Installation Instructions: TRITON AP-WEB

Installation Instructions | TRITON AP-WEB | v8.3.x

Use these instructions to complete a typical installation of TRITON® AP-WEB. In this configuration:

- The policy source (the standalone or primary Policy Broker and its Policy Server) resides on the TRITON management server machine.
  - This configuration is not required. Policy Broker and Policy Server may reside on another Windows or Linux server, or on a TRITON appliance.
  - Regardless of where they reside, always install a central Policy Broker and Policy Server before installing any other components.
- 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 whose requests are managed by Filtering Service has no direct or indirect influence over the database. Although the log entry for each request is stored in the SQL Server database, the user does not direct its storage and cannot retrieve the record.

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

This procedure includes steps for installing the components required to enable the Web Hybrid and Web DLP modules, if purchased.

This installation procedure includes the following steps:

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.

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.

      ○ 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 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.)

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.
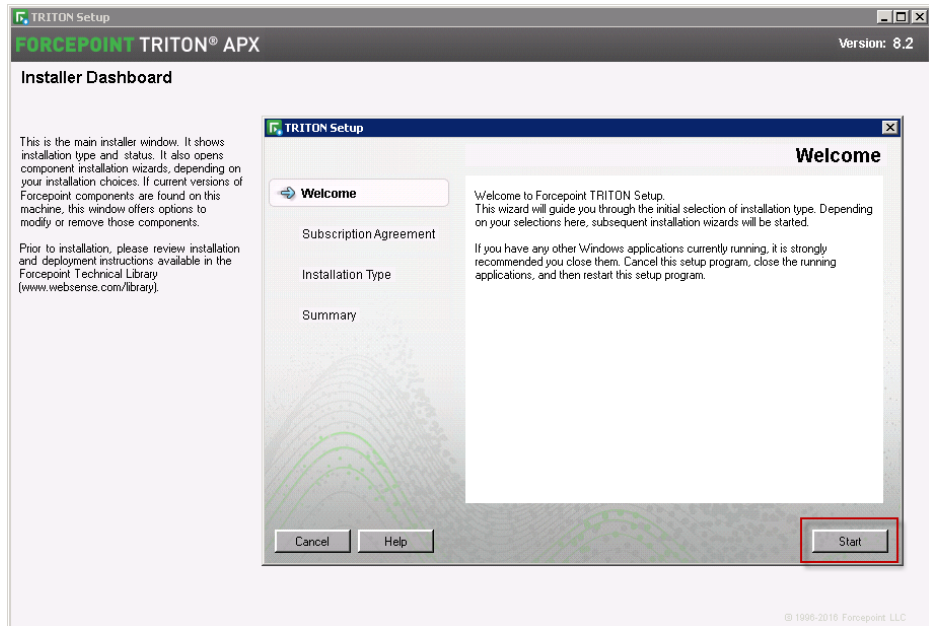
> **Important**
> If you are installing data protection components, do not change this account after installation. Be sure it's a dedicated account that you want installed services to use when interacting with the operating system-the service account. If you must change the account, contact Technical Support first.

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:

   a. Select **TRITON Manager**.

   b. Mark the **TRITON AP-WEB or Web Filter & Security** check box.

   c. If you have purchased the Web DLP Module, also mark the **TRITON AP-DATA** check box.

   d. Click **Next**.
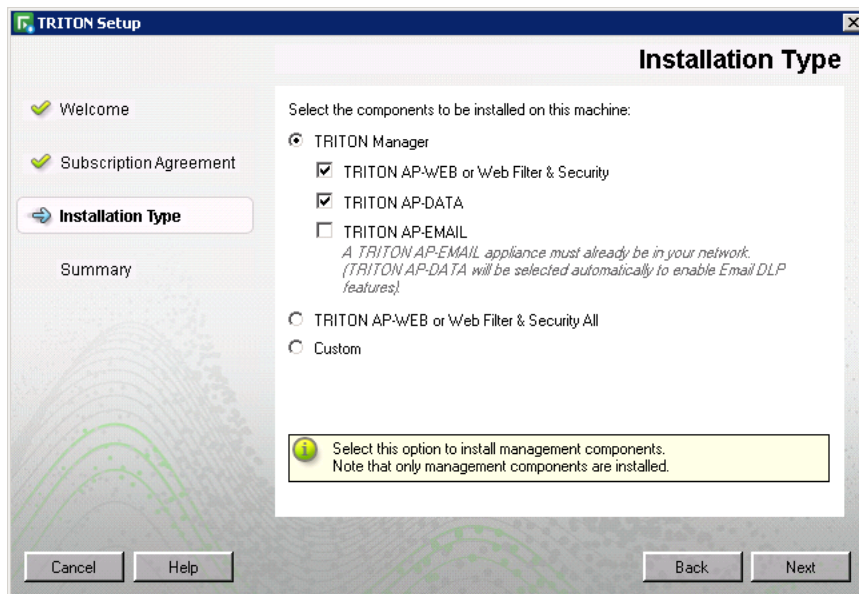
5. On the **Summary** screen, click **Next** to continue the installation.

