Installation Guide: Forcepoint URL Filtering

Installation Guide | Forcepoint URL Filtering | v8.5.x | 30-Nov-2018

Follow the instructions in this document to complete a typical installation of Forcepoint™ URL Filtering. In this configuration:

- The policy source (the standalone or primary Policy Broker and its Policy Server) resides on the Forcepoint Security Manager machine (the management server).
- Log Server resides on a dedicated Windows server.
- The reporting databases are hosted on a full version (not Express) of Microsoft SQL Server on its own machine.

This installation procedure includes the following steps:

Step 1: Prepare for installation

Make sure the servers you intend to use meet or exceed the System requirements for this version.

Prepare the database server

Make sure that:

- A supported version of Microsoft SQL Server is installed and running in your network. See this article to see a list of supported versions.
- The latest service pack for your version has been applied.
- The SQL Server Agent service is running on the database host.
- The database host can be reached from the machine that will host the management server.
- You have identified a SQL Server or Windows Trusted account with appropriate permissions to create the database and run SQL Agent jobs.

  See Installing with SQL Server for details on the necessary permissions.

Note

An end user whose traffic is managed by Filtering Service has no direct or indirect influence over the database. Thus, although the log entry is stored in the SQL Server database, the user did not direct its storage and cannot retrieve it.

The only interface to the database itself is from Log Server, the reporting services, and the management console. Filtering Service does not access the database, but instead sends information via Log Server.

Verify support for your integration product

If you will be integrating your software solution with a third-party proxy, cache, firewall, or network appliance:

- Verify that you have selected a supported integration product.
  - Cisco Adaptive Security Appliance (ASA) v8.0 and later, or Cisco IOS routers v15 and later

    See Integrating Forcepoint URL Filtering with Cisco for more information.
  - Citrix XenApp 5.0, 6.0, and 6.5

    See Integrating Forcepoint URL Filtering with Citrix for more information.
  - Microsoft Forefront Threat Management Gateway (TMG)

    See Integrating Forcepoint URL Filtering with TMG for more information.
  - Blue Coat appliances via ICAP

    See Integrating Forcepoint URL Filtering using ICAP Service for more information.
  - Other third-party products are supported using the “universal integrations” option. See Installing for Universal Integrations for more information.
- Make sure that the integration product is installed and running before you begin.

Prepare your Windows servers

Because Forcepoint URL Filtering management and reporting components can only reside on Windows servers, prepare at least two Windows servers: one to be the management server and one to host Log Server.

Before starting the installation process, on every Windows server that will host Forcepoint URL Filtering components, do the following:

1. Make sure there are no underscores in the machine's fully-qualified domain name (FQDN). 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.

2. Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
3. Verify that there is enough disk space to download the installer, extract temporary installation files, and install the management components on the Windows installation drive (typically C).
4. Make sure that .NET Framework versions 3.5 **and** 4.5 are installed.
   - Windows Server 2008 R2 (v8.5 only): You can use Server Manager to install .NET 3.5. Usually the feature is on by default. You must download .NET 4.5 from the Microsoft site.
   - Windows Server 2012 or 2012 R2: Both .NET 3.5 and .NET 4.5 can be installed using the Server Manager. Usually, v3.5 is off by default and v4.5 is on by default. Turn them both **on**.

   Note that .NET Framework 4.5 must be installed before adding any language packs to the operating system (as noted in the following article from Microsoft: https://msdn.microsoft.com/en-us/library/5a4x27ek(v=vs.110).aspx#To install language packs.).
5. Synchronize the clocks on all machines (including appliances) where a component will be installed. It is a good practice to point the machines to the same Network Time Protocol server.
6. Disable the antivirus software on the machine before installation. After installation, before restarting your antivirus software, see this section of the Deployment and Installation Center.
7. Disable any firewall on the machine before starting the installer and then re-enable it after installation. Open ports as required by the components you have installed, and make sure that required ports are not being used by other local services on the machine.
   - Some ports are used only during installation and can be closed once installation is complete.

- See the Web tab of the Forcepoint Ports spreadsheet for more information about ports.

8. Disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation.
9. Copy the Forcepoint Security Installer (**Forcepoint85xSetup.exe**) to a temporary directory on the machine.

   Find the installer executable on the Downloads tab of the My Account page at forcepoint.com. You can download the installer to your network, then copy it to each Windows server that will host Forcepoint components.

   Note that the installer is quite large, so the download process may take some time.

Prepare your Linux servers

Before starting the installation process, on every Linux server that will host Forcepoint URL Filtering components, do the following:

1. If SELinux is enabled, disable it or set it to permissive.
2. If a firewall is active, open a command shell and use the **service iptables stop** command to shut down the firewall before running the installation.

   After installation, restart the firewall. In the firewall, be sure to open the ports used by web protection components installed on this machine. See the Web tab of the Forcepoint Ports spreadsheet for more information about ports.

   Important
   Do **not** install Network Agent on a machine running a firewall. Network Agent uses packet capturing that may conflict with the firewall software.

