

Installation Instructions: Web Filter & Security

Installation Instructions | Web Filter & Security | Version 8.3.x

Use the steps to complete a typical installation of Web Filter & Security. In this configuration:

- The policy source (the standalone or primary Policy Broker and its Policy Server) resides on the TRITON management server machine.
- Log Server resides on a dedicated Windows server.
- The reporting databases are hosted on a full version (not Express) of Microsoft SQL Server 2008 R2, 2012, 2014, or 2016 with the latest service pack from Microsoft.

An end user who uses the Filtering Service has no direct or indirect influence over the database. Thus, although the log entry is stored in the MSSQL database, the user did not direct its storage and cannot retrieve it.

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

This installation procedure includes the following steps:

- [Step 1: Prepare for installation, page 2](#)
- [Step 2: Prepare the management server, page 2](#)
- [Step 3: Select management server components, page 4](#)
- [Step 4: Install the TRITON infrastructure, page 4](#)
- [Step 5: Install Web management components, page 9](#)
- [Step 6: Install an instance of Filtering Service, page 10](#)
- [Step 7: Install Log Server, page 19](#)
- [Step 8: Install additional components, page 23](#)
- [Step 9: Install Integration Plug-in \(if applicable\), page 28](#)
- [Step 10: Initial Configuration, page 34](#)

Step 1: Prepare for installation

Make sure that a supported version of Microsoft SQL Server (not Express) is installed and running in your network, and that:

- 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.

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 Web Filter & Security with Cisco](#) for more information.
 - Citrix XenApp 5.0, 6.0, and 6.5
See [Integrating Web Filter & Security with Citrix](#) for more information.
 - Microsoft Forefront Threat Management Gateway (TMG)
See [Integrating Web Filter & Security with TMG](#) for more information.
 - Blue Coat appliances via ICAP
See [Integrating Web Filter & Security using ICAP Service](#) for more information.

Other third-party products are supported using the “universal integrations” option.

- See the [list of TRITON Security Alliance partners and the list of Vendor Alliance partners](#) for a list of supported vendors.
- See [Installing for Universal Integrations](#) for more information.
- Make sure that the integration product is installed and running before you begin.

Step 2: Prepare the management server

In a typical installation, the TRITON management server hosts management components, Policy Broker, and Policy Server.

1. On the Windows machine that will host the TRITON management server:

- a. 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.

- b. Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
- c. Verify that there is sufficient disk space to download the installer, extract temporary installation files, and install the management components on the Windows installation drive (typically C).
- d. Make sure that the appropriate version of .NET Framework is installed. Versions 3.5 and 4.5 are required.
 - o Windows Server 2008 R2: 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](#).
 - o 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 or later 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.](https://msdn.microsoft.com/en-us/library/5a4x27ek(v=vs.110).aspx#To_install_language_packs.))

- e. Synchronize the clocks on all machines (including appliances) where a web protection component will be installed. It is a good practice to point the machines to the same Network Time Protocol server.
- f. 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.
- g. Disable any firewall on the machine before starting the installer and then re-enable it after installation. Open ports as required by the web protection 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 TRITON Ports spreadsheet](#) for more information about ports.

- h. Disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation.
2. Log on to the machine with domain admin privileges.
 3. Use the Downloads tab of the [My Account](#) page at forcepoint.com to download the TRITON Unified Installer (**TRITON83xSetup.exe**).

Step 3: Select management server components

Use the TRITON Unified Installer to install components on the management server machine.

1. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
2. On the Welcome screen, click **Start**.
3. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
4. On the Installation Type screen, select **TRITON Manager**, then mark the **TRITON AP-WEB or Web Filter & Security** check box and click **Next**.

Although the option says “TRITON AP-WEB or Web Filter & Security,” the correct components for managing Web Filter & Security are installed. After installation, when you enter your subscription key, the correct features for your product will be displayed.

5. On the **Summary** screen, click **Next** to continue the installation.
TRITON Infrastructure Setup launches.

Step 4: Install the TRITON infrastructure

The TRITON infrastructure includes data storage and common components for the management modules of the TRITON console.