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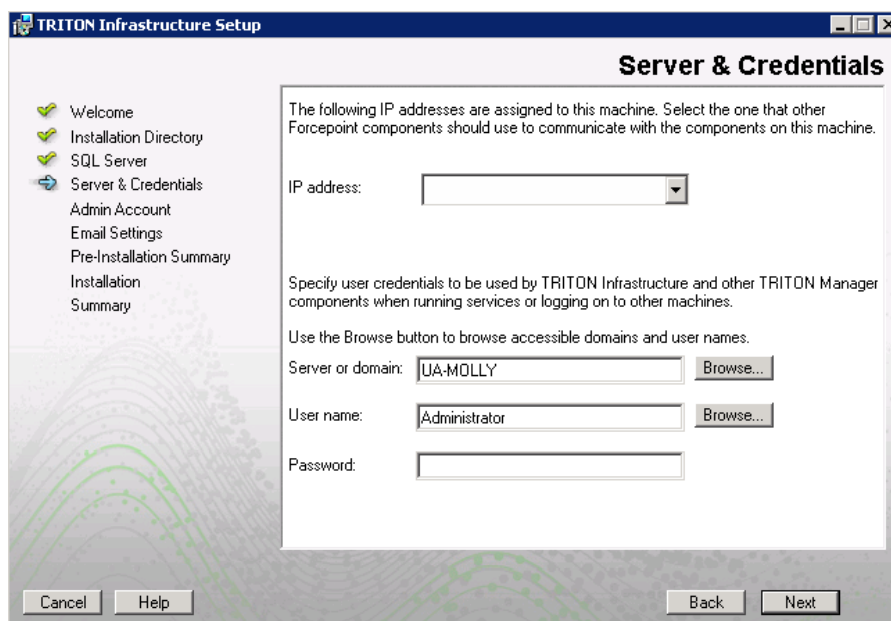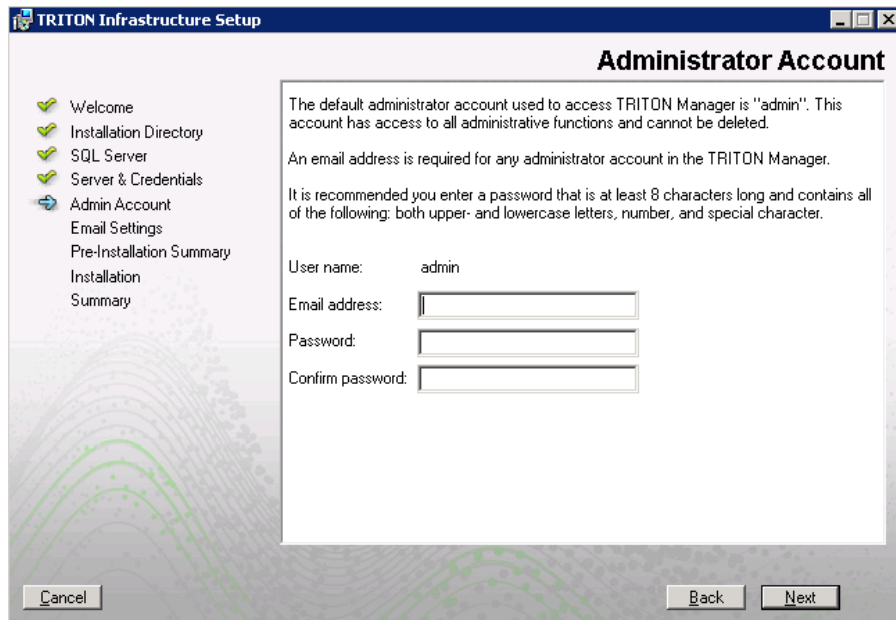
■ Select an **IP address** for this machine. If this machine has a single network interface card (NIC), only one address is listed.

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.

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.

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 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.

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

8. 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 the Web management components

In a typical deployment, the TRITON Manager, the standalone or primary Policy Broker, and the central Policy Server reside on the Windows-based 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**.

   Linking Service cannot be installed until Filtering Service is running in your network. You will add an instance of Linking Service later.

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.

   Depending on your current configuration, the Native Client installer may run silently in the background, or prompt you for input.

   - When the Native Client installer runs in the background, you will know the process is complete when the Forcepoint installer continues to the next screen. This may take a few minutes.

   - When the Native Client installer runs in the foreground, follow the prompts to complete the installation. Note that if you are prompted to reboot the machine, do not reboot at this point. Instead, complete the Forcepoint software installation first, then reboot.

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**.

8. If you have chosen to install the Data Security module, you are returned to the Installer Dashboard and the next component installer is launched.

Step 6: (Web DLP module only) Install the Data Security management components

If you have purchased the Web DLP module for TRITON AP-WEB, install the components used to enable data loss prevention over web channels (Web DLP) on the TRITON management server machine, as described below. To support Web DLP, TRITON AP-WEB and TRITON AP-DATA must reside on the same TRITON management server.

If you have not purchased the Web DLP module, continue with *Step 7: Install an instance of Filtering Service*, page 12.

1. On the TRITON AP-DATA installer **Welcome** screen, click **Next**.

2. On the Select Components screen, click **Next** to accept the default selections.

3. If prompted, click **OK** to indicate that services such as ASP.NET and SMTP will be enabled.

   Required Windows components will be installed. You may need access to the operating system installation disc or image.