3. If you receive an error during installation regarding the **/etc/hosts** file, use the following information to correct the problem.

   Make sure the **hosts** file contains a hostname entry for the machine, in addition to the loopback address. (Use the **hostname -f** command to check this.)

   To configure a hostname:

   a. Enter the following command:

      ```
      hostname <host>
      ```

   b. Update the HOSTNAME entry in the **/etc/sysconfig/network** file:

      ```
      HOSTNAME=<host>
      ```

   c. In the **/etc/hosts** file, specify the IP address to associate with the hostname. This should be static, and not served by DHCP. Do not delete the second line in the file (the IPv4 loopback address) or the third line in the file (the IPv6 loopback address).

```
<IP address>    <FQDN>                    <host>
127.0.0.1       localhost.localdomain     localhost
::1             localhost6.localdomain6   localhost6
```

Here, <FQDN> is the fully-qualified domain name of this machine (i.e., <host>.<subdomains>.<top-level domain>)—for example, myhost.example.com—and <host> is the name assigned to the machine.

Important

The hostname entry you create in the **hosts** file must be the first entry in the file.

4. Your web protection software supports only TCP/IP-based networks. If your network uses both TCP/IP- and non-IP-based network protocols, only users in the TCP/IP portion of the network are filtered.
5. Make sure the following are installed.
   - haveged service

     Make sure this service is running.
   - xorg-x11-fonts-Type1
   - dejavu-serif-fonts

   The installer will check for these and display a message with instructions on how to install if any are not found.
6. Copy the Web Security Linux installer (**Web85xSetup_Lnx.tar.gz**) to the machine:
   a. Log on to the installation machine with full administrative privileges (typically, **root**) and create a setup directory for the installer files. For example:

      ```
      /root/Websense_setup
      ```

   b. Find the installer on the Downloads tab of the My Account page at forcepoint.com. You can download the installer to your network, then copy it to each Linux server that will host Forcepoint components.
   c. Enter the following to uncompress and extract files:

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

Prepare for appliance installation

Refer to the Firstboot Wizard section of the Forcepoint Appliances Getting Started Guide and gather information as instructed under “Gather data for firstboot”.

Step 2: Start the management server installation

In a typical installation, the management server machine hosts Forcepoint Security Manager components, Policy Broker, and Policy Server.

To begin the installation process:

1. Log on to the machine.
2. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. After a few seconds, a progress dialog box appears, as files are extracted.
3. On the Welcome screen, click **Start**.
4. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
5. On the Installation Type screen, select **Forcepoint Security Manager**, then mark the **Forcepoint Web Security or Forcepoint URL Filtering** check box and click **Next**.

   After installation, when you enter your subscription key, the correct features for your product will be enabled.

   On the second Installation Type screen, select **Use the SQL Server database installed on another machine** and click **Next**.
6. On the **Summary** screen, click **Next** to continue the installation.

   Forcepoint Management Infrastructure Setup launches.

Step 3: Install the Forcepoint Management Infrastructure

The Forcepoint Management Infrastructure includes data storage and common components for the Forcepoint Security Manager.

1. On the Forcepoint Management Infrastructure Setup Welcome screen, click **Next**.
2. On the Installation Directory screen, specify the location where you want Forcepoint Management Infrastructure to be installed and then click **Next**.
   - To accept the default location (recommended), simply click **Next**.
   - To specify a different location, click **Browse**.

   

   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 and connection credentials for a database server located elsewhere in the network.
   a. Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any, and the **Port** to use for SQL Server communication.
      - 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.

   b. Specify whether to use **SQL Server Authentication** (a SQL Server account) or **Windows Authentication** (a Windows trusted connection), then provide the **User Name** or **Account** and its **Password**.

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

c. 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, the following message appears:

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

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

4. On the Server & Credentials screen, do the following:

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

Administrators will use this address to access the console (via a web browser), and web protection components on other machines will use the address to connect to the management server.

b. Specify the **Server or domain** of the user account to be used by Forcepoint Management Infrastructure and the Forcepoint Security Manager. The name cannot exceed 15 characters.

c. Specify the **User name** of the account to be used by the Security Manager.

d. Enter the **Password** for the specified account.

5. On the **Administrator Account** screen, enter an email address and password for the default Security Manager administration account: **admin**. When you are finished, click **Next**.

- The Administrator password must be a minimum of 8 characters, with at least 1 each of the following: upper case letter, lower case letter, number, special character.
- System notification and password reset information is sent to the email address specified (once SMTP configuration is done; see next step).

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

Important

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

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

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

   The Installation screen appears, showing installation progress. Wait until all files have been installed.

   If the following message appears, check to see if port 9443 is already in use on this machine:

   Error 1920. Server '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.

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

   You are returned to the Installer Dashboard and, after a few seconds, the Web Protection Solutions setup program launches.

Step 4: Install Web management components

In a typical deployment, all management components, the standalone or primary Policy Broker, and the central Policy Server reside on a Windows server called the management server.