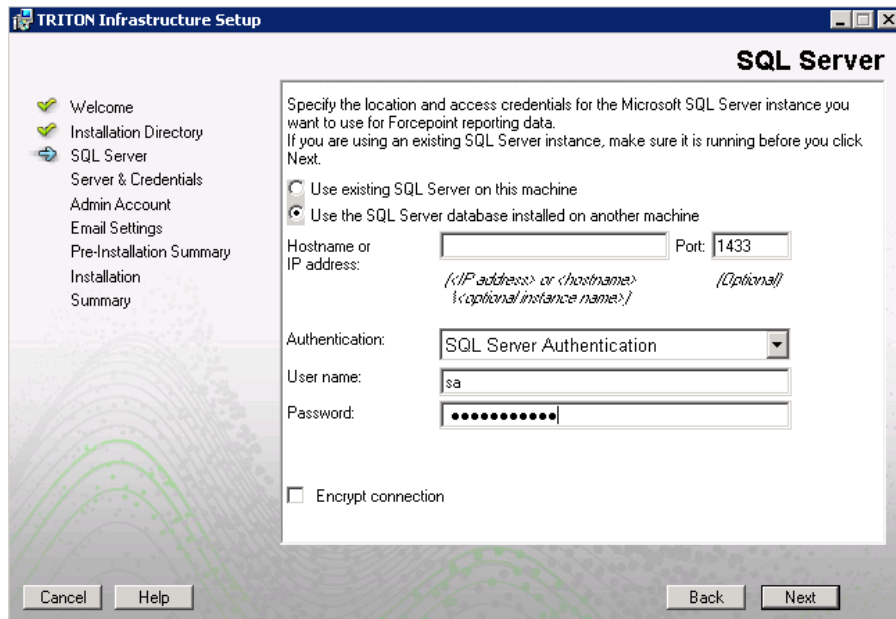
1. On the TRITON Infrastructure Setup Welcome screen, click **Next**.
2. On the Installation Directory screen, specify the location where you want TRITON Infrastructure to be installed and then click **Next**.
 - To accept the default location (recommended), simply click **Next**.
 - To specify a different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



Important

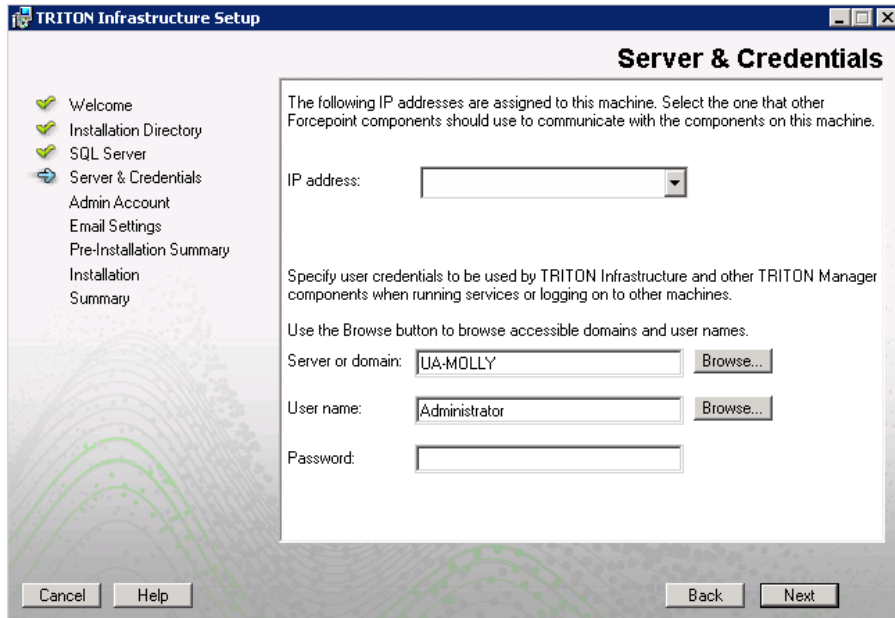
The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

3. On the SQL Server screen, select **Use the SQL Server database installed on another machine**, then specify the location and connection credentials for a database server located elsewhere in the network.



