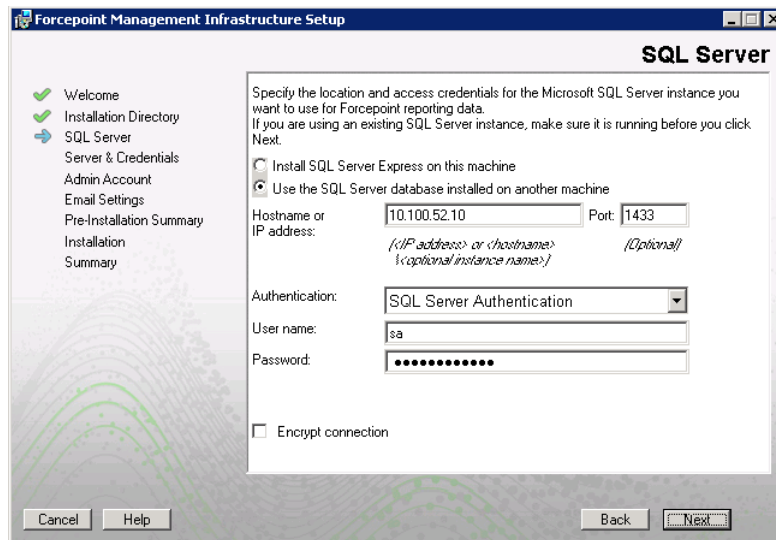
- Select **Use existing SQL Server on this machine** if the Forcepoint Security Installer has already been used to install SQL Server 2008 R2 Express on this machine.

- Select **Install SQL Server Express on this machine** to install SQL Server 2008 R2 Express on this machine.

  A default database instance named **mssqlserver** is created, by default. If a database instance with the default name already exists on this machine, an instance named TRITONSQL2K8R2X is created instead.

  If a reboot is required after installing SQL Server Express, use the Forcepoint Security Setup shortcut to relaunch the installer. The shortcut is found on the Windows Start screen, or in the Forcepoint folder of the Start menu:

- (*Recommended*) 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 2, 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 <u>Administering Forcepoint Databases</u>.

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 Management 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.
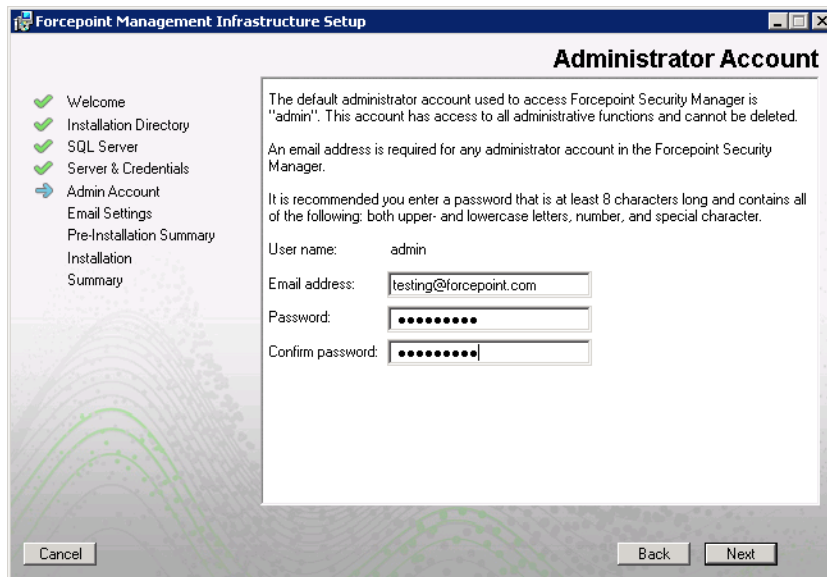
The password must:

■   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.
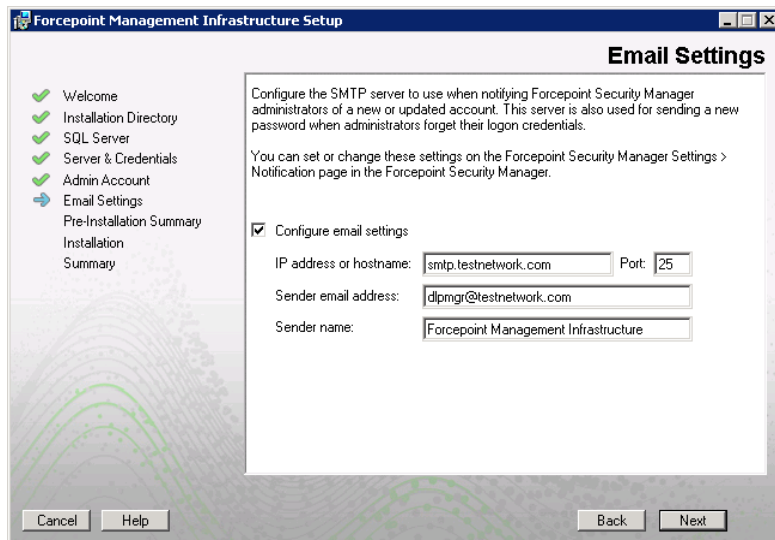
> **Important**
>
> SMTP server configuration must be completed before password recovery email messages can be sent.

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.

> **Warning**
>
> If SQL Server Express is selected for installation, the machine may be automatically restarted up to two times during the installation process. Restarts are not required if all prerequisites were previously installed.

> **Note**
>
> If SQL Server Express is selected for installation, it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

9. If you chose to install SQL Server Express, PowerShell 1.0 and Windows Installer 4.5 will be installed if not already present. Wait for Windows to configure components.

    a. If the following message appears during this process, click **OK**:

        Setup could not restart the machine. Possible causes are insufficient privileges, or an application rejected the restart. Please restart the machine manually and setup will restart.

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

    c. 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.

10. If SQL Server Express is selected for installation, SQL Server 2008 R2 Setup is launched. Wait for it to complete.

    The Setup Support Files screen appears and then an Installation Progress screen appears. Wait for these screens to complete automatically. It is not necessary to click or select anything in these screens.

    Note that it may take approximately 10-15 minutes for the SQL Server 2008 R2 Express installation to complete.

11. 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.

12. On the Installation Complete screen, click **Finish**.

The Installer Dashboard is displayed. 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.
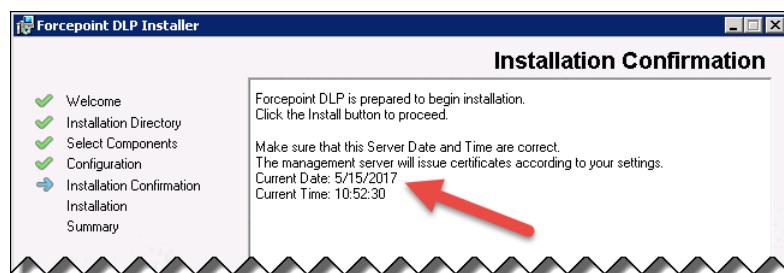
7. The Installation Progress screen is displayed.

    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, mobile agent, or endpoint client, see:

- *Installing Supplemental Forcepoint DLP Servers*, page 17
- *Installing Forcepoint DLP Agents*, page 23
- *Installing the Protector*, page 41
- *Installing Web Content Gateway*, page 49
- *Installing the Cloud Agent*, page 61

To later add, change, or remove components from a Forcepoint DLP machine, see *Adding, Modifying, or Removing Components*, page 83.

2 | Installing Supplemental Forcepoint DLP Servers

In this topic:

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

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

Supplemental server system requirements

Find system requirements for supplemental Forcepoint DLP servers in the *Deployment & Installation Center*.

● 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\<user>\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 (Forcepoint84xSetup.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.
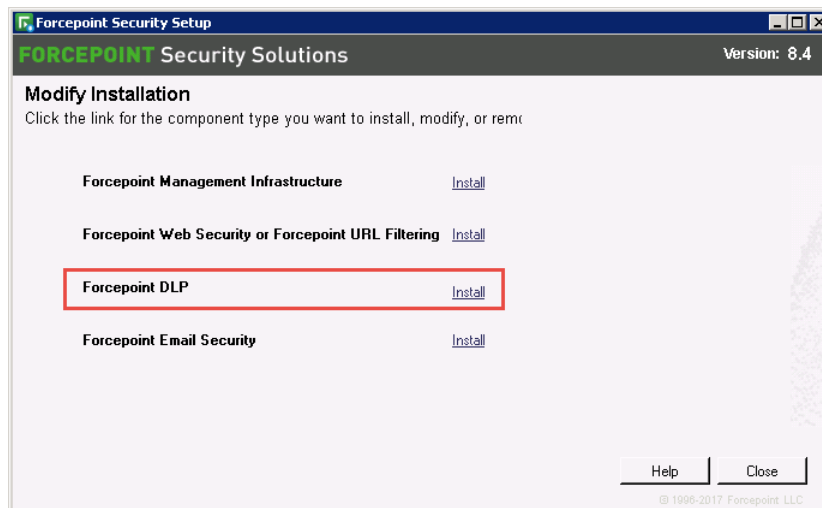
6. On the Welcome screen, click **Next** to begin the installation.