1. On the Select Components screen, select:
   - Forcepoint Security Manager (Web module) (selected by default)
   - Real-Time Monitor
   - Policy Broker and Policy Server
2. Still on the Select Components screen, **clear** the check box next to **Linking Service**, then click **Next**.

   If this service is required in your deployment, it will be installed in a later step, when all component dependencies have been met.
3. On the Policy Broker Replication screen, indicate which Policy Broker mode to use.
   - Select **Standalone** if this will be the only Policy Broker instance in your deployment.
   - Select **Primary**, then create a **Synchronization password** if you will later install additional, replica instances of Policy Broker.

The password may include between 4 and 300 alphanumeric characters.

Important

If you are installing the primary Policy Broker, be sure to record the synchronization password. You must provide this password each time you create a Policy Broker replica.

- Do **not** select Replica at this stage. You must install a standalone or primary Policy Broker before you can install a replica.

If you are not sure about which Policy Broker mode to choose, see Managing Policy Broker Replication.

4. If the management server machine does not include a supported version of the Microsoft SQL Server Native Client and related tools, you are prompted to install the required components. Follow the on-screen prompts to complete this process.
5. On the Pre-Installation Summary screen, verify the installation path, selected components, and other information, then click or select **Next**.

   A progress screen is displayed while components are installed.
6. On the Installation Complete screen, click **Next**.

Continue with the next section to install an instance of Filtering Service that connects to your management server components.

Step 5: Install an instance of Filtering Service

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

This instance of Filtering Service may reside:

- On a supported Windows server (see *Installing Filtering Service on Windows*)
- On a supported Linux server (see *Installing Filtering Service on Linux*)
- On a **filtering only** appliance (see *Using a filtering only appliance*)

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

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

Installing Filtering Service on Windows

Before installing Filtering Service on a supported Windows server, make sure you have prepared the machine (including downloading the installer file) as described in *Prepare your Windows servers*, page 3.

To install Filtering Service:

1. Log on to the machine.
2. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. After a few seconds, a progress dialog box appears, as files are extracted.
3. On the Welcome screen, click **Start**.
4. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
5. On the Installation Type screen, select **Custom** and then click **Next**.
6. On the Summary screen, click **Next**.
7. On the Custom Installation screen, click the **Install** link next to **Forcepoint Web Security or URL Filtering**.
8. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
9. Accept the subscription agreement, then click **Next**.
10. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that software components should use for communication, then click **Next**.
11. Select the **Custom** installation type, then click **Next**.
12. On the Select Components screen, select the following components, then click **Next**:
    - Filtering Service
    - User Service
    - Usage Monitor

    Optionally, you may also select:
    - Network Agent
    - State Server
    - DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent
13. On the Policy Server Connection screen, enter the IP address of the Policy Server for this Filtering Service, and the Policy Server communication port (55806, by default), then click **Next**.
14. On the Active Directory screen, indicate whether you are using Windows Active Directory to authenticate users in your network, then click **Next**.
15. On the Computer Browser screen, indicate that the installer should attempt to start the service, then click **Next**.
16. On the Integration Option screen, make a selection as described below, then click **Next**:

- If you intend to integrate your product with a third-party proxy, firewall, or similar product, select **Install Forcepoint URL Filtering to integrate with a third-party product or device**.
- To use Network Agent to monitor Internet activity and enable policy enforcement, select **Install Forcepoint Web Security or URL Filtering in standalone mode**.

See Understanding standalone and integrated modes for web protection solutions if you aren't sure which option to pick.

17. If you selected the Integrated option, on the Select Integration screen, select your integration product or method, then click **Next**.
18. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other components, then click **Next**.
19. On the Feedback screen, indicate whether you want your web protection software to send feedback to Forcepoint LLC, then click **Next**.
20. On the Directory Service Access screen, enter the domain, user name, and password of an account that is a member of the Domain Admins group on the domain controller, then click **Next**.

    User Service, DC Agent, and Logon Agent use this information to query the domain controller for user and group information.
21. On the Installation Directory screen, accept the default installation path, or click or select **Choose** to specify another path, and then click **Next**.

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

    The installer creates this directory if it does not exist.

    Important
    The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.
22. On the Pre-Installation Summary screen, verify the installation path, selected components, and other information, then click **Next**.

    A progress screen is displayed while components are installed.
23. When the installation process finishes, the Installation Complete screen is displayed. Click **Next** to exit the installer.

Continue with *Step 6: Install Log Server*, page 14.

Installing Filtering Service on Linux

Before installing Filtering Service on a supported Linux server, make sure you have prepared the machine (including downloading the installer file) as described in *Prepare your Linux servers*, page 4.