4. On the Fingerprinting Database screen, accept the default location or use the **Browse** button to specify a different location.

   Note that you can install the Fingerprinting database to a local path only.

5. On the Temporary Folder Location screen, complete the fields as follows:

- **Enable incident archiving and system backup**: Check this box if you plan to archive old or aging incidents and perform system backup or restore. This box does not appear when you run the installer in Modify mode and perform a disaster recovery restore operation.

- **From SQL Server**: Enter the path that the SQL Server should use to access the temporary folder. For best practice, it should be a remote UNC path, but local and shared network paths are supported. For example: c:\folder or \\10.2.1.1.\folder. Make sure the account used to run SQL has write access to this folder.

- **From TRITON Management Server**: Enter the UNC path the management server should use to access the temporary folder. For example: \\10.2.1.1.\folder. Enter a user name and password for a user who is authorized to access this location.

6. On the Local Administrator screen, enter or verify the local administrator user name and password that will be used to run some Web DLP services, then click **Next**.

7. On the Installation Confirmation screen, click **Install** to begin installation of Data Security components.

   - A message may appear stating that port 80 is required. Click **Yes** to continue the installation.

   - A message may appear stating that port 443 may appear. Click **Yes** to continue the installation.

   - If prompted to install required software, click **Yes** to continue the installation.

8. The Installation progress screen appears. Wait for the installation to complete.

9. When the Installation Complete screen appears, click **Finish** to close the TRITON AP-DATA installer.

> **!** **Important**
>
> When you exit the installer, be sure to select the option that allows you to save installation files on this machine. There is one more component to install on the management server, but it cannot be installed until after you install Filtering Service.

Step 7: 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.

The security mode	TRITON AP-WEB
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. If Content Gateway will be configured to perform Integrated Windows Authentication, the hostname cannot exceed 11 characters (excluding the domain name). For more information, see the section titled **Integrated Windows Authentication** in the Content Gateway Manager Help.	
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) *Optional* 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 TRITON AP-WEB 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) *Optional*	
Tertiary DNS server for network interface C (IP address) *Optional*	

Unified password
 This password is for the:
 • Appliance manager
 • Content Gateway manager
 The password must be 8 to 15 characters and:
 • Include at least
   ■ 1 uppercase character
   ■ 1 lowercase character
   ■ 1 number
   ■ 1 non-alphanumeric (special) character.
 • Not include
   ■ The username, hostname, or name of a service or component
   ■ Any of the 3 previous passwords
   ■ Any of these special characters
     space $: ` \ "
 The password applies to the CLI and Content Gateway Manager	

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 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 **TRITON AP-WEB** 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 Content Gateway 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.).

e. Synchronize the clocks on all machines (including appliances) where a Web Security 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.

   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 Monitor

    Optionally, you may also select:

    ■ Network Agent

    ■ State Server

    ■ DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent

    ■ Directory Agent (*used by the Web Hybrid module*)

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, select **Install TRITON AP-WEB to connect to Content Gateway**, then click **Next**.

19. 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**.

20. On the Feedback screen, indicate whether you want your web protection software to send feedback to Forcepoint LLC, then click **Next**.

21. 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.

22. 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.

23. 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.

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

25. 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 f**ile, use the following 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.gz

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

   ■ Directory Agent (*used by the Web Hybrid module*)

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, select **Install TRITON AP-WEB to connect to Content Gateway** then click or select **Next**.

   When you install Content Gateway (as described in), you will be prompted for the Filtering Service IP address.

8. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other software components, then click or select **Next**.

9. On the Feedback screen, indicate whether you want your web protection software to send feedback to Forcepoint LLC, then click or select **Next**.

10. 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.

11. 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.

12. 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.

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

Step 8: Install Log Server and (optionally) Sync Service

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

If you have purchased the Web Hybrid module, Sync Service is responsible for sending policy information to the hybrid service, and passing reporting information from the hybrid service to Log Server. In most cases, it is best to install Sync Service on the same machine as Log Server. However, Sync Service is supported on Linux as well as Windows.

To prepare for installation on the Windows machine that will host Log Server and (optionally) Sync Service:

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 sufficient 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 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.).

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 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.

8. Disable User Account Control (UAC) and Data Execution Prevention (DEP) settings, and make sure that no Software Restriction Policies will block the installation.

To install Log Server and (optionally) Sync Service:

1. Log on to the machine with domain adm 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, and then click **Next**.

12. Select the **Custom** installation type, then click **Next.**

13. On the Select Components screen:

    a. Select **Log Server**.

    b. If you have purchased the Web Hybrid module, select **Sync Service**.

    c. Click **Next**.

14. 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**.

15. On the Policy Broker Connection screen, enter the IP address of the primary (or standalone) Policy Broker, and the Policy Broker communication port (55880, by default), and then click **Next**.

16. If the Log Server 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.

    Depending on your current configuration, the Native Client installer may run silently in the background, or prompt you for input.

    ■ When the Native Client installer runs in the background, you will know the process is complete when the Forcepoint installer continues to the next screen. This may take a few minutes.

    ■ When the Native Client installer runs in the foreground, follow the prompts to complete the installation. Note that if you are prompted to reboot the machine, do not reboot at this point. Instead, complete the Forcepoint software installation first, then reboot.