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 18, 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. For example, the mobile agent monitors email being synchronized to mobile devices.

> **! 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.

- The on-premises **analytics engine** is used to calculate the relative risk of user activity, correlate it with similar activity, and assign it a risk score. (See *Installing the analytics engine*, page 24.)

- The **cloud agent** included with Forcepoint DLP Cloud Applications provides cloud activity content inspection for files uploaded into and stored within enterprise cloud collaboration services, such as Microsoft Office 365. (See *Installing the Cloud Agent*, page 61.)

- The on-premises **mobile agent** monitors and blocks data downloaded to mobile devices that perform synchronization operations with the Exchange server. The mobile agent can monitor and block data transmitted in email messages, calendar events, and tasks. The mobile agent supports ActiveSync (wireless communication protocol used to push resources, such as email, from applications to mobile devices). (See *Installing the mobile agent*, page 26.)

- 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 35.)

- **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.

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 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 analytics engine on a 64-bit Linux machine as described in this section.

Analytics engine system requirements

Find system requirements for the analytics in the *Deployment & Installation Center*.

- 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

Before starting the installation, make sure the following Linux packages are installed on the machine that will host the analytics engine:

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

If the system is connected to a yum repository, use the following command to install the packages:

```
yum install apr apr-util perl-Switch unixODBC freetds
```

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

1. To download the analytics engine installer (AnalyticsEngine84):

   a. Go to support.forcepoint.com and click the **My Account** link to log in.

   b. Click the **Downloads** link in the toolbar at the top of the page.

   c. Select the product **Forcepoint DLP** and the version **8.4** to locate the installer file.

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:

   ```
   ./AnalyticsEngine84
   ```

   ■ If a "permission denied" error appears, run the following command:

   ```
   chmod +x AnalyticsEngine84
   ```

   ■ 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 **./AnalyticsEngine84** command again.

Single-command analytics engine installation

To simplify installation, run the following command on the Linux server. The command downloads the analytics engine installers, installs all the necessary packages, configures the necessary server configurations, and kicks off the Analytics Setup Wizard.

```
cd /tmp; yum -y install open-vm-tools; yum -y install epel-
release; yum -y install apr apr-util perl-Switch unixODBC
freetds; yum -y install wget; wget http://cdn.websense.com/
downloads/files/v8.4/AnalyticsEngine84; yum -y install
ntpdate; ntpdate time.nist.gov; chmod +x AnalyticsEngine84;
./AnalyticsEngine84
```

In the command above, the temporary directory (cd /tmp) and ntp server (ntpdate time.nist.gov) can optionally be customized.

Forcepoint Security Manager connection for analytics engine

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.

   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 mobile agent

In this topic:

- *Mobile agent system requirements*, page 26
- *Mobile agent installation steps*, page 26

The mobile agent is a CentOS 7-based appliance used to secure the type of email content that is synchronized to users' mobile devices when they connect to the network. This includes content in email messages, calendar events, and tasks.

Mobile agent system requirements

Find system requirements for the analytics in the *Deployment & Installation Center*.

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

Mobile agent installation steps

The mobile agent may be installed on a Forcepoint appliance, s meet these requirements, or you can host the agent on your own CentOS 7-based hardware.

> **Note**
> For best performance, make sure that the mobile agent is located in close proximity to the back-end server.

You access the installation wizard for your mobile agent through a putty Command Line Interface (CLI).

To install the mobile agent:

1. If the mobile agent will run on a Forcepoint DLP appliance, follow the instructions on its quick start poster to rack, cable, and power on the appliance.

   If the mobile agent will run on other hardware:

   a. Use either a direct terminal or connect via serial port to access the command line. For serial port connection, configure the terminal application as follows:
      - 19200 baud
      - 8 data bits
      - no parity
      - 1 stop bit
      - no flow control

   b. The mobile agent software is provided on an ISO image. Download the image, **ProtectorMobile84x.iso**, from the [My Account](#) > Downloads page at support.forcepoint.com, and burn it to a CD or bootable USB.

   c. Place the media in the machine's CD drive or USB port and restart the machine.

   d. An installer page appears. Press **Enter**. The machine is automatically restarted a second time.

2. When prompted, enter a user name and password. Enter **root** for user name and **admin** for password.

3. To access the wizard, type **wizard** at the command prompt, then press **Enter**.

4. When prompted to install either the protector or mobile agent, enter **M** for mobile agent.

5. Follow the instructions in the wizard to configure basic settings.

   When the wizard requires data entry, it presents a prompt. In some cases, a default setting is provided:

   ■ A capital letter indicates the default value, such as Yes/no.

   ■ Square brackets ([ ]) show the current value. They are usually followed by text, such as: Press [Enter] to leave as is.

   If the default setting is acceptable, press **Enter** to keep the default value.

STEP 1: Accept license agreement

Each time the installation wizard opens, the end-user license agreement appears. Use the page-down/ scroll / space keys to read/scroll to the end of the agreement.

Carefully read the license agreement and when prompted, type yes to accept the license agreement.

STEP 2: Set administrator password

Enter and confirm a new password for the "admin" account. For security reasons, it is best practice to change the default password.

> **Important**
>
> A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:
>
> - One digit
> - One symbol
> - One capital letter
> - One lowercase letter
>
> If you begin the password with a capital letter or end it with a digit, these characters do not count as one of these classes.

The Operating System (OS) prompts you to change (refresh) your password every 90 days.

STEP 3: Set root password

Enter and confirm a new password for the root user. The root account provides full access to the device and should be used carefully.

> **Important**
>
> A valid password should be at least 7 characters in length. It should contain at least 2 of the following classes:
>
> - One digit
> - One symbol
> - One capital letter
> - One lowercase letter
>
> If you begin the password with a capital letter or end it with a digit, these characters do not count as one of these classes.

STEP 4: Network configuration

1. Select the network interface (NIC) from the list of available NICs (eth0 by default), or for advanced configuration, type c.

```
Step 4/8: Network Configuration


Configured network interfaces and their current configuration:
(0)  eth0 : 192.168.1.1/24

Please select the management IP/interface from the list above (0 0)
or type (c) to configure networking: _
```

2. To configure a network interface, choose the NIC index number from the list of displayed by the wizard.

```
Step 4/8: Network Configuration
------------- Network interfaces configuration ----------------------
Available network interfaces:
(0)        eth0 :         192.168.1.1/255.255.255.0
(1)        eth1 :         Not configured
(2)        eth2 :         Not configured

(0-2)  - Enter the index of the entry above to modify it or delete it
[Enter] - Finish setting up the network interfaces and continue to the routing
setup:
0_
```

3. Enter **e** to configure the NIC, then:

```
-------------------------------------
Configuring Network interface eth0...
Device:  Advanced Micro Devices [AMD], 79c970 [PCnet32 LANCE]

  eth0 :         192.168.1.1/255.255.255.0

(e)      - Edit or delete current eth0 setup
(a)      - Change current eth0 aliases setup
(b)      - Blink eth0 associated LED for easy identification
[Enter] - Exit eth0 configuration

_
```

a. Enter an the IP address.

b. Type the netmask (network prefix). This is the subnet mask in abbreviated format (number of bits in the subnet mask). The default is 255.255.255.0 for eth0.

```
c
Configuring eth0:
Please enter the eth0 IP address or type (d) to delete
current configuration [10.212.16.10]:
Please enter the NETMASK [255.255.0.0]: _
```

c. If prompted, enter the IP address for the default gateway to be used to access the network. This prompt appears only for the first NIC to be configured.

d. After configuring the NIC, the wizard offers the option to redefine it (change the IP address, network prefix, or gateway) or remove it (type e, then d), if necessary.

To return to the previous menu and define other NICs, type **Enter**.

```
---------------------------------
Configuring Network interface eth0...
Device:  Intel Corporation, 82546GB Gigabit Ethernet Controller

  eth0 :         192.168.1.1/255.255.255.0

(e)     - Edit or delete current eth0 setup
(a)     - Change current eth0 aliases setup
(b)     - Blink eth0 associated LED for easy identification
[Enter] - Exit eth0 configuration
e
```

4. Enter a NIC index number to configure another NIC (or reconfigure the same NIC). Repeat as many times as needed.

After all interfaces have been configured, type **Enter** to finish setting up the NICs and continue to the routing setup.

5. Select one of the following options:

   ■ Type **Enter** to accept the routing configuration.

   ■ Type an index number to modify or delete a routing entry index.

   ■ Type **a** to add a routing entry.

```
Step 4/8: Network Configuration
------------- Routing table configuration ------------------------
(0):     default 192.168.1.254

(0)     - Index of entry above - Modify or delete an entry
(a)     - Add a new route entry
[Enter] - Exit routing configuration
0_
```

> **Note**
>
> If the IP address of the Forcepoint DLP server is not on the same subnet as the one specified for the mobile management NIC, a gateway is required to tell the mobile agent how to communicate with the Forcepoint DLP server.

6. After the routing configuration is complete, the wizard displays a prompt to store the network configuration.

■ To store the network definitions, type **Y**. The network configuration details are saved, and the network service is reloaded with the new parameters. The new parameters (IP address, network prefix, and gateway) are displayed in the wizard.