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

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

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

```
./install.sh
```

2. On the Introduction screen, click or select **Next**.
3. On the Subscription Agreement screen, choose to accept the terms of the agreement and then click or select **Next**.
4. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that software components should use for communication.
5. On the Installation Type screen, select **Custom** and then click or select **Next**.
6. On the Select Components screen, select the following components, then click or select **Next**:
   - Filtering Service
   - User Service
   - Usage Monitor

   Optionally, you may also select Network Agent, State Server, Logon Agent, eDirectory Agent, or RADIUS Agent.
7. On the Policy Server Connection screen, enter the IP address of the Policy Server for this Filtering Service, and the Policy Server communication port (55806, by default).
8. On the Integration Option screen, make a selection as described below, then click or select **Next**:
   - To integrate your product with a third-party proxy, firewall, or similar product, select **Install Forcepoint URL Filtering to integrate with a third-party product or device**.
   - To use Network Agent to monitor Internet activity and enable policy enforcement, select **Install Forcepoint Web Security or URL Filtering in standalone mode**.

   See Understanding standalone and integrated modes for web protection solutions if you aren't sure which option to pick.
9. If you selected the Integrated option, on the Select Integration screen, select your integration product or method, then click or select **Next**.
10. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other components, then click or select **Next**.
11. On the Feedback screen, indicate whether you want your web protection software to send feedback to Forcepoint LLC, then click or select **Next**.
12. On the Installation Directory screen, accept the default installation path (/opt/Websense/), or click or select **Choose** to specify another path. The installation path:
    - Must be absolute (not relative)

- Must use only ASCII characters (no extended ASCII or double-byte characters)

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

The installer creates the installation directory if it does not exist and compares the installation's system requirements with the machine's resources.

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

13. On the Pre-Installation Summary screen, verify the installation path, selected components, and other information, then click or select **Next**.

    A progress screen is displayed while components are installed.

> **Note**
> Do **not** click the Cancel button (GUI) or press Ctrl-C (command-line) after the **Pre-Installation Summary**, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

14. On the Installation Complete screen, click or select **Done**. (In the graphical installer, be careful not to click Cancel.)

Continue with *Step 6: Install Log Server*, page 14.

Using a filtering only appliance

The instructions that follow assume that you have already followed the instructions provided in *Prepare for appliance installation*, page 5.

Follow the instructions found in the "Run firstboot" section of the Forcepoint Appliances Getting Started Guide, selecting **Forcepoint URL Filtering** as your security mode.

After the firstboot script has completed, a command-line interface (CLI) logon prompt displays. Log on to perform post-firstboot configuration, including configuring network interfaces. See Forcepoint Appliances Getting Started for details.

> **Note**
> It is not possible to rerun the firstboot script. However, all of the settings established during firstboot, except the security mode, can be changed in the CLI. See the Forcepoint Appliances CLI Guide.
>
> Changing the security mode requires re-imaging the appliance.

Step 6: Install Log Server

Log Server enables most reporting components, and must reside on a Windows machine.

Before installing Log Server on a supported Windows server, make sure you have prepared the machine (including downloading the installer file) as described in *Prepare your Windows servers*, page 3.

To install Log Server:

1. Log on to the machine.
2. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. After a few seconds, a progress dialog box appears, as files are extracted.
3. On the Welcome screen, click **Start**.
4. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
5. On the Installation Type screen, select **Custom** and then click **Next**.
6. On the Summary screen, click **Next.**
7. On the Custom Installation screen, click the **Install** link next to **Forcepoint Web Security or URL Filtering**.
8. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
9. Accept the subscription agreement, then click **Next**.
10. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that software components should use for communication, and then click **Next**.
11. Select the **Custom** installation type, then click **Next**.
12. On the Select Components screen, select **Log Server**, then click **Next**:
13. On the Policy Server Connection screen, enter the IP address of the Policy Server for this Log Server, and the Policy Server communication port (55806, by default), and then click **Next**.
14. If the Log Server machine does not include a supported version of the Microsoft SQL Server Native Client and related tools, you are prompted to install the required components. Follow the on-screen prompts to complete this process.
15. On the Database Information screen, enter the hostname or IP address of the machine on which a supported database engine is running. If you are using SQL Server clustering, enter the virtual IP address of the cluster. Also indicate how to connect to the database engine:
    - Select **Trusted connection** to use a Windows account to connect to the database. Enter the user name and password of a trusted account with local administration privileges on the database machine. Note that the trusted account you specify here should be the same as that with which you logged onto this machine before starting the installer.

If you use a trusted account, an additional configuration step is required after installation to ensure that reporting data can be displayed in the Forcepoint Security Manager. See the Reporting FAQ.

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

Note that some fields may be pre-filled on this screen. Be sure to replace the pre-filled content with correct connection information for your deployment.

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

    The default location is **C:\Program Files\Microsoft SQL Server** on the SQL Server machine.

    Note that if you specify a custom directory, that directory must already exist. The installer cannot create a new directory on the SQL Server machine.

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

    - (Recommended) **Log Web page visits**: Enable this option to log fewer records that combine hits and bandwidth data for a requested website, rather than a logging a separate record for each file included in the request. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities.
    - **Consolidate requests**: Enable this option to combine Internet requests that share the same value for all of the following elements, within a certain interval of time (1 minute, by default):
      - Domain name (for example: www.forcepoint.com)
      - Category
      - Keyword
      - Action (for example: Category Blocked)
      - User/workstation

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

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

    The installer creates this directory if it does not exist.