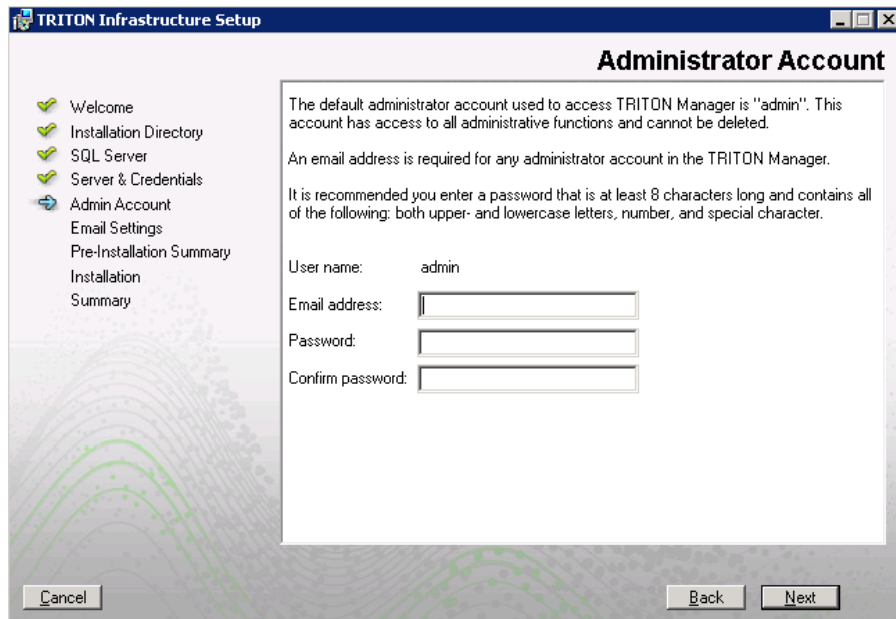
- a. Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any, and the **Port** to use for SQL Server communication.
If you are using a named instance, the instance must already exist.
If you are using SQL Server clustering, enter the virtual IP address of the 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 TRITON 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, select the IP address of this machine and specify network credentials to be used by TRITON Manager.



- 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 TRITON console (via a web browser), and web protection components on other machines will use the address to connect to the TRITON management server.
 - Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and TRITON Manager. The name cannot exceed 15 characters.
 - Specify the **User name** of the account to be used by TRITON Manager.
 - Enter the **Password** for the specified account.
5. On the **Administrator Account** screen, enter an email address and password for the default TRITON console 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.



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

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

It is a best practice to use a strong password as described on screen.

- 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 TRITON console.



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 TRITON console, the “Forgot my password” link on the logon page does not provide password recovery information. SMTP server configuration must be completed before password recovery email can be sent.

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

9. 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 5: Install Web management components

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

1. On the Select Components screen, select:
 - TRITON 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**.

This service is not used by Web Filter & Security.
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 information shown, then click **Next**.
6. A progress screen is displayed. Wait for installation to complete.
7. On the Installation Complete screen, click **Next**.

Step 6: Install an instance of Filtering Service

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

This instance of Filtering Service may reside:

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

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

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 TRITON management server machine.

Using a filtering only appliance

The instructions that follow assume that you have already set up your appliance hardware as directed on the in-box Quick Start poster for your appliance.

Gather the data

Gather the following information before running the firstboot configuration script. Some of this information may have been written down on the Quick Start poster during hardware setup.

Security mode	Web Filter & Security
Hostname (example: appliance.example.com) 1 - 60 characters long. The first character must be a letter. Allowed: letters, numbers, dashes, or periods. The name cannot end with a period.	

IP address for the appliance management network interface C	Must be an IPv4 address.
Subnet mask for network interface C	
Default gateway for network interface C (IP address) <i>Optional</i>	
NOTE: If you do not provide access to the Internet for interface C, use the Web module of the TRITON Manager to configure P1 to download Master Database updates from Forcepoint servers. See the Appliance Manager Help for information about configuring the interfaces. See the Web Filter & Security Administrator Help for information about configuring database downloads.	
Primary DNS server for network interface C (IP address)	
Secondary DNS server for network interface C (IP address) <i>Optional</i>	
Tertiary DNS server for network interface C (IP address) <i>Optional</i>	
Appliance manager password The password must be 8 to 15 characters and: <ul style="list-style-type: none"> ● Include at least <ul style="list-style-type: none"> ■ 1 uppercase character ■ 1 lowercase character ■ 1 number ■ 1 non-alphanumeric (special) character. ● Not include <ul style="list-style-type: none"> ■ The username, hostname, or name of a service or component ■ Any of the 3 previous passwords ■ Any of these special characters space \$: ` \ " 	
Integration method for this appliance (Choose one): <ul style="list-style-type: none"> ● Standalone (Network Agent only) ● Microsoft TMG ● Cisco ASA ● Citrix 	Choose your third-party integration product (if any).
Send usage statistics?	Usage statistics from appliance modules can optionally be sent to Forcepoint to help improve the accuracy of categorization.
Policy mode	Filtering only

Run the firstboot script

The initial command-line configuration script (**firstboot**) starts automatically when you power on the appliance for the first time.