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 (-).

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. Restart the following 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 9: (Web DLP module only) Install Linking Service on the management server

If you have purchased the Web DLP module, Linking Service allows the TRITON AP-DATA services that provide Web DLP functionality to get category and user information from Filtering Service.

This service was not installed when you installed the rest of the management server components because it is dependent on Filtering Service.

To install Linking Service:

1. Relaunch the TRITON Unified Installer on the management server machine from the Start menu or Start screen.

2. On the Modify Installation page, click the **Modify** link next to TRITON AP-WEB.

3. On the Add Components screen, select **Install additional components on this machine**, then click **Next**.

4. Use the Select Components screen to select **Linking Service**, then click **Next**.

5. On the Filtering Service Communication screen, enter the IP address of the Filtering Service machine and the Filtering Service communication port (15868, by default), then click **Next**.

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

    The summary shows the components to be installed.

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

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

Step 10: Install additional web protection components

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

- All components except Content Gateway 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, Network Agent, and Content Gateway. Directory Agent can also be enabled on these appliances. During setup, you are prompted to connect to Policy Broker (which typically resides on the TRITON management server).
    - **Filtering only** appliances include Filtering Service, Network Agent, and Content Gateway. 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).

Using TRITON 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 script. Some of this information may have been written down on the Quick Start poster during hardware setup.

The security mode	TRITON AP-WEB
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. If Content Gateway will be configured to perform Integrated Windows Authentication, the hostname cannot exceed 11 characters (excluding the domain name). For more information, see the section titled **Integrated Windows Authentication** in the Content Gateway Manager Help.	

IP address for appliance management network interface C	Must be an IPv4 address.
Subnet mask for network interface C	
Default gateway for network interface C (IP address) *Optional* 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 TRITON AP-WEB 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) *Optional*	
Tertiary DNS server for network interface C (IP address) *Optional*	
Unified password This password is for the: ● Appliance manager ● Content Gateway manager The password must be 8 to 15 characters and: ● Include at least ■ 1 uppercase character ■ 1 lowercase character ■ 1 number ■ 1 non-alphanumeric (special) character. ● Not include ■ The username, hostname, or name of a service or component ■ Any of the 3 previous passwords ■ Any of these special characters space $: ` \ " The password applies to the CLI and Content Gateway Manager	
Send usage statistics?	Usage statistics from appliance modules can optionally be sent to Forcepoint to help improve the accuracy of categorization.
Policy mode	User directory and filtering, or Filtering only

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 **TRITON AP-WEB** 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 Content Gateway 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 3.
2. 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.
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**.

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.

   ■ Each time you install a Filtering Service instance, select **Content Gateway** as the integration product.

   When you install Content Gateway (as described in *Step 11: Install Content Gateway*, page 32), you will be prompted for a Policy Server IP address and a Filtering Service IP address.

   ■ 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 18.

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.

   ■ Each time you install a Filtering Service instance, select **Content Gateway** as the integration product.

     When you install Content Gateway (as described in *Step 11: Install Content Gateway*, page 32), you will be prompted for a Policy Server IP address and a Filtering Service IP address.

   ■ 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 11: Install Content Gateway

If you are not using appliances to host policy enforcement components, complete these steps to install Content Gateway on one or more Linux servers.

Prepare for installation

1. Make sure that the server you intend to use meets or exceeds the requirements listed in the "Content Gateway" section of "Requirements for web protection solutions" in <u>System requirements for this version</u>.

   See *Installing on Red Hat Enterprise Linux 6, update 5 and higher* for additional details on installing on Red Hat Linux 6.

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

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

      ```
      hostname <hostname>
      ```

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

      ```
      HOSTNAME=<hostname>
      ```

   c. Specify the IP address to associate with the hostname in the **/etc/hosts** file. This should be static and not served by DHCP.

      The proxy uses this IP address in features such as transparent authentication and hierarchical caching. This must be the first line in the file.

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

      ```
      xxx.xxx.xxx.xxx    <FQDN>       <hostname>
      127.0.0.1          localhost.localdomain   localhost
      ::1                localhost6.localdomain6 localhost6
      ```

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

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

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

      ```
      search <subdomain1>.<top-level domain>
      <subdomain2>.<top-level domain> <subdomain3>.<top-
      level domain>

      nameserver xxx.xxx.xxx.xxx

      nameserver xxx.xxx.xxx.xxx
      ```

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

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

3. For Content Gateway to operate as a caching proxy, it must have access to at least one raw disk. Otherwise, Content Gateway will function as a proxy only.

To create a raw disk for the proxy cache when all disks have a mounted file system:

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

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

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

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

```
df -k
```

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

c. Save and close the file.

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

```
umount <file_system>
```

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

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

4. If you plan to deploy multiple, clustered instances of Content Gateway:

■ Find the name of the network interface you want to use for cluster communication. This must be a dedicated interface.

■ Find or define a multicast group IP address.

If a multicast group IP address has not already been defined, enter the following at a command line to define the multicast route:

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

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

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

5. It is recommended that the Content Gateway host machine have Internet connectivity before starting the installation procedure. The software will install without Internet connectivity, but analytic database updates (not available when Content Gateway is a component of TRITON AP-DATA) cannot be performed until Internet connectivity is available.