    

    Important

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

19. On the Pre-Installation Summary screen, verify the installation path, components selected, and other information shown, then click **Next**.

    A progress screen is displayed while components are installed.

20. When the installation process finishes, the Installation Complete screen is displayed. Click **Next** to exit the installer.
21. After installing Log Server, restart the following services on the management server machine:
    - Websense TRITON - Web Security
    - Websense Web Reporting Tools

    This step is required to ensure that reporting tools operate properly, and that any scheduled reports that you create are saved properly.

To install additional policy enforcement and user identification components, continue with *Step 7: Install additional components*, page 16.

To install the Citrix or Microsoft Forefront TMG plug-in, continue with *Step 8: Install Integration Plug-in (if applicable)*, page 20.

If you are done installing components, continue with *Step 10: Initial Configuration*, page 27.

Step 7: Install additional components

Depending on your network configuration and size, you may need to install multiple instances of several policy enforcement and user identification components.

- All Forcepoint URL Filtering components can reside on Windows servers (see *Installing components on Windows*, page 16).
- Most components can reside on Linux servers (see *Installing components on Linux*, page 18).
- Most components can reside on appliances in the following configurations:
    - **User directory and filtering appliances** include Policy Server, plus Filtering Service, User Service, Usage Monitor, and Network Agent. During setup, you are prompted to connect to Policy Broker (which typically resides on the management server).
    - **Filtering only** appliances host Filtering Service and Network Agent. During setup, you are prompted to connect to a Policy Server instance (which may reside on a user directory and filtering appliance, or a Windows or Linux server).

    See *Installing components on appliances*, page 19.

Installing components on Windows

Before installing components on a supported Windows server, make sure you have prepared the machine (including downloading the installer file) as described in *Prepare your Windows servers*, page 3.

To install the components:

1. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer. After a few seconds, a progress dialog box appears, as files are extracted.
2. On the Welcome screen, click **Start**.
3. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
4. On the Installation Type screen, select **Custom** and then click **Next**.
5. On the Summary screen, click **Next.**
6. On the Custom Installation screen, click the **Install** link next to **Forcepoint Web Security or URL Filtering.**
7. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
8. Accept the subscription agreement, then click **Next**.
9. Select the **Custom** installation type, then click **Next**.
10. Select the components that you want to install, keeping in mind that:
    - Policy Server must always be installed before or with its dependent components.

      You **will** be prompted to provide the Policy Server IP address during installation of most components if Policy Server resides on a different machine.
    - Filtering Service must always be installed before or with dependent instances of Network Agent.

      You will be prompted for the Filtering Service IP address during Network Agent installation if Filtering Service resides on another machine.
    - Unlike the primary or standalone Policy Broker, which must always be installed first, replica Policy Brokers may be added at any time.

      You can configure which Policy Broker instance any Policy Server (and its dependent components) connects to after installation (use the **Web > Settings > General > Policy Brokers** page in the Forcepoint Security Manager).
11. Click **Next** to configure your installation.

    Many of the screens that display depend on which components you have selected. If you are not clear about what information to provide, click **Help** in the installer for context and instructions.
12. On the Installation Directory screen, accept the default installation path, or click or select **Choose** to specify another path, and then click **Next**.

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

    The installer creates this directory if it does not exist.

Important

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

13. On the Pre-Installation Summary screen, verify the installation path, selected components, and other information, then click or select **Next**.

    A progress screen is displayed while components are installed.

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

Repeat the steps in this section for any additional components that you want to install.

When you are finished, do one of the following:

- If your product will integrate with Citrix or Microsoft Forefront TMG, continue with *Step 8: Install Integration Plug-in (if applicable)*, page 20.
- If you are finished installing components, see *Step 10: Initial Configuration*, page 27.

Installing components on Linux

Before installing Filtering Service on a supported Linux server, make sure you have prepared the machine (including downloading the installer file) as described in *Prepare your Linux servers*, page 4.

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

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

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

   ```
   ./install.sh
   ```

2. On the Introduction screen, click or select **Next**.
3. On the Subscription Agreement screen, choose to accept the terms of the agreement and then click **Next**.
4. On the Installation Type screen, select **Custom** and then click or select **Next**.
5. On the Select Components screen, select the components that you want to install:
   - Policy Server must always be installed before or with its dependent components.

     You **will** be prompted to provide the Policy Server IP address during installation of most components if Policy Server resides on a different machine.
   - Filtering Service must always be installed before or with dependent instances of Network Agent.

     You will be prompted for the Filtering Service IP address during Network Agent installation if Filtering Service resides on another machine.
   - Unlike the primary or standalone Policy Broker, which must always be installed first, replica Policy Brokers may be added at any time.