1. Access the appliance console with the integrated DELL Remote Access Controller (iDRAC) Virtual Console, or by directly connecting a USB keyboard and monitor, or using a serial port connection.



Note

For serial port activation, use:

- 9600 baud rate
 - 8 data bits
 - no parity
-

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to start the **firstboot** configuration process.
4. At the next prompt, select **Web Filter & Security** as your security mode.
5. Follow the on-screen instructions to provide the information collected above.

After the firstboot script has completed, a command-line interface (CLI) logon prompt displays. Log on to perform post-firstboot configuration, including configuring additional network interfaces. See [TRITON 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 [TRITON Appliances CLI guide](#).

Changing the security mode requires re-imaging the appliance.

Installing Filtering Service on Windows

To install Filtering Service on a supported Windows platform:

1. On the Windows machine that will host the first instance of Filtering Service:
 - a. 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.

- b. Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
- c. Verify that there is sufficient disk space to download the installer, extract temporary installation files, and install the management components on the Windows installation drive (typically C).
- d. Make sure that the appropriate version of .NET Framework is installed. Versions 3.5 and 4.5 are required.
 - Windows Server 2008 R2: 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](https://msdn.microsoft.com/en-us/library/5a4x27ek(v=vs.110).aspx#To_install_language_packs)).

- e. Synchronize the clocks on all machines (including appliances) where a Forcepoint component will be installed. It is a good practice to point the machines to the same Network Time Protocol server.
- f. 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.
- g. Disable any firewall on the machine before starting the installer and then re-enable it after installation. Open ports as required by the web protection 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 TRITON Ports spreadsheet](#) for more information about ports.

- h. Disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation.
2. Log on to the machine with domain admin privileges.
3. Use the Downloads tab of the [My Account](#) page at forcepoint.com to download the TRITON Unified Installer (**TRITON83xSetup.exe**).
4. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
5. On the Welcome screen, click **Start**.
6. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
7. On the Installation Type screen, select **Custom** and then click **Next**.
8. On the Summary screen, click **Next**.
9. On the Custom Installation screen, click the **Install** link next to **TRITON AP-WEB or Web Filter & Security**.
10. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
11. Accept the subscription agreement, then click **Next**.
12. 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**.
13. Select the **Custom** installation type, then click **Next**.
14. On the Select Components screen, select the following components, then click **Next**:
 - Filtering Service
 - User Service
 - Usage MonitorOptionally, you may also select:
 - Network Agent
 - State Server
 - DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent
15. 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**.
16. On the Active Directory screen, indicate whether you are using Windows Active Directory to authenticate users in your network, then click **Next**.
17. On the Computer Browser screen, indicate that the installer should attempt to start the service, then click **Next**.
18. On the Integration Option screen, make a selection as described below, then click **Next**:

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

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

19. If you selected the Integrated option, on the Select Integration screen, select your integration product or method, then click **Next**.
20. 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**.
21. On the Feedback screen, indicate whether you want your web protection software to send feedback to Forcepoint LLC, then click **Next**.
22. 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.

23. 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.

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

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

25. A progress screen is displayed. Wait for the installation to complete.
26. On the Installation Complete screen, click **Next**.

Installing Filtering Service on Linux

Prepare the Linux server

To install Filtering Service on a supported Linux platform:

1. On the Linux machine that will host Filtering Service:

- a. If SELinux is enabled, disable it or set it to permissive.
- b. 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 TRITON 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.

- c. If you receive an error during installation regarding the `/etc/hosts` file, use this information to correct the problem.

Make sure the **hosts** file (by default, in `/etc`) contains a hostname entry for the machine, in addition to the loopback address. (Note: you can check whether a hostname has been specified in the **hosts** file by using the **hostname -f** command.) To configure hostname, first use the following command:

```
hostname <host>
```

Also update the HOSTNAME entry in the `/etc/sysconfig/network` file:

```
HOSTNAME=<host>
```

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 one that begins with 127.0.0.1 (the IPv4 loopback address). And do not delete the third line in the file, the one that begins `::1` (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.