6. Use the Download tab of My Account page at forcepoint.com to download the **ContentGateway83xSetup_Lnx.tar.gz** installer tar archive to a temporary directory on the machine that will host Content Gateway.

   To unpack the tar archive, use the command:

```
tar -xvzf ContentGateway83xSetup_Lnx.tar.gz
```

7. Consider the following security issues prior to installing Content Gateway:

   ■ Physical access to the system can be a security risk. Unauthorized users could gain access to the file system, and under more extreme circumstances, examine traffic passing through Content Gateway. It is strongly recommended that the Content Gateway server be locked in an IT closet and that a BIOS password be enabled.

   ■ Ensure that root permissions are restricted to a select few persons. This important restriction helps preclude unauthorized access to the Content Gateway file system.

   ■ (When Content Gateway is a component of TRITON AP-Web) For a list of default ports, see the Web tab of the TRITON Ports spreadsheet. They must be open to support the full set of TRITON AP-WEB features.

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

   Restrict inbound traffic to as few other ports as possible on the Content Gateway server. In addition, if your subscription does not include certain features, you can restrict inbound traffic to the unneeded ports. For example, if your subscription does not include the Web DLP module, you may choose to restrict inbound traffic to those ports related to TRITON AP-DATA.

   ■ If your server is running the Linux IPTables firewall, you must configure the rules in a way that enables Content Gateway to operate effectively. See IPTables for Content Gateway.

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

Installing on Red Hat Enterprise Linux 6, update 5 and higher

biosdevname

Red Hat Enterprise Linux 6, update 1 introduced **biosdevname**. This new convention is not supported by Content Gateway version 8.3.x and lower.

What is biosdevname? The Red Hat Enterprise Linux update 6.1 release notes state:

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

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

The presence of a single Ethernet device that does not have the SMIBIOS Slot # and biosdevname field causes the Red Hat Enterprise Linux 6.x installer and "udev" to fall back to the eth# device naming convention for all interfaces.

> **Important**
> To ensure interface name consistency among hardware platforms and Red Hat Enterprise Linux 6.5 and higher, Content Gateway Version 8.3.x requires "eth#" names. If any non-"eth#" names exist, the Content Gateway installer exits and provides a link to instructions for modifying system startup files.

Upgrading from Red Hat Enterprise Linux 6.0 to 6.5 and higher poses no risk. There was no biosdevname support in Update 6.0 and device names are not altered by the upgrade to 6.4 or higher.

Disabling biosdevname

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

There are 2 ways to disable biosdevname:

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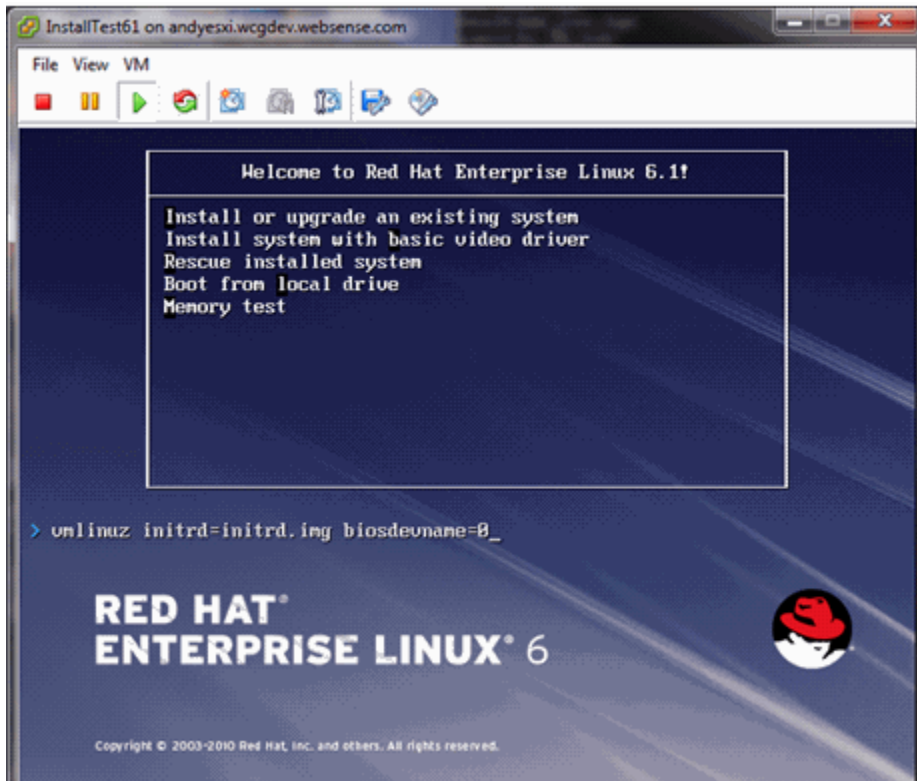2. Post-operating system installation through modification of several system files and other activities.