     You can configure which Policy Broker instance any Policy Server (and its dependent components) connects to after installation (use the **Settings** > **General** > **Policy Brokers** page in the Forcepoint Security Manager).

6. Click or select **Next** to configure your installation.

   Many of the screens that display depend on which components you have selected. If you are not clear about what information to provide, click or select **Help** in the installer for context and instructions.

7. On the Installation Directory screen, accept the default installation path (/opt/Websense/), or click or select **Choose** to specify another path. The installation path:

   - Must be absolute (not relative)
   - Must use only ASCII characters (no extended ASCII or double-byte characters)

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

   The installer creates the installation directory if it does not exist and compares the installation's system requirements with the machine's resources.

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

8. On the Pre-Installation Summary screen, verify the installation path, selected components, and other information, then click or select **Next**.

   A progress screen is displayed while components are installed.

   

   Note

   Do **not** click the Cancel button (GUI) or press Ctrl-C (command-line) after the **Pre-Installation Summary**, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

9. On the Installation Complete screen, click or select **Done**. (In the graphical installer, be careful not to click Cancel.)

Repeat the steps in this section for any additional components that you want to install.

When you are finished, do one of the following:

- If your product will integrate with Citrix or Microsoft Forefront TMG, continue with *Step 8: Install Integration Plug-in (if applicable)*, page 20.
- If you are finished installing components, see *Step 10: Initial Configuration*, page 27.

Installing components on appliances

The instructions that follow assume that you have already followed the instructions provided in *Prepare for appliance installation*, page 5.

Follow the instructions found in the "Run firstboot" section of the Forcepoint Appliances Getting Started Guide.

After the firstboot script has completed, a command-line interface (CLI) logon prompt displays. Log on to perform post-firstboot configuration, including configuring network interfaces. See Forcepoint Appliances Getting Started for details.

Note

It is not possible to rerun the firstboot script. However, all of the settings established during firstboot, except the security mode, can be changed in the CLI. See the Forcepoint Appliances CLI Guide.

Changing the security mode requires re-imaging the appliance.

Repeat the steps in this section for any additional components that you want to install.

When you are finished, do one of the following:

- If your product will integrate with Citrix or Microsoft Forefront TMG, continue with *Step 8: Install Integration Plug-in (if applicable)*, page 20.
- If you are finished installing components, see *Step 10: Initial Configuration*, page 27.

Step 8: Install Integration Plug-in (if applicable)

If you have configured Filtering Service to integrate with Citrix, or with Microsoft Forefront TMG, an additional component must be installed to enable the integration.

See:

- *Install the Citrix Integration Service*, page 20
- *Install the ISAPI Filter plug-in for Microsoft Forefront TMG*, page 24

Install the Citrix Integration Service

Obtain the Citrix configuration package

Everything you need to configure and install Citrix Integration Service is contained in a self-extracting archive (the Citrix configuration package) on the management server or Log Server machine. It can be found in the following directory:

C:\Program Files *or* Program Files (x86)\Websense\Web Security\Citrix Plugin\

Note that there are separate 32-bit and 64-bit configuration packages. Select the appropriate one for the **target** operating system (the Citrix server operating system).

You can copy the configuration package to any machine to create your Citrix Integration Service installer.

Configure the Citrix Integration Service installer

Extract the contents of the Citrix configuration package and run the configuration utility to create a Citrix Integration Service installer to deploy to Citrix servers.

1. Double-click the configuration package executable, then click **Extract**. The package name is either:
   - WCISUtil_Win32_*nnnn*.exe (32-bit)
   - WCISUtil_x64_*nnnn*.exe (64-bit)
2. Double-click **Forcepoint Citrix Integration Service Configuration.exe** to start the configuration utility.

   Important
   The 32- and 64-bit versions of the configuration utility have the same name. Make sure you are launching the correct version.

3. In the **Profile Source** screen, click **Browse** and select the folder containing either the default Citrix installation package template or an existing installation package that you want to modify, then click **Next**.

   If the following message appears, make sure all necessary files are present in the folder you specified:

   ```
   The selected installation package does not include all of
   the necessary files.
   ```

   The folder you specify must contain all of the files extracted from the Citrix configuration package in step 1.
4. In the **Connections** screen, configure Filtering Service connection behavior for Citrix Integration Service as described below. When you are finished, click **Next**.
   a. If **127.0.0.1:15868** appears, select it and then click **Remove**.

      Filtering Service should never be installed on the Citrix server machine itself.

   b. Under **Connection Details**, enter the IP address or hostname of a Filtering Service machine, then enter the connection port (15868 by default).

      Note
      To determine which port is being used, check the **WebsenseServerPort** value in the **eimserver.ini** file on the Filtering Service machine. The file is located in the product's **bin** directory (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/, by default).

      Important: Do not modify the **eimserver.ini** file.

c. Click the right arrow (>) to add the IP address/hostname and port entry.

d. Repeat the previous 2 steps for each Filtering Service instance you want used by the Citrix server.