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

```
/root/Websense_setup
```


4. Use the Downloads tab of the [My Account](#) page at forcepoint.com to download the web module Linux installer package. The installer package is called **Web83xSetup_Lnx.tar.gz**.

Place the installer archive in the setup directory you created.

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

```
tar -xvzf Web83xSetup_Lnx.tar
```

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

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

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

```
./install.sh
```

Use the graphical installer to install Filtering Service

1. On the Introduction screen, click or select **Next**.
2. On the Subscription Agreement screen, choose to accept the terms of the agreement and then click or select **Next**.
3. 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.
4. On the Installation Type screen, select **Custom** and then click or select **Next**.
5. On the Select Components screen, select the following components, then click or select **Next**:

- Filtering Service

- User Service

Note that if User Service is installed on Linux, and you use Windows Active Directory as your user directory, you must configure a WINS server to enable User Service to retrieve user and group information.

- Usage Monitor

Optionally, you may also select:

- Network Agent

- State Server

- Logon Agent, eDirectory Agent, or RADIUS Agent

6. 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).
7. On the Integration Option screen, make a selection as described below, then click **Next**:
 - To integrate your product with a third-party proxy, firewall, or similar product, select **Install Web Filter & Security to integrate with a third-party product or device**.

- To use Network Agent to monitor Internet activity and enable policy enforcement, select **Install TRITON AP-WEB or Web Filter & Security in standalone mode**.

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

8. If you selected the Integrated option, on the Select Integration screen, select your integration product or method, then click **Next**.
9. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other components, then click or select **Next**.
10. On the Feedback screen, indicate whether you want your web protection software to send feedback to Forcepoint LLC, then click or select **Next**.
11. On the Installation Directory screen, accept the default installation path, or click or select **Choose** to specify another path, and then click or select **Next**.

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

The installer creates this directory if it does not exist.



Important

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

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

- Insufficient disk space prompts an error message. The installer closes when you click or select **OK**.
 - Insufficient RAM prompts a warning message. The installation continues when you click or select **OK**. To ensure optimal performance, increase your memory to the recommended amount.
12. On the Pre-Installation Summary screen, verify the information shown, then click or select **Next**.

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

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



Note

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.)

Step 7: Install Log Server

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

1. On the Windows machine that will host Log Server:
 - a. 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.

- b. Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
- c. Verify that there is sufficient disk space to download the installer, extract temporary installation files, and install the management components on the Windows installation drive (typically C).
- d. Make sure that the appropriate version of .NET Framework is installed. Versions 3.5 and 4.5 are required.
 - Windows Server 2008 R2: 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 3.5 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.](https://msdn.microsoft.com/en-us/library/5a4x27ek(v=vs.110).aspx#To_install_language_packs.))

- e. 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.
- f. 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.
- g. 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 TRITON Ports spreadsheet](#) for more information about ports.

- h. Disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation.
2. Log on to the machine with domain admin privileges.
3. Use the Downloads tab of the [My Account](#) page at forcepoint.com to download the TRITON Unified Installer (**TRITON83xSetup.exe**).
4. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
5. On the Welcome screen, click **Start**.
6. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
7. On the Installation Type screen, select **Custom** and then click **Next**.
8. On the Summary screen, click **Next**.
9. On the Custom Installation screen, click the **Install** link next to **TRITON AP-WEB or Web Filter & Security**.
10. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
11. Accept the subscription agreement, then click **Next**.
12. 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**.
13. Select the **Custom** installation type, then click **Next**.
14. On the Select Components screen, select **Log Server**, then click **Next**:
15. 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**.
16. 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.
17. 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 Web module of the TRITON Manager. See [this section](#) of 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.

18. 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.

19. 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 one record (or a few records) with combined hits and bandwidth data for each requested website, rather than a record for each separate 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

20. 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.

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

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

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

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

24. After installing Log Server, restart the follow services on the TRITON 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.

Step 8: 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 Web Filter & Security components can reside on Windows servers.
- Most components can reside on Linux servers.
- 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 TRITON 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).

Installing components on appliances

The instructions that follow assume that you have already set up your appliance hardware as directed on the in-box Quick Start poster for your appliance.