■ To start over without storing the network definitions, type **n**.

```
This wizard is about to reload your network.
Running services may disconnect during this process.
Do you want to continue (Y/n) Y
```

7. Type the index number of the management NIC, or type **c** to define the network parameters.

This NIC can be used for other purposes, such as SSH connections, access points for mobile devices, and Exchange communications.

```
Step 4/8: Network Configuration


Configured network interfaces and their current configuration:
(0)  eth0 : 10.0.32.9/24

Please select the management IP/interface from the list above (0-0)
or type (c) to configure networking: 0
```

STEP 5: Define the host name

1. Type the Fully Qualified Domain Name (FQDN) for the mobile appliance.

```
Step 5/8: Hostname and Domain

Enter the Fully Qualified Domain Name (FQDN) of this appliance:
[protector-5515]: oldprotector

To secure connection, users must set up their mobile devices to accept
security certificates from the server. The default certificate is a self signed
certificate automatically generated by Forcepoint.

Please enter the name to use for the default certificate in the Subject field
or press Enter to use the FQDN for the mobile appliance.
[oldprotector]: _
```

2. Type the name to use for the default security certificate in the Subject field.

This can be used to secure the connections between mobile devices and the mobile agent using the default certificate. The default certificate is a self-signed certificate automatically generated by Forcepoint.

STEP 6: Define the domain name server

Optionally, in the wizard, type the IP address of the Domain Name Server (DNS) that will service this mobile agent. A DNS will allow access to other network resources using their names instead of their IP addresses.

```
Step 6/8: Domain Name Servers (DNS)

No DNS servers defined

Enter the IP address of the DNS server to add.
(Press [Enter] to skip this stage): 10.11.1.37


The following DNS server(s) are currently defined:
10.11.1.37

Enter the IP address of the DNS server to add.
(Press [Enter] to leave current settings or type 'Delete' to delete it.): _
```

> **Important**
> Type the IP address of the DNS server if the back-end Exchange server is identified by its hostname in the Forcepoint Security Manager instead of by its IP address.

STEP 7: Set the date, time, and time zone

1. Type the current time zone (to view a list of all time zones, type **list**).
2. Type the current date in "dd-mm-yyyy" format.
3. Type the current time in "HH:MM:SS" format. Note that this is a 24-hour clock.

```
Step 7/8: Date and Time

Current timezone: GMT0
Enter a new timezone
(Press [Enter] to leave unchanged or type 'List' to view all available zones):
Asia/Jerusalem

Current date: 02/08/2016
Enter new date in dd-mmm-yyyy format
(Press [Enter] to leave unchanged):

Current time: 10:09:25
Enter time in HH:mm:ss format (24-hour format)
(Press [Enter] to leave unchanged): _
```

STEP 8: Register with a Forcepoint DLP Server

In this step, a secure channel will be created connecting the mobile agent to a Forcepoint DLP Server. This can be 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.

3. Type **Enter** to exit the wizard. A message displays stating that the configuration was successful.

Step 9: Reboot the mobile agent appliance

Reboot the mobile agent appliance. This completes the IPv6 disabling process that the wizard starts.

Final step: Verification

In the Data Security module of Security Manager, verify that the mobile agent status is no longer pending, and that the icon displays its active status. Refresh the browser.

Click **Deploy**.

The mobile agent is now ready to be configured. See the Getting Started Guide for instructions.

Integration agent

In this topic:

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 35
● *Special considerations for IBM Notes and Domino*, page 35
● *Installing the crawler agent*, page 36

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*.

● For operating system requirements, see <u>System requirements for this version</u>.

● For port requirements, see <u>Forcepoint DLP ports</u> (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 (Forcepoint84xSetup.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 38
- *Deploy settings fails*, page 39
- *Subscription errors*, page 39

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/mgmtd.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 Asuthorities > 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 41.
2. Perform the installation. See *Installation steps*, page 42.
3. Configure the protector in the Data Security module of the Security Manager. See *Final step: Verify the protector installation*, page 47.

Protector installation prerequisites

Before installing the protector:

- Make sure the hardware that will host the protector soft appliance meets the requirements specified in <u>System requirements for this version</u>.
- 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 <u>Forcepoint DLP ports</u> (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.

Installation steps

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, **DataProtectorMobile84x.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.

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: pcnet32   mac: 00:0C:29:59:56:2B  inet: 192.168.1.1/24)
(1)   eth1  (driver: pcnet32   mac: 00:0C:29:59:56:35  inet: 0.0.0.0/0)
(2)   eth2  (driver: pcnet32   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.

6. 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:       79c970 [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]: _
```
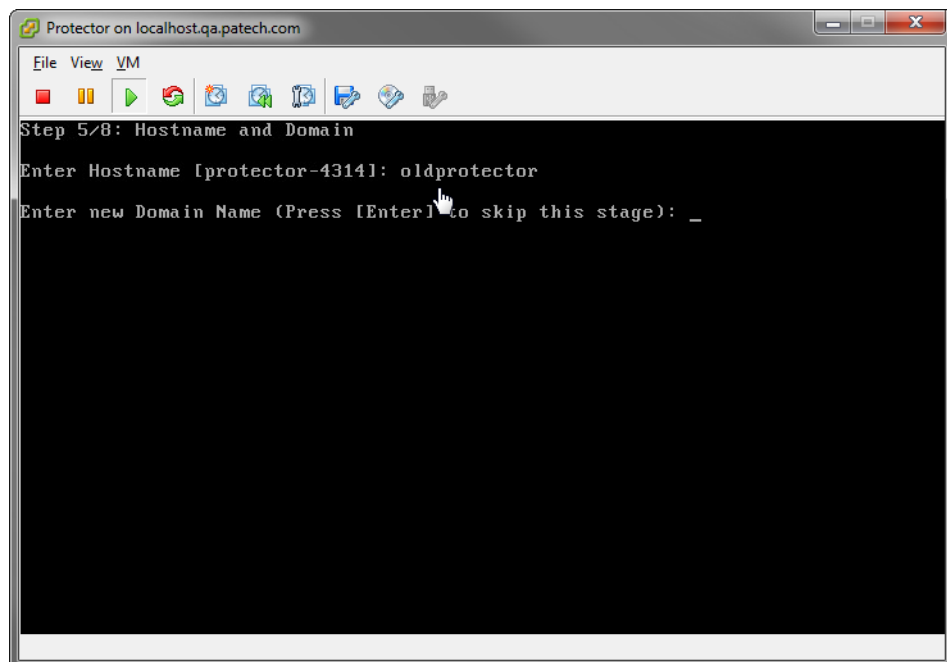
STEP 5: Define the hostname and domain name

1. 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): _
```

2. 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.
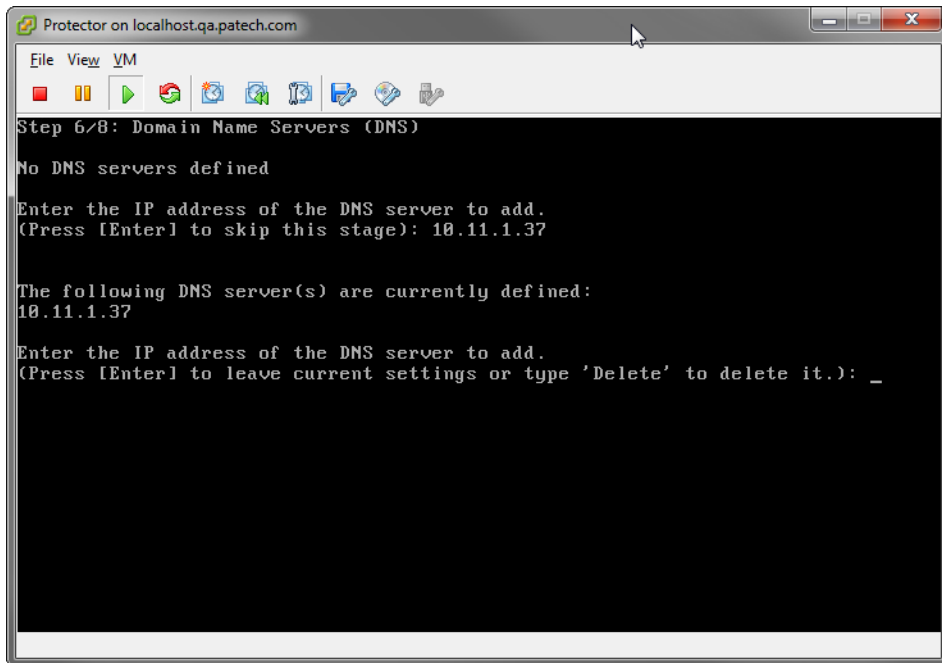
STEP 7: Set the date, time and time zone