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

Disabling biosdevname during operating system installation:
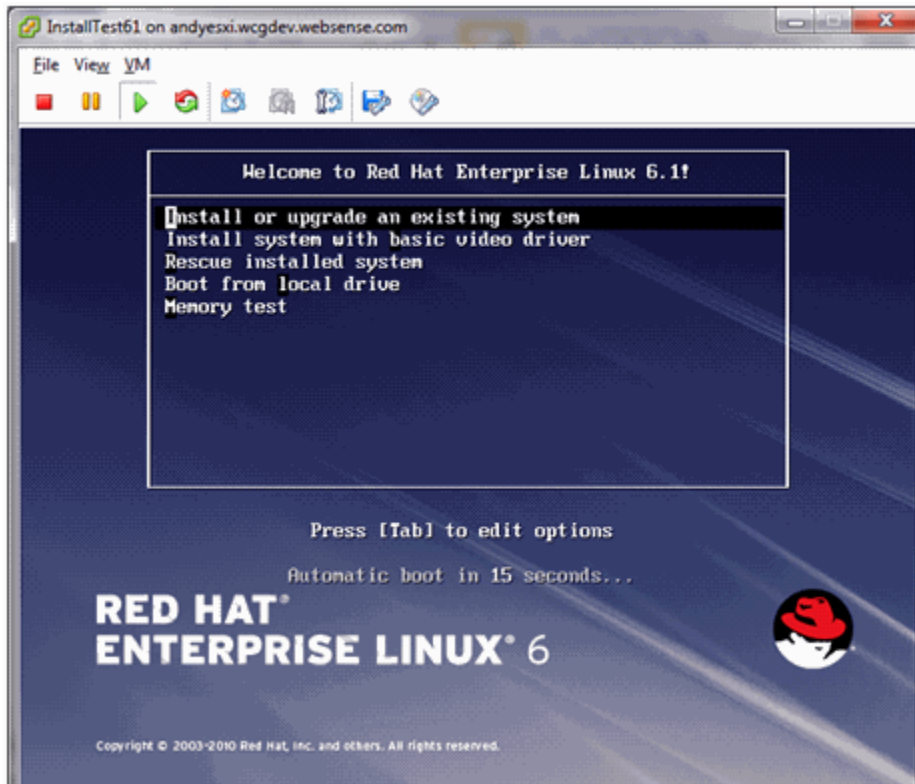
When the installer starts, press [TAB] and alter the boot line to add "biosdevname=0" as follows:

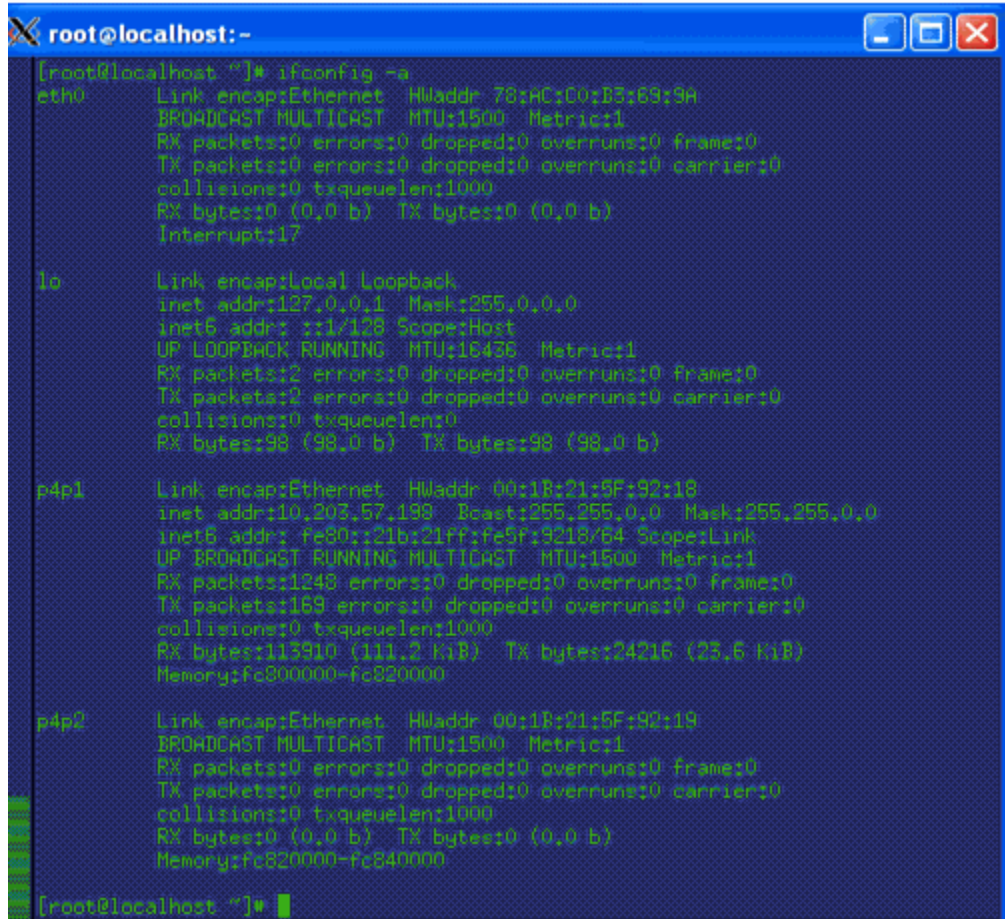Proceed through the rest of the installer as usual.