Gather the data

Gather the following information before running the firstboot configuration script. Some of this information may have been written down on the Quick Start poster during hardware setup.

Security mode	Web Filter & Security
Hostname (example: appliance.example.com) 1 - 60 characters long. The first character must be a letter. Allowed: letters, numbers, dashes, or periods. The name cannot end with a period.	
IP address for the appliance management network interface C	Must be an IPv4 address.
Subnet mask for network interface C	

<p>Default gateway for network interface C (IP address) <i>Optional</i></p> <p>NOTE: If you do not provide access to the Internet for interface C, use the Web module of the TRITON Manager to configure P1 to download Master Database updates from Forcepoint servers. See the Appliance Manager Help for information about configuring the interfaces. See the Web Filter & Security Administrator Help for information about configuring database downloads.</p>	
<p>Primary DNS server for network interface C (IP address)</p>	
<p>Secondary DNS server for network interface C (IP address) <i>Optional</i></p>	
<p>Tertiary DNS server for network interface C (IP address) <i>Optional</i></p>	
<p>Appliance manager password The password must be 8 to 15 characters and:</p> <ul style="list-style-type: none"> ● Include at least <ul style="list-style-type: none"> ■ 1 uppercase character ■ 1 lowercase character ■ 1 number ■ 1 non-alphanumeric (special) character. ● Not include <ul style="list-style-type: none"> ■ The username, hostname, or name of a service or component ■ Any of the 3 previous passwords ■ Any of these special characters space \$: ` \ " 	
<p>Integration method for this appliance (Choose one):</p> <ul style="list-style-type: none"> ● Standalone (Network Agent only) ● Microsoft TMG ● Cisco ASA ● Citrix 	<p>Choose your third-party integration product (if any).</p>
<p>Send usage statistics?</p>	<p>Usage statistics from appliance modules can optionally be sent to Forcepoint to help improve the accuracy of categorization.</p>
<p>Policy mode</p>	<p>User directory and filtering, or Filtering only</p>

Run the firstboot script

The initial command-line configuration script (**firstboot**) starts automatically when you power on the appliance for the time.

1. Access the appliance console with the integrated DELL Remote Access Controller (iDRAC) Virtual Console, or by directly connecting a USB keyboard and monitor, or using a serial port connection.

**Note**

For serial port activation, use:

- 9600 baud rate
 - 8 data bits
 - no parity
-

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to start the **firstboot** configuration process.
4. At the next prompt, select **Web Filter & Security** as your security mode.
5. Follow the on-screen instructions to provide the information collected above.

After the firstboot script has completed, a command-line interface (CLI) logon prompt displays. Log on to perform post-firstboot configuration, including configuring additional network interfaces. See [TRITON 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 [TRITON Appliances CLI guide](#).

Changing the security mode requires re-imaging the appliance.

Installing components on Windows

1. Prepare the machine and download the installer as described in [Step 2: Prepare the management server, page 2](#).
2. Right-click **TRITON82xSetup.exe** and select **Run as administrator** to launch the 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 **TRITON AP-WEB or Web Filter & Security**.

8. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
9. Accept the subscription agreement, then click **Next**.
10. Select the **Custom** installation type, then click **Next**.
11. 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 (go to the **Settings > General > Policy Brokers** page in the Web module of the TRITON Manager).
12. 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.
13. 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.

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

The summary shows the installation path and size, and the components to be installed.
15. A progress screen is displayed. Wait for the installation to complete.
16. On the Installation Complete screen, click **Next**.

Installing components on Linux

1. Prepare the machine and download and launch the installer as described in [Prepare the Linux server, page 15](#).
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 (go to the Settings > General > Policy Brokers page in the Web module of the TRITON 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, or click or select **Choose** to specify another path, and then click or select **Next**.
The installation path must be absolute (not relative). The default installation path is: `/opt/Websense/`
The installer creates this directory if it does not exist.



Important

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

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

- Insufficient disk space prompts an error message. The installer closes when you click or select **OK**.

- Insufficient RAM prompts a warning message. The installation continues when you click or select **OK**. To ensure optimal performance, increase your memory to the recommended amount.
8. On the Pre-Installation Summary screen, verify the information shown, then click or select **Next**.
The summary shows the installation path and size, and the components to be installed.
 9. An Installing progress screen is displayed. Wait for the installation to complete.