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.
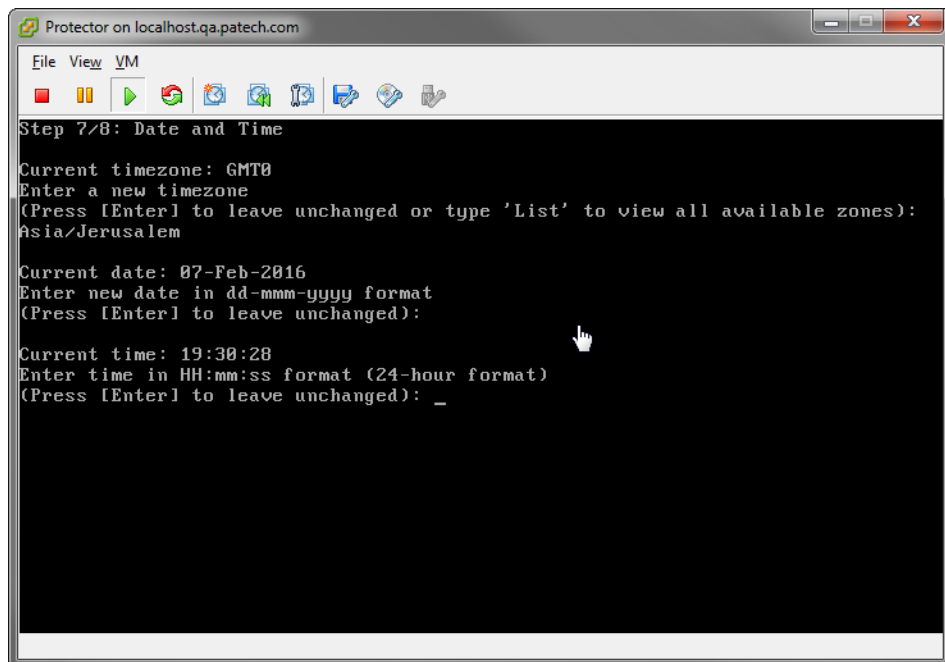
STEP 8: Register with a Forcepoint DLP Server

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 PAMA Watchdog...                                  [  OK  ]


Ebtables 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.

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.

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.

Content Gateway is also included in Forcepoint Web Security. In this mode, Content Gateway also offers URL categorization, content security, web policy enforcement, and more.

This document describes how to install the core Web Content Gateway component for Forcepoint DLP. For instructions on setting up Forcepoint Web Security, see the [Forcepoint Web Security Installation Guide](#).

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

Preparing the operating system for Content Gateway

Content Gateway supports Red Hat Linux 6 series, 64-bit, Basic Server and the corresponding CentOS version.

Special steps must be taken to install and configure such versions to work with Content Gateway v8.4.x.

> ⚠️ **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.

biosdevname

Red Hat Enterprise Linux 6, update 1 introduced **biosdevname**, which is not supported by Content Gateway.

The easiest way to disable biosdevname is to do it during operating system installation (recommended). To do this:

1. Start the installation:

2. When the installer starts, press [TAB] and alter the boot line to add **biosdevname=0** as follows:
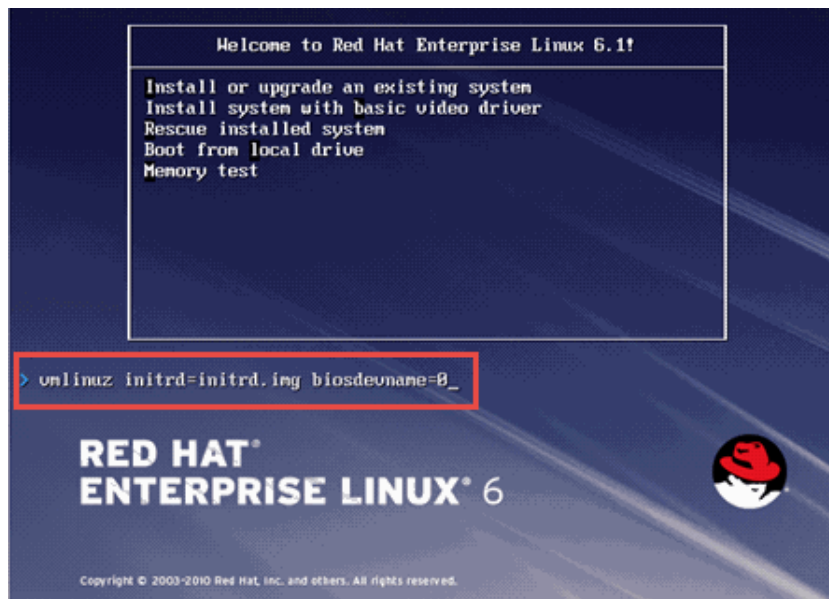
3. Proceed through the rest of the installer as usual.

If biosdevname was not disabled during operating system installation, it can be disabled later, as follows:

1. 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#," continue with step 2.

2. Log in as **root**.

3. Navigate to the network-scripts directory:

   ```
   cd /etc/sysconfig/network-scripts
   ```

4. Rename all "ifcfg-<ifname>" files except "ifcfg-lo" so that the names take the following format:

   ```
   ifcfg-eth#
   ```

   a. Start by renaming "ifcfg-em1" to **ifcfg-eth0**, then continue with the rest of the "ifcfg-em#" files.

   b. After renaming the "ifcfg-em#" files, 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, suppose the initial set of interfaces presented by "ifconfig -a" is:

      ```
      em1 em2 em3 em4 p1p1 p1p2 p2p1 p2p2
      ```

      In this case, rename the interfaces as follows:

      ```
      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 there are 6 interfaces, they are named eth0 through eth5.

5. Edit all the ifcfg-eth# files as follows:

    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#"

6. Remove the old udev device mapping file if it exists:

```
rm -f /etc/udev/rules.d/70-persistent-net.rules
```

7. Modify the "grub.conf" file to disable biosdevname for the kernel that is booted:

    a. Edit the **/boot/grub/grub.conf** file.

    b. Add the following to the end of the "kernel /vmlinuz" line:

```
biosdevname=0
```

8. Reboot.

9. Reconfigure the interfaces as required.

Prepare for installation

1. 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](#).

2. 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).

```
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).

3. 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.

4. If there will be multiple, clustered instances of Content Gateway:

- Find the name of the network interface 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
    ```

5. 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.

6. Download the **ContentGateway84xSetup_Lnx.tar.gz** installer tar archive from the My Account > Downloads page at support.forcepoint.com. Save the file to a temporary directory on the machine that will host Content Gateway.

    To unpack the tar archives, use the command:

    ```
    tar -xvzf ContentGateway84xSetup_Lnx.tar.gz
    ```

7. 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 Web Content Gateway features.

> **Note**
> If you customized any ports that Forcepoint software uses for communication, replace the default port with the custom port you implemented.

- 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]().

8. 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]().

Install Content Gateway

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.

Step 1: Starting the installation

1. Elevate to root permissions:

   ```
   su root
   ```

2. In the directory containing the unpacked tar archive, use the following command to launch the installation.

   ```
   ./wcg_install.sh
   ```

The installer installs Content Gateway in the /opt/WCG directory. It is installed as **root**.

> **Note**
>
> Up to the configuration summary, it is possible to quit the installer by pressing Ctrl-C. After that point, to abandon the installation, first allow the installation to complete, then uninstall Content Gateway.
>
> The configuration summary gives the option to change the answer to any installer prompt. It is not necessary to quit the installer and restart to change a setting.

3. If the server does not meet the minimum hardware requirements, is missing required operating system packages, or has conflicting processes running, error or warning messages appear.

   ■ If system packages are missing, the message looks like this:

   ```
   Error: Forcepoint Content Gateway v8.4.x on x86_64
   requires several packages that are not present on your
   system.

   Please install the following packages: <list of packages>

   If you are connected to a yum repository you can install
   these packages with the following command:

   yum install <list of packages>
   ```

   Install the missing packages and restart the Content Gateway installer.

   ■ System resource warnings give the option to continue the installation:

   ```
   Warning: Forcepoint 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. Performance may be affected if Content Gateway is installed on a system with insufficient resources.