Disabling biosdevname after operating system installation:

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

```
ifconfig -a
```

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

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

1. Log in as root.
2. cd /etc/sysconfig/network-scripts
3. Rename all "ifcfg-<ifname>" files except "ifcfg-lo" so that they are named "ifcfg-eth#".

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

   b. When the above are done, rename the "ifcfg-p#p#" files.

   If there are multiple "ifcfg-p#p1" interfaces, rename all of them in the order of the lowest "ifcfg-p#" first. For example, if the initial set of interfaces presented by "`ifconfig -a" is:

   em1 em2 em3 em4 p1p1 p1p2 p2p1 p2p2

   > em1 -> eth0
   >
   > em2 -> eth1
   >
   > em3 -> eth2
   >
   > em4 -> eth3
   >
   > p1p1 -> eth4
   >
   > p1p2 -> eth5

p2p1 -> eth6

p2p2 -> eth7

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

4. Edit all the ifcfg-eth# files.

   a. Update the DEVICE= sections to refer to the new name: "eth#"

   b. Update the NAME= sections to refer to the new name: "System eth#"

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

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

6. Modify the "grub.conf" file to disable biosdevname for the kernel you boot.

   a. Edit /boot/grub/grub.conf

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

```
biosdevname=0
```

7. Reboot.

8. Reconfigure the interfaces as required.

Installer gives NetworkManager or avahi-daemon error

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

```
Error: The avahi-daemon service is enabled on this system
and must be disabled before Content Gateway v8.3.x can be
installed.
```

```
Please disable the avahi-daemon service with the following
commands and restart the Content Gateway installation.
    chkconfig --levels 2345 avahi-daemon off
    service avahi-daemon stop
```

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

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

1. To disable the avahi-daemon service:

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

2. To restart the installer:

```
    ./wcg_install.sh
```

Install Content Gateway

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

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

2. Make sure you have root permissions:

   ```
   su root
   ```

3. In the directory where you unpacked the tar archive, begin the installation, and respond to the prompts to configure the application.

   ```
   ./wcg_install.sh
   ```

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

   > **Note**
   >
   > Up to the configuration summary, you can quit the installer by pressing Ctrl-C. If you choose to continue the installation past the configuration summary and you want to quit, do **not** use Ctrl-C. Instead, allow the installation to complete and then uninstall it.
   >
   > If you want to change your answer to any of the installer prompts, you will be given a chance to start over at the first prompt once you reach the configuration summary; you do not have to quit the installer.

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

   ```
   Error: Content Gateway v8.3.x on x86_64 requires several
   packages that are not present on your system.

   Please install the following packages: <list of packages>

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

   yum install <list of packages>

   See the Technical Library (www.websense.com/library) for
   information about the software requirements for x86_64
   installation.
   ```

   Install the missing packages and again start the Content Gateway installer.

   Here is an example of a system resource warning:

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

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

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

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

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

6. Enter and confirm a password for the Content Gateway Manager administrator account:

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

This account enables you to log on to the management interface for Content Gateway (the Content Gateway manager). The default username is **admin**.

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

> **Important**
> The password cannot contain the following characters:
>
> - space
> - $ (dollar symbol)
> - : (colon)
> - ' (backtick; typically shares a key with tilde, ~)
> - \ (backslash)
> - " (double-quote)

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

7. Enter an email address where Content Gateway can send alarm messages:

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

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

8. Select the Content Gateway Integration Configuration you wish to install:

    ```
    '1' - Select '1' to configure Content Gateway as a
    component of TRITON AP-WEB

    '2' - Select '2' to configure Content Gateway as a
    component of TRITON AP-DATA (without TRITON AP-WEB)
    ```

    If you select '1', proceed to the next step.

    If you select '2', you will need to enter the IP address for the TRITON management server to connect to.

    ```
    Enter Data Security Manager Server IP: [] >
    ```

    Use dot notation (i.e., xxx.xxx.xxx.xxx). The address must be IPv4.

    Skip to step 11.

9. Enter the IP address for Policy Server:

    ```
    Enter the Policy Server IP address (leave blank if
    integrating with Data Security only): [] >
    ```

    Use dot notation (i.e., xxx.xxx.xxx.xxx). The address must be IPv4.

10. Enter the IP address for Filtering Service:

    ```
    Enter the Filtering Service IP address: [<Policy Server
    address>] >
    ```

    The default is the same address as Policy Server.

11. Review default Content Gateway ports:

    ```
    Content Gateway uses 9 ports on your server:

    Port Assignments:

    -----------------
    '1'  Content Gateway Proxy Port          8080
    '2'  Web Interface port                  8081
    '3'  Auto config port                    8083
    '4'  Process manager port                8084
    '5'  Logging server port                 8085
    '6'  Clustering port                     8086
    '7'  Reliable service port               8087
    '8'  Multicast port                      8088
    '9'  Endpoint Authentication Server Port 9090


    Enter the port assignment you would like to change:
    '1-9' - specific port changes
    'X'   - no change
    'H'   - help
    [X] >
    ```

    Change a port assignment if it will conflict with another application or process on the machine. Otherwise, leave the default assignments in place.

If you do not want to use these ports for Content Gateway, or if the installation program indicates that a port conflict exists, make any necessary changes. Any new port numbers you assign must be between 1025 and 65535, inclusive.