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.

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

Step 9: 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 28](#)
- [Install the ISAPI Filter plug-in for Microsoft Forefront TMG, page 32](#)

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 TRITON 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

The Filtering Service port must be in the range 1024-65535. To determine what port is used by Filtering Service, check the **eimserver.ini** file—located in C:\Program Files or Program Files (x86)\Websense\Web Security\bin or /opt/Websense/bin/—on the Filtering Service machine. In this file, look for the **WebsenseServerPort** value.

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

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

- 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 independently. If the Citrix Integration Service fails over from one Filtering Service instance to another, usage quotas may be different and override passwords may need to be entered again.

- e. Enable or disable the **Do not send user name information to Filtering Service** option. 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. Enable or disable the **Block all HTTP/HTTPS/FTP traffic if unable to connect to a Filtering Server** option to determine whether Citrix Integration Service blocks or permits all requests when it cannot communicate with Filtering Service.
5. In the **Client Settings** screen, select options as described below. When you are finished, click **Next**.
 - **Notify users when HTTPS or FTP traffic is blocked:** 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.
 - **Protect installation directory from modification or deletion:** This option prevents 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**.

The URLs you specify here are trusted by any Citrix server on which this Citrix Integration Service is install. It has no bearing on how Filtering Service instances

filter requests from non-Citrix users and other 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 different folders.

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.



Note

If you want to use the same Citrix Integration Service configuration on multiple Citrix servers, use the same Citrix installation package for them. Repeat the procedure, below, on each Citrix server.

1. Log on with **local** administrator privileges to the Citrix server.
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.

Install the ISAPI Filter plug-in for Microsoft Forefront TMG

To enable integration with Microsoft Forefront TMG, use the TRITON Unified 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 (Control Service communication port) must be open locally for the ISAPI Filter plug-in to be installed successfully.
-

Before beginning the installation process:

- Use the Downloads tab of the [My Account](#) page at forcepoint.com to download or copy the TRITON Unified Installer to the TMG machine.
- Close all applications and stop any antivirus software.

To perform the installation:

1. Log on to the machine with domain admin privileges.
2. Use the Downloads tab of the [My Account](#) page at forcepoint.com to download the TRITON Unified Installer (**TRITON83xSetup.exe**)

3. Right-click **TRITON83xSetup.exe** and select **Run as administrator** to launch the installer. After a few seconds, a progress dialog box appears, as files are extracted.
4. On the Welcome screen, click **Start**.
5. On the Subscription Agreement screen, select **I accept this agreement**, then click **Next**.
6. On the Installation Type screen, select **Custom** and then click **Next**.
7. On the Summary screen, click **Next**.
8. On the Custom Installation screen, click the **Install** link next to **TRITON AP-WEB or Web Filter & Security**.
9. On the Welcome screen for the Web Protection Solutions setup program, click **Next**.
10. Accept the subscription agreement, then click **Next**.
11. 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**.
12. Select the **Custom** installation type, then click **Next**.
13. On the Select Components screen, select **Filtering Plug-in**, then click **Next**.
14. 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.
15. On the **Select Integration** screen, select **Microsoft Forefront Threat Management Gateway** and click **Next**.
16. On the **Installation Directory** screen, accept the default location and click **Next**.
17. 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.
18. 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, go to the Windows Services tool (**Start > Administrative Tools > Services** or **Server Manager > Tools > Services**). 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.

19. 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**. The Firewall Service may also be started from the Forefront TMG management console. See the Microsoft documentation for more information.

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

You can verify successful installation of the ISAPI Filter plug-in by logging into the Forefront TMG management console. Navigate to **System > Web Filters** and verify that WsISAFilter is present in the list of Web Filters.

## Step 10: Initial Configuration

---



#### Tip

All Web Filter & Security 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 TRITON Manager 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 TRITON Manager, make sure that Enhanced Security Configuration (IE ESC) is disabled on their machines.
2. Use a supported browser to launch the TRITON Manager and log on using the default account (**admin**) and the password created during installation.

The TRITON Manager URL is:

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

Here, <IP\_address> is the IP address of the TRITON management server.

3. Enter your subscription key. At first startup, the Web module of the TRITON Manager prompts for a subscription key in the Initial Setup Checklist.
4. If you did not provide SMTP server details during installation, use the **TRITON 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.