   ■ If the NetworkManager or avahi-daemon process is running, an error like the following is displayed:

   ```
   Error: The avahi-daemon service is enabled on this system
   and must be disabled before Forcepoint Content Gateway
   v8.4.x can be installed.

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

       chkconfig --levels 2345 avahi-daemon off

       service avahi-daemon stop
   ```

To continue, stop the conflicting processes, then restart the installer. For example:

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

4. 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
```

Step 2: 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.

Step 3: 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 Installing the Cloud Agent

In this topic:

Forcepoint DLP Cloud Applications includes a cloud agent that provides cloud activity content inspection for files uploaded into and stored within cloud enterprise services, including Microsoft OneDrive for Business and Box. By applying established DLP policies to data stored in enterprise cloud applications, the agent is able to audit and prevent the storage of sensitive data that could expose organizations to data loss and compliance infringements.

The cloud agent can be installed in a private data center (on-premises) or in the Microsoft Azure cloud with management components on-premises.

The system can support multiple cloud agents, each running on a different cloud service.

Cloud agent system requirements

- For operating system requirements, see <u>System requirements for this version</u>.
- For port requirements, see <u>Forcepoint DLP ports</u> (the "Cloud agent" section).
- Make sure that the Docker containerization system (instructions below) is at v1.12 or later.

Supported cloud services

- Microsoft OneDrive for Business
- Box

Preparing Box for use with the cloud agent

The cloud agent can be deployed through the Azure cloud or installed on-premises. Because the services it interacts with are hosted in the cloud, deploy the agent in the cloud for best performance.

STEP 1: Create a Box application

1. Go to https://developer.box.com/ and log in with **Admin** credentials.

    > **Important**
    >
    > Logging in with Admin credentials is required. Only the admin account has permissions to manipulate data for the entire enterprise.

2. On the Create A New Box App page, select Custom App, then click **Next**.

3. On the Authentication Method page, select **Standard OAuth 2.0 (User Authentication)**, then click **Next**.

4. Give the app a unique name, then click **Create App**.

5. A confirmation message displays to say that the app has been created. Click **View Your App**.

6. When the Developer Console opens, go to the **Configuration** page.
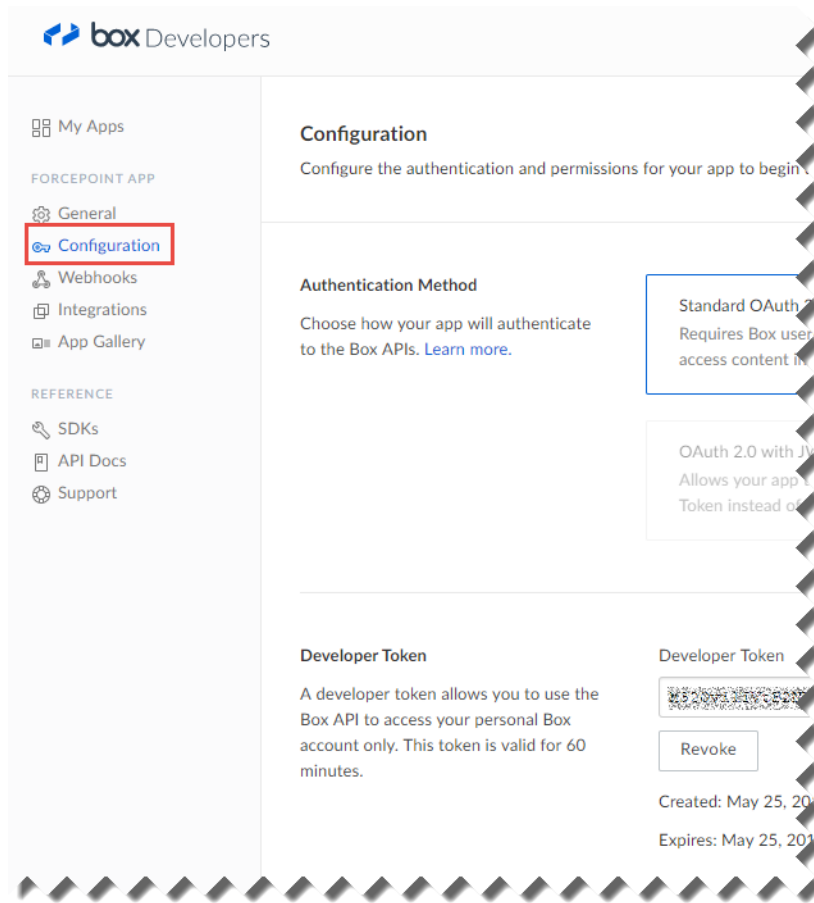
7. Copy the Client ID and Client Secret. They will be needed in future steps.

8. Fill in OAuth 2.0 Redirect URI with the following:

    ```
    https://<manager_IP/host>:9443/dlp/pages/cloudService/
    cloudServiceCompletedAuthClientWindow.jsp
    ```

    Replace <manager_IP/host> with the IP address or hostname of the Forcepoint Security Manager.

    The URL is used to connect to the Forcepoint Security Manager, which must therefore be reachable from the Internet.

    > **Note**
    >
    > The on-premises cloud agent must be reachable from the Internet on port 8080. This may require a DNS update, in addition to a firewall rule for NAT.

9. Click **Save Changes**.

It is always possible to go back to https://developer.box.com/ to view or edit the application.

STEP 2: Submit a case to Box Support to enable the As-User functionality

1. Go to https://community.box.com/t5/custom/page/page-id/ BoxSearchLithiumTKB.

2. Log in with Admin credentials.

3. In the Select Area drop-down list, select **API or Developer Question/Issue**.

4. In the List Keywords drop-down list, enter **As-User**.

5. In the pop-up, click **Continue**.

6. In the Submit an API Case Description add the following:

   I would like to enable the As-User functionality in my Box Application.

   Thank you.

7. Set the Severity to **High**.

8. Use the CC field to add the email addresses of anyone who should be copied on this case.

9. In the API Key field, enter the app's Client ID (saved from the procedure above).

10. Click **Submit**.

Once the case is resolved by Box Support, continue with continue with *Cloud agent installation steps*, page 80.

Preparing One Drive for use with the cloud agent

> **Note**
> The instructions in this section show the classic Azure portal. Administrators can use the matching configuration options in the new Azure portal.

STEP 1a: Create an Azure Active Directory application for OneDrive

To connect Azure Active Directory with the management server, start by creating an Azure application. The application acts as a bridge between the cloud service and Forcepoint DLP.

1. Log onto the Azure Portal, https://manage.windowsazure.com.
2. Click **Active Directory**, then select a user directory.
3. Click **Applications**.
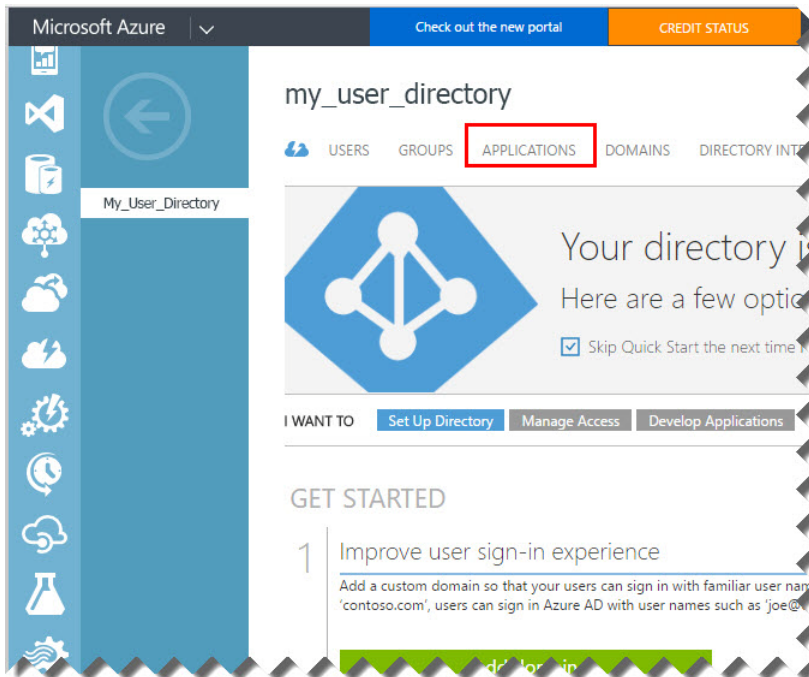
4. To create a new application:

   a. Click **Add**.
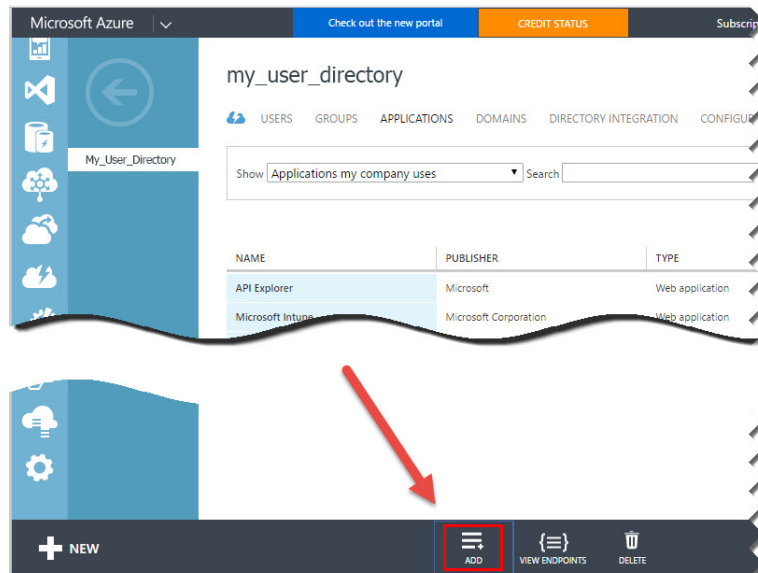
b. Select **Add an application my organization is developing**.
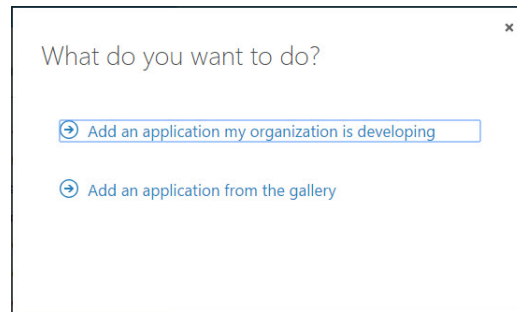
c. Enter a descriptive **Name** for the application, such as "Forcepoint cloud agent."

d. For Type, select **Web application and/or web API**.

e. When prompted, enter a sign-on URL in the following format:

    ```