When multiple Filtering Service instances are specified, if the first instance is unavailable, Citrix Integration Service attempts communication with the next instance in the list.

If no Filtering Service instances are available, Citrix Integration Service continues to attempt communication in the background every 1 minute. Until communication is established, Citrix Integration Service fails open (permits all requests) or fails closed (blocks all requests) depending on your select in **step f** (below).

Note

If State Server is not installed, each Filtering Service instance tracks continue, quota, and password override information separately. If the Citrix Integration Service fails over from one Filtering Service to another, users may receive an unexpected quota, confirm, or password override prompt, and could receive extra quota time.

e. Mark or clear **Do not send user name information to Filtering Service**. If this option is selected (enabled), user name information for Citrix users is not included in reports.

The setting applies to all Filtering Service instances listed.

f. Mark or clear **Block all HTTP/HTTPS/FTP traffic if unable to connect to a Filtering Server** to specify whether Citrix Integration Service blocks or permits all requests when it cannot communicate with Filtering Service.

5. Use the **Client Settings** to set notification and anti-tampering options, then click **Next**.

- Use **Notify users when HTTPS or FTP traffic is blocked** to determine whether users see a browser pop-up message when HTTPS or FTP traffic is blocked. If so, also specify the how long the pop-up message remains visible.
- Use **Protect installation directory from modification or deletion** to prevent tampering with the Citrix Integration Service on the Citrix server. Attempts to delete it, replace files, or modify registry entries are stopped.

6. On the **Trusted Sites** screen, specify any URLs or domains that should be ignored (not forwarded for policy enforcement). When you are finished, click **Next**.

- To add a URL or regular expression, click **Add**, then enter either a URL or a regular expression specifying a set of URLs. Any regular expression adhering to ISO/IEC TR 19768 (within the character-number limit) is valid. When you are finished, click **OK**.
- To edit a URL or regular expression, select it and then click **Edit**.
- To remove a URL or regular expression, select it and then click **Remove**.

These URLs are trusted by any Citrix server on which this Citrix Integration Service configuration is installed. It has no bearing on how Filtering Service

responds to requests from non-Citrix users, and does not affect Citrix servers that use a different Citrix Integration Service configuration.

7. On the **Save** screen, specify how you want the customized installation package saved. When you are finished, click **Finish**.
   - Select **Overwrite the existing installation** to overwrite the Citrix installation package you used as a template.
   - Select **Save the customized installation package to a new location** to save the customized installation package to a different location. Click **Browse**, and specify a folder. It is a best practice to save to an empty folder. Then, you can be certain that all files in that folder are part of the installation package.

The installation package is now ready for use.

If you have multiple Citrix servers for which you want different customized settings, repeat this procedure to create an installation package for each. Save each customized installation package to a different folder.

Install the Citrix Integration Service on the Citrix server

A Citrix installation package includes the following files:

• 0x0409.ini	• CI.cab
• CIClientConfig.hsw	• CIClientMessage.hsw
• DLP.cab	• GClientConfig.hsw
• setup.exe	• Setup.ini
• Websense Citrix Integration Service.msi	• WEP.cab

All of the files must be present to install Citrix Integration Service.

Use the same Citrix installation package for all Citrix servers that will share a Citrix Integration Service configuration.

On each Citrix Server:

1. Log on to the server with **local** administrator privileges.
2. Close all applications and stop any antivirus software.
3. Copy the Citrix installation package (all files listed above) to the Citrix server. Keep the files in the same folder.

   If you installed the Citrix configuration package to the Citrix server itself, and customized the installation package there, skip this step.
4. Double-click **setup.exe** to start the Citrix Integration Service installer. It may take a few seconds for the program to begin to run.

   When the Welcome screen appears, click **Next**.
5. Accept the subscription agreement, then click **Next**.
6. On the **Destination Folder** screen, accept the default location shown or click **Change** to choose a different location, then click **Next**.

7. On the **Ready to Install the Program** screen, click **Install** to install the Citrix Integration Service.
8. Wait until the **InstallShield Wizard Completed** screen appears, then click **Finish**.
9. If you stopped your antivirus software, be sure to start it again.

When you have installed the Citrix Integration Service on all of your Citrix servers, continue with either *Install the ISAPI Filter plug-in for Microsoft Forefront TMG*, page 24 (if applicable) or *Step 10: Initial Configuration*, page 27.

Install the ISAPI Filter plug-in for Microsoft Forefront TMG

To enable integration with Microsoft Forefront TMG, use the Forcepoint Security Installer to install the ISAPI Filter plug-in on the TMG machine.

The only web protection components installed on the Forefront TMG machine are the ISAPI Filter plug-in and Control Service (which manages installation and removal of web protection software components).

Important

- As part of the installation process, you must stop the Microsoft Forefront TMG Firewall service (Firewall service). Because this may stop network traffic, perform the installation during a time when a stoppage will least affect your organization. Do not stop the Firewall service until prompted by the installer.
- Port 55933 (the Control Service communication port) must be open locally for the ISAPI Filter plug-in to be installed successfully.