    https://<server_ip>:9443/dlp/pages/cloudService/
    cloudServiceCompletedAuthClientWindow.jsp
    ```

■ This is the URL where users can sign in and use the app.

■ The URL is used to connect to the Forcepoint Security Manager, which must therefore be reachable from the Internet.

■ App ID URI is not required for the Forcepoint DLP cloud agent.

> **Note**
>
> The on-premises cloud agent must be reachable from the Internet on port 8080. This may require a DNS update, in addition to a firewall rule for NAT.

5. Click **Configure**. The properties for the new application are shown.
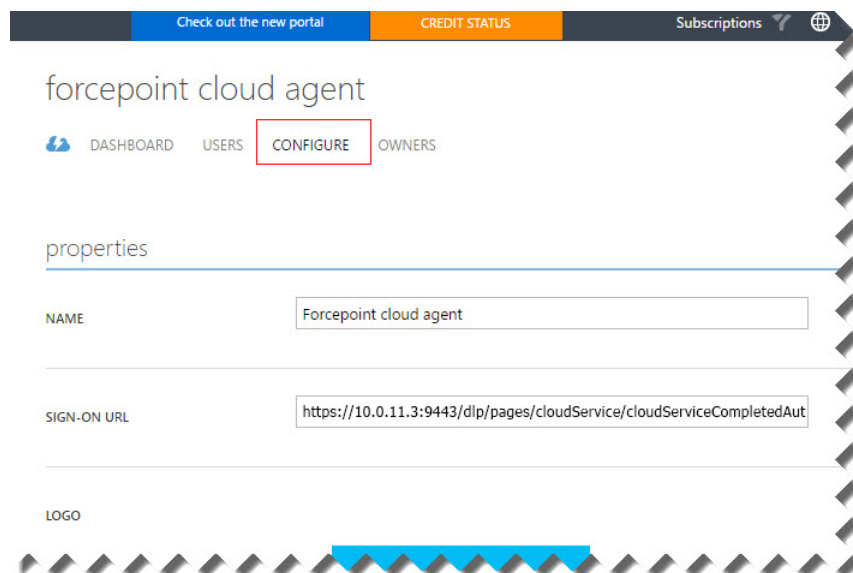
6. Scroll down to view the **Keys** section. Select a key duration (1 year or 2 years).

7. Under Permissions to other applications, click **Add application**.

8. One by one, add the Office 365 services for which your app requires permissions:

   ■ Office 365 Management APIs

   ■ Office 365 SharePoint Online

   Windows Azure Active Directory is already chosen.

   To locate a service, select **All Apps** under **Show**, and search for the first letter of its name. Select the service name when it appears, then click the check mark.
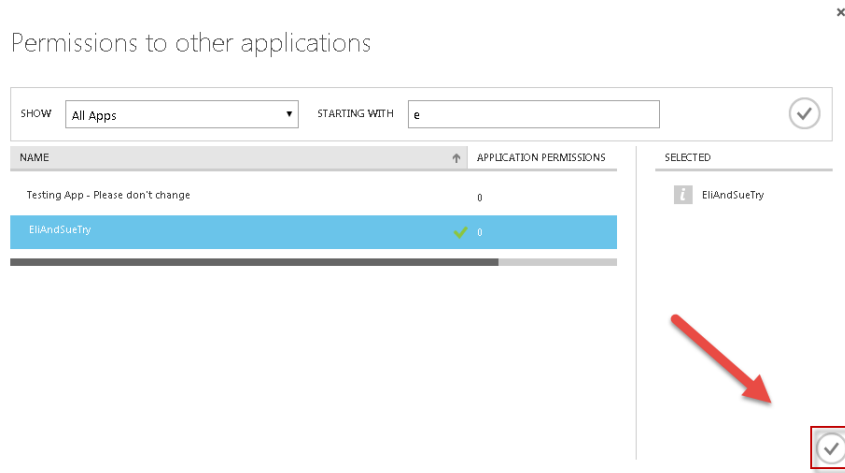
9. Using drop-down menus, select the **Application Permissions** and **Delegated Permissions** that the app requires for each service. These are the permissions that will be displayed to app users when Azure prompts them to consent to the app's permission request.

   The cloud agent requires the following permissions:

Application	Application Permissions	Delegated Permissions
Windows Azure Active Directory	• Read all hidden memberships • Read and write devices • Read and write directory data • Read and write domains • Read directory data	none
Office 365 Management APIs	• Read DLP policy events including detected... • Read activity data for your organization • Read service health information for your organization	• Read DLP policy events including detected ... • Read activity data for your organization • Read service health information for your organization

Application	Application Permissions	Delegated Permissions
Office 365 SharePoint Online	• Read user profiles • Read and write user profiles • Read and write managed metadata • Read managed metadata • Have full control of all site collections • Read items in all site collections • Read and write items in all site collections	none
Microsoft Graph	none	Access directory as the signed in user

10. Click **Save**.

    Copy and store the Client ID and Key that display. These are needed to configure the cloud agent in the Forcepoint Security Manager.
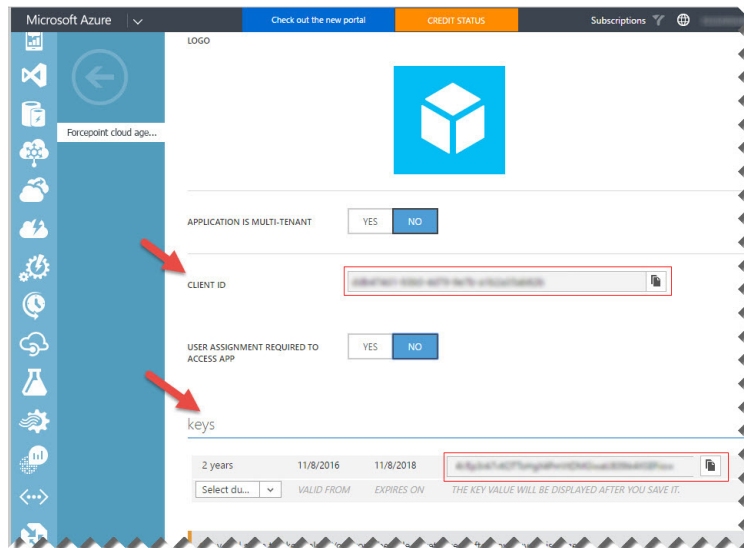
STEP 2: Create a virtual (or physical) machine

On-premises deployments

For on-premises deployments, install a VM or physical machine with CentOS 7.

Continue with *Preparing the CentOS environment*, page 73.

Azure deployments

1. In the Azure Portal, click **Virtual Machines** in the left navigation pane, and then click **New > Compute > Virtual Machine > From Gallery**.
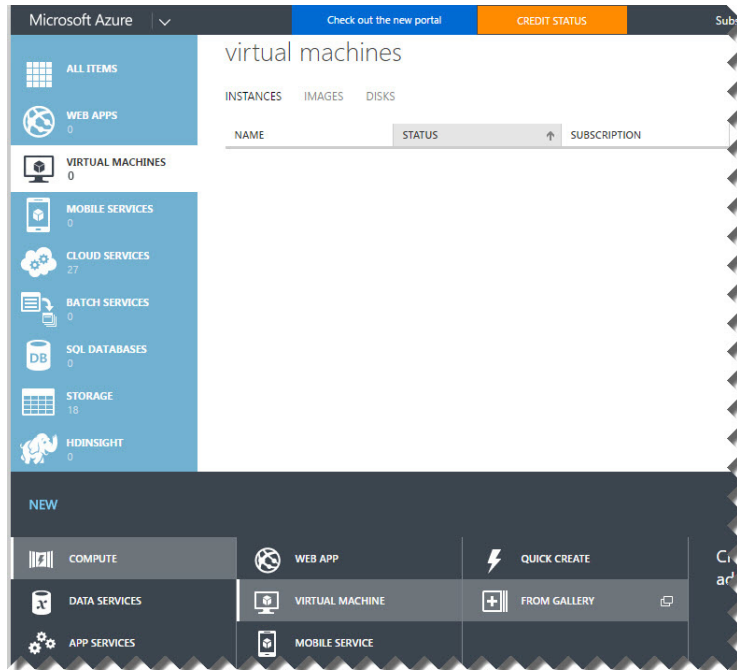
2. Under Choose an Image, select **CENTOS-BASED**, and then select an **OpenLogic** version. As a best practice, select the latest for more security and scalability.

   When you are finished, click the right arrow.
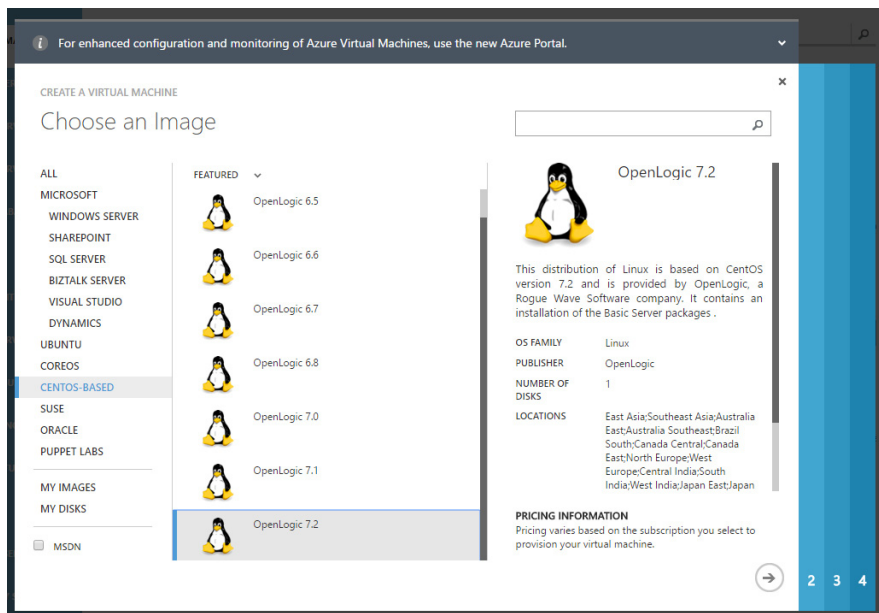
3. On page 2 of the wizard, under Virtual machine configuration:

   a. Enter the **Virtual Machine Name** for the cloud agent VM. This is usually the DNS name.

   b. Under Tier, select **Standard**.

   c. Select a **Size**. A3 is the minimum recommended.

   d. Enter a **New user name**.

   e. Under Authentication, select **Provide a password**.

   f. Enter and confirm the password.

   g. Click the right arrow to continue.

Note that controlling the VM and doing root activities remotely require activating a remote logon as root user. Your HelpDesk can assist with this.

4. On page 3, under Virtual machine configuration:

   a. Select **Create a new cloud service** (recommended), or select an existing cloud service.

   b. Enter a **Cloud Service DNS Name**. This name will be published on the Web. It is not part of the organization's local DNS.

   c. Select an Azure **Subscription** type.

   d. Under Storage Account, select **Use an automatically generated storage account**.

   e. Under Availability Set, select **None**.

   f. Modify the ports as shown below: SSH, TCP, 22, 22.

g. Click the right arrow to continue.

Note that the Region/Virtual Network and Virtual Network Subnets field show values inherited from VPN set up. These do not need to be changed.

5. Click the check mark in the lower right corner of page 4 to build the VM.

Continue with *Preparing the CentOS environment*, page 73.

Preparing the CentOS environment

After installing CentOS, perform the following steps to ensure a successful deployment:

1. Log in to the CentOS machine or VM as root.

2. Enter the following command:

    ```
    yum install ntpdate -y
    ```

3. Enter the following command:

    ```
    yum install net-tools -y
    ```

    This is for support of the "ifconfig" command used by the cloud agent installer.

4. Enter the following command:

    ```
    ntpdate time.nist.gov
    ```

5. Enter the following command:

    ```
    yum update -y
    ```

6. For successful cloud agent installation, ensure that the "cloud_app_agent" directory is in the system $PATH. To do this:

   a. Open the **/root/.bashrc** file for editing.

    b.   Add the following line after the alias declarations:

```
export DCA_HOME="/opt/forcepoint/cloud_app_agent/"
```

    c.   Safe and close the file.

7.   Reboot the machine or VM.

8.   Log in to the machine again and verify that the time is correct.
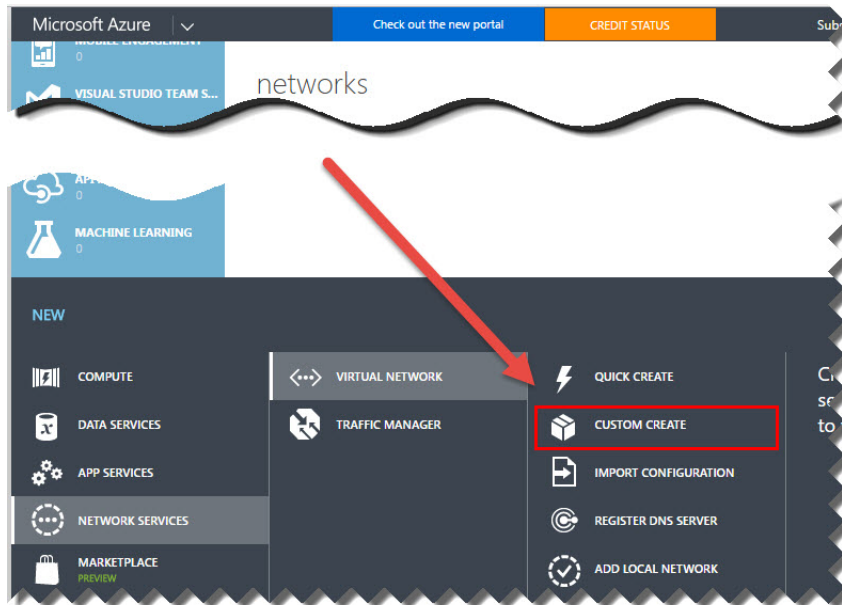
Continue with *STEP 3: (Azure deployments only) Configure a Virtual Network and Point-to-Site VPN in Azure*, page 74.

STEP 3: (Azure deployments only) Configure a Virtual Network and Point-to-Site VPN in Azure

1.   In the Azure Portal, click **Networks** and then **New** to create a new virtual network.
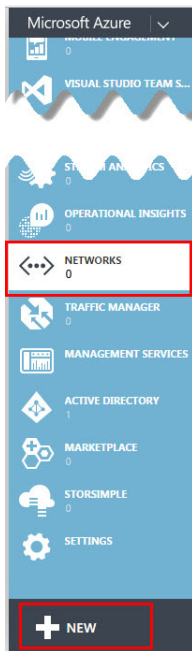
2.	Click **Custom Create**.

3.	Enter a name for the virtual network you are creating, choose a location, then click the right arrow.

	Location refers to the physical location (region) where you want your resources (VMs) to reside. Choose the location closest to you. It will be used for all the other components such as the storage space and the VM.

4.	Optionally, enter a DNS server name and IP address, then select **Configure a point-to-site VPN** and click the right arrow.

	If DNS will not be used, leave the DNS Servers section blank.

For instructions on creating site-to-site VPNs, see this Microsoft article.
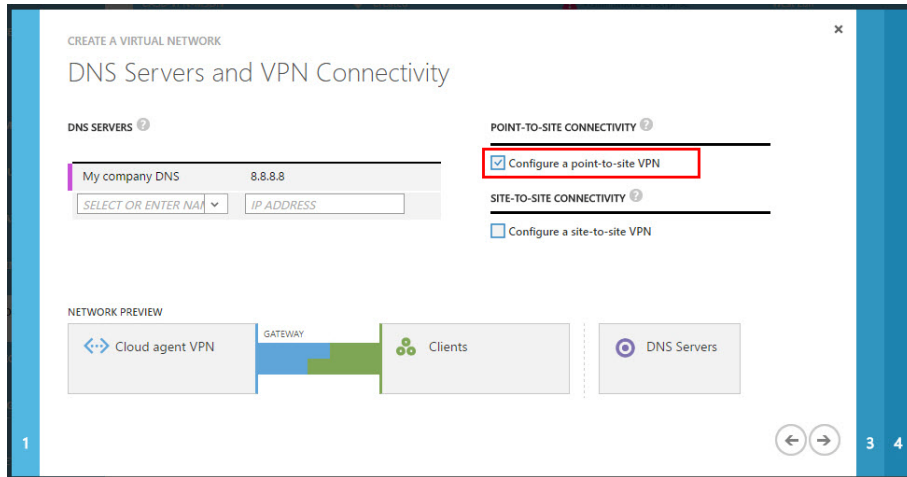
5. Configure the VPN client's IP address range.

   Include a starting IP address and address count.

   ■ This cannot be the IP address range that is being used for on-premises Forcepoint DLP components. (Using the same range would cause a routing issue on the management server and SQL Server machines.)

      For example, if the on-premises servers are using 10.x.x.x, use 192.168.x.x or 172.16.x.x as the starting IP address for this virtual network.

   ■ Only one address space is required. Click the right arrow when done.
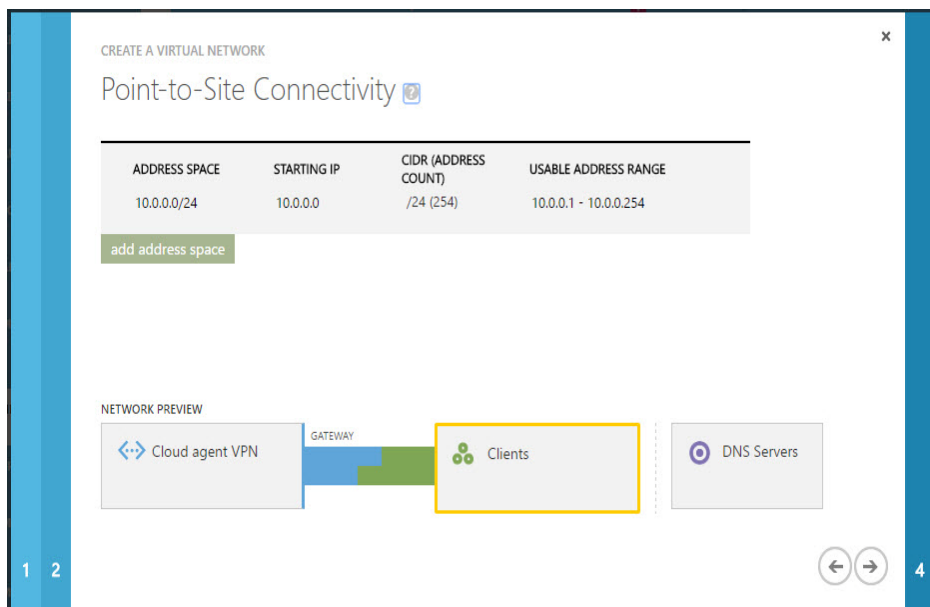
6. Specify the address range to use for the virtual network. The VM created in Azure will be allocated an IP address from this VPN's range.

   Click **Add Gateway Subnet** to create a subnet for the gateway (required).

For best practice use a 29-bit subnet mask. This ensures that your IP address pool has 6 addresses and helps ensure a speedy recovery in case of disconnection.

Click the check mark when done.

> **Note**
>
> None of the virtual IP addresses should be on same subnet as the on-premises management server. Keeping them on separate subnets prevents problems with the automatic VPN connection script that will be used later in this procedure.

7. Select the network that was just created from the list, then click **Create Gateway** to create the gateway. This can take 15-30 minutes.
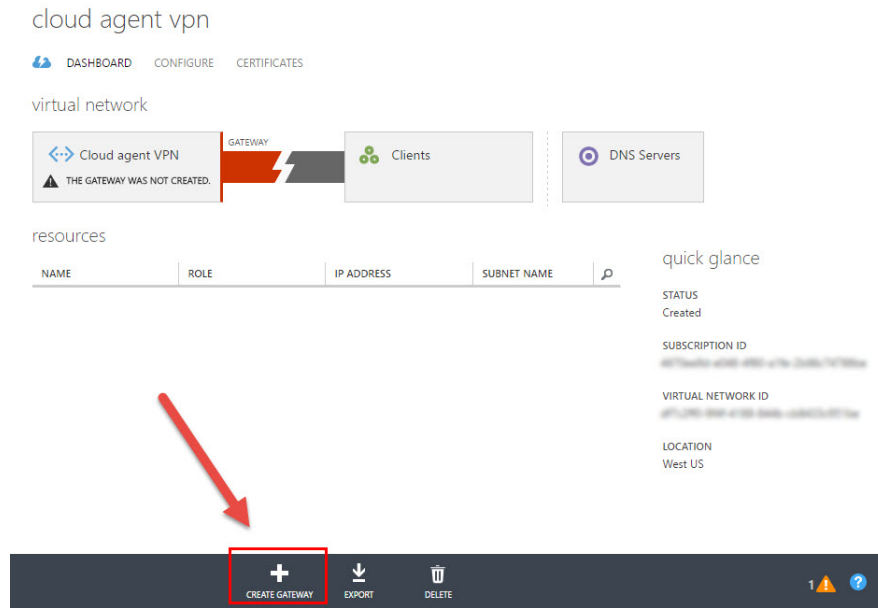
8. Create security certificates to authenticate VPN clients. For instructions, see [this Microsoft article](). To complete the process:

    a. Generate a self-signed root certificate.

    b. Upload the root certificate file to the Azure Portal.

    c. Generate a client certificate.

    d. Export and install the client certificate on the Forcepoint management server.

9. Download the 64-bit client VPN package to the management server and install it.
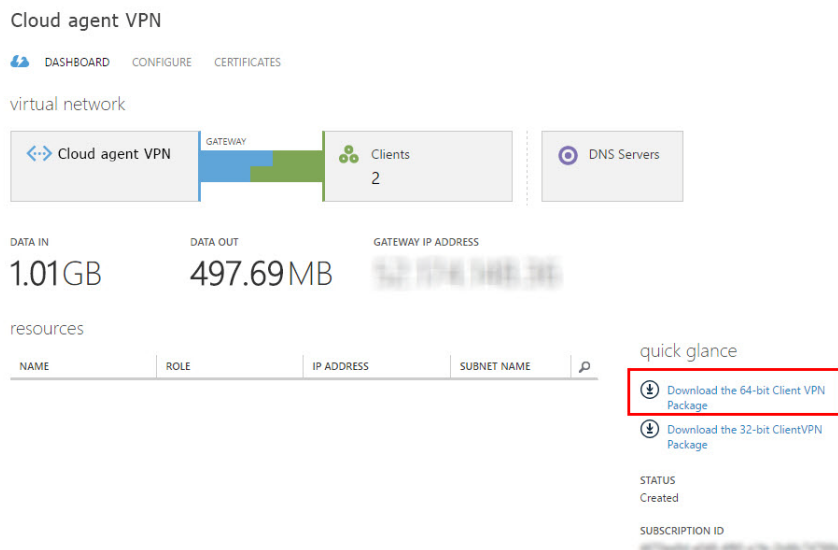
10. Open the VPN client software and click **Connect** to connect the client to the virtual network.

11. On the VPN client machine, open a command prompt and use the **ipconfig** command to find the IP address assigned to the machine.

12. Connect the management server to the Azure VPN network as follows:

    a. On the management server, download the VPN connection script, **p2s_vpn_connect.ps1**, from the My Account > Downloads page at support.forcepoint.com.

    b. Open the script in a text editor.

    c. Edit the following parameters with the values used in the **pre-deploy.ps1** script. This is the script that was edited when building the virtual network in Azure.

    The default values are:

    ○ $vpnName - ForcepointVNet (virtual network name)
    ○ $vpnNet - 192.168.0.0 (VPN network IP, server side)
    ○ $vpnNetmask - 255.255.0.0 (VPN subnet mask, server side)
    ○ $vpnClientIP - 172.16.1.1 (VPN client's IP address)

    Make sure each entry is on a separate line, and place quotation marks around the entries, as shown below:

    ```
    <parameter> = "<value>"
    ```

    For example:

    ```
    #Name of virtual network
    ############################################
    $vpnName = "ForcepointVNet"


    #The VPN network IP and subnet mask (server side)
    ############################################
    $vpnNet = "192.168.0.0"


    $vpnNetmask = "255.255.255.0"


    #The VPN client IP (Windows side IP)
    ############################################
    $vpnClientIP = "172.16.1.1"
    ```

    The default log path is c:\vpn_reconnect.log. This can be changed, if needed.

    The default user directory path is C:\Users\Administrator\AppData\Roaming\. The administrator named here must be the one who installed the Azure VPN client. Edit the Administrator as needed.

    d. Save and close the file.

e. Use the following command to change the PowerShell Script Execution Policy from Restricted to RemoteSigned so that local PowerShell scripts can be run:

```
Set-ExecutionPolicy RemoteSigned
```

f. Run the revised script from PowerShell. This connects the management server to the VPN network and keeps them connected at all times.

> **Important**
>
> If the management server is restarted for any reason, this script must be run again. As a best practice, add the script to the Windows Task Scheduler so that it runs on startup. For instructions, see this knowledge base article.

g. If the system is using a remote database, copy the script onto the database machine and run it there as well.

Continue with *Cloud agent installation steps*, page 80.

Cloud agent installation steps

STEP 1: Install Docker

This section applies to both Azure and on-premises deployments.

- If the Docker containerization system version 1.12 or later is already installed, skip to *STEP 2: Run the cloud agent installation wizard*, page 80.
- If an earlier version of Docker is installed, follow the product's update instructions to move to version 1.12 or later (see https://docs.docker.com/).
- Otherwise, install Docker version 1.12 or later according to the product's installation instructions (available at https://docs.docker.com/).

STEP 2: Run the cloud agent installation wizard

This section applies to both Azure and on-premises deployments.

1. On the Linux server, use the following command to run the Forcepoint installation wizard:

```
./CloudAgent84
```

2. You are asked if you want to proceed with the installation. Type **Y**.

3. The installer checks prerequisites and begins installing the module.

4. To accept the license agreement, enter **Y** when prompted.

5. Do one of the following:

   ■ If the server will connect to an Azure VPN network, enter **Y**.

■ If the server will connect to an on-premises server, enter **N**.

6. Enter the IP address or FQDN of the Forcepoint DLP server to which this cloud agent will connect. This can be the management server or a supplemental server.

7. Enter the **user name** of the Forcepoint DLP service account administrator.

8. Enter the account **password**.

9. Wait, while the installer registers the module with the management server and with Azure.

    When the process completes successfully, a message is displayed.

To complete the setup process, see the Getting Started Guide for initial configuration steps.

7 Adding, Modifying, or Removing Components

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 executable.
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 83
- *Repairing Forcepoint DLP components*, page 84
- *Changing the Forcepoint DLP service account*, page 85

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 (**Forcepoint84Setup.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**.

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.