Before beginning the installation process:

- Copy the Forcepoint Security Installer (**Forcepoint85xSetup.exe**) to the TMG machine.
- Close all applications and stop any antivirus software.

To perform the installation:

1. Log on to the machine.
2. Use the **Run as administrator** option to launch the **Forcepoint85xSetup.exe** installer.. After a few seconds, a progress dialog box appears, as files are extracted.
3. On the Welcome screen, click **Start**.
4. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
5. On the Installation Type screen, select **Custom** and then click **Next**.
6. On the Summary screen, click **Next.**

7. On the Custom Installation screen, click the **Install** link next to **Forcepoint Web Security or URL Filtering**.
8. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
9. Accept the subscription agreement, then click **Next**.
10. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that software components should use for communication, then click **Next**.
11. Select the **Custom** installation type, then click **Next**.
12. On the Select Components screen, select **Filtering Plug-in**, then click **Next**.
13. On the **Filtering Service Communication** screen, enter the IP address of the machine on which Filtering Service is installed and the port Filtering Service uses to communicate with integration products and Network Agent (default is 15868). Then click **Next**.
    - The port used by Filtering Service to communicate with integration products and Network Agent must be in the range 1024-65535.
    - To verify the Filtering Service port, check the **WebsenseServerPort** value in the **eimserver.ini** file, located in the **bin** directory on the Filtering Service machine.
14. On the **Select Integration** screen, select **Microsoft Forefront Threat Management Gateway** and click **Next**.
15. On the **Installation Directory** screen, accept the default location and click **Next**.
16. On the **Pre-Installation Summary** screen, verify that **Filtering Plug-in** is the only component selected for installation, then click **Install**.

    An **Installing** progress screen is displayed. Wait for the installation to complete.
17. When the **Stop Microsoft Forefront TMG Firewall Service** screen appears, stop the Microsoft Forefront TMG Firewall service (Firewall service) and then click **Next**.

    

    Note

    Leave the installer running as you stop the Firewall service, and then return to the installer to continue installation.

    To stop the Firewall service, open the Windows Services tool and right-click **Microsoft Forefront TMG Firewall**, then select **Stop**. When the service has stopped, return to the installer and continue the installation process. The Firewall

service may also be stopped from the Forefront TMG management console. See the Microsoft documentation for more information.

Important
When the Firewall service is stopped, Forefront TMG goes into lockdown mode. Network traffic may be stopped. Typically, the Firewall service must be stopped for only a few minutes.

18. When the following message appears, start the Firewall service and click **OK**:

```
The ISAPI Filter has been configured, you can now start
the Microsoft Firewall Service.
```

Note
Leave the installer running as you start the Firewall service, and then return to the installer to continue installation.

To start the Firewall service, go to the Windows Services tool and right-click **Microsoft Forefront TMG Firewall**, then click **Start**.

19. On the **Installation Complete** screen, click **Next**.
20. If you stopped antivirus software on this machine, restart it now.

To verify that the ISAPI Filter plug-in installed correctly, log in to the Forefront TMG management console. Navigate to **System** > **Web Filters** and verify that **WsISAFilter** is present in the list of filters.

Continue with *Step 10: Initial Configuration*.

Step 9: Post installation activities

After you have finished installing components, refer to the following to ensure that your Web Security installation is complete.

- If multiple Policy Servers were installed and assigned to the same Policy Broker, and any of them reside on a Microsoft Windows 2016 server, some of the services on all of the Windows 2016 machines in the deployment may fail to restart at the end of the install process.

  Log on to each machine and restart the following services as needed:

  - Websense Event Message Broker
  - Websense Cloud App Service
  - Websense Bridge Service
  - Websense SIEM Connector

  Optionally, reboot each machine.

Step 10: Initial Configuration

Tip

All Forcepoint URL Filtering tools and utilities installed on Windows Server platforms (such as wsbackup.exe and websenseping.exe), as well as text editors used to modify configuration files (such as websense.ini), **must** be run as the local administrator. Otherwise, you may be prevented from running the tool or the changes you make may not be implemented.

After installation is complete, log on to the Forcepoint Security Manager (console) and enter your subscription key. Entering the key:

- Allows your product to be verified
- Initiates database downloads that activate your solution
- Enables several management console features.

To get started:

1. If administrators use Internet Explorer to access the console, make sure that Enhanced Security Configuration (IE ESC) is disabled on their machines.
2. Use a supported browser to launch the console and log on using the default account (**admin**) and the password created during installation.

   The console URL is:

   ```
   https://<IP_address>:9443/triton/
   ```

   Here, <*IP_address*> is the IP address of the management server.
3. Enter your subscription key. At first startup, you are prompted for a subscription key in the Initial Setup Checklist.
4. If you did not provide SMTP server details during installation, use the **GLOBAL SETTINGS > Notifications** page to specify the SMTP server used to enable administrator password reset functionality and account change notifications.
5. Use the Initial Setup Checklist to start configuring your system.