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

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

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

13. If two or more network interfaces are found on this machine, you are asked whether this instance of Content Gateway should be part of a cluster:

```
Content Gateway Clustering Information

----------------------------------------------

'1' - Select '1' to configure Content Gateway
        for management clustering. The nodes in the cluster
        will share configuration/management information
        automatically.

'2' - Select '2' to operate this Content Gateway
        as a single node.


Enter the cluster type for this Content Gateway
installation:

[2] >
```

If you do not want this instance of Content Gateway to be part of a cluster, enter 2.

If you select 1, provide information about the cluster:

```
Enter the name of this Content Gateway cluster.

><cluster_name>
```

Note: All members of a cluster must use the same cluster name.

```
Enter a network interface for cluster communication.

Available interfaces:
<interface, e.g., eth0>
<interface, e.g., eth1>

Enter the cluster network interface:

>

Enter a multicast group address for cluster <cluster_name>.
Address must be between 224.0.1.27 - 224.0.1.254:
[<default IP address>] >
```

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

```
No disks are detected for cache.

Content Gateway will operate in PROXY_ONLY mode.
```

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

15. If a raw disk is detected, you can enable the web cache feature of Content Gateway:

> ✅ **Note**
> If you choose to not enable raw disk cache now, cache disks may be added after Content Gateway has been installed. For instructions, see Content Gateway Manager Help.

```
Would you like to enable raw disk cache [y/n]? y
```

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

```
Select available disk resources to use for the cache.
Remember that space used for the cache cannot be used for
any other purpose.
Here are the available drives
(1) /dev/sdb 146778685440 0x0
```

Note: The above drive is only an example.

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

b. Indicate if you want to add or remove disks individually or as a group.

```
Choose one of the following options:
'A'   - Add disk(s) to cache
'R'   - Remove disk(s) from cache
'S'   - Add all available disks to cache
'U'   - Remove all disks from cache
'X'   - Done with selection, continue
        Content Gateway installation.
Option: > A
[ ] (1) /dev/sdb 146778685440 0x0
```

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

```
Enter number to add item, press 'F' when finished:
[F] >1
Item '1' is selected
[F] >
```

d. Your selections are confirmed. Note the "x" before the name of the disk.

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

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

```
Choose one of the following options:
'A'    - Add disk(s) to cache
'R'    - Remove disk(s) from cache
'S'    - Add all available disks to cache
'U'    - Remove all disks from cache
'X'    - Done with selection, continue
          Content Gateway installation.
Option: >X
```

16. As a way of improving the Content Gateway product, you can elect to send Forcepoint LLC, information about usage statistics, scanned content, and activated product features. **Important:** Individual users are never identified.

    Enter **y** or **n**.

17. A configuration summary appears, showing your answers to the installer prompts (note: summary below is an example):

```
Configuration Summary
--------------------------------------------------------------
Content Gateway Install Directory : /opt/WCG
Admin Username for Content Gateway Manager: admin
Alarm Email Address                      : <email address>

Content Gateway Install Type             : TRITON AP-WEB

Policy Server IP Address                 : <IP address>
Filtering Service IP Address             : <IP address>

Content Gateway Cluster Type             : NO_CLUSTER

Content Gateway Cache Type               : LRAW_DISK
  Cache Disk                             : /dev/sdb
  Total Cache Partition Used             : 1

                ******************
                *  W A R N I N G  *
                ******************
   CACHE DISKS LISTED ABOVE WILL BE CLEARED DURING
   INSTALLATION!! CONTENTS OF THESE DISKS WILL BE
   COMPLETELY LOST WITH NO CHANCE OF RETRIEVAL.

   Installer CANNOT detect all potential disk mirroring
   systems. Please make sure the cache disks listed
   above are not in use as mirrors of active file
   systems and do not contain any useful data.
Do you want to continue installation with this configuration
[y/n]?
```

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

> **Important**
>
> If you enter **y** to proceed but you decide you want to cancel the installation, do not attempt to quit the installer by pressing Ctrl-C. Allow the installation to complete. Then uninstall it.

18. Wait for the installation to complete.

> **Note**
>
> The subscription key is shared automatically with Content Gateway when it is entered in the Web module of the TRITON Manager.
>
> If you receive an email from Content Gateway (to the address you specified during installation) with "WCG license download failed" in the subject line, this alert does not mean a problem occurred with the installation. The alert indicates that your deployment may require you to manually enter the subscription key in the Content Gateway manager.
>
> When Content Gateway is a component of TRITON AP-DATA, the subscription must be entered manually.

19. When installation is complete, reboot the Content Gateway server.
20. When the reboot is complete, check Content Gateway status with:

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

    All services should be running. These include Content Cop, Content Gateway, Content Gateway Manager, and Analytics Server (if Content Gateway is a component of TRITON AP-WEB).

Step 12: Initial Configuration

> **Tip**
>
> All web protection 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.

Enter your subscription key

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 console URL is:

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

   Here, *<IP_address>* is the IP address of the TRITON management server.

3. Enter your subscription key or keys. At first startup:

   - The Web module of the TRITON Manager prompts for a subscription key in the Initial Setup Checklist. The key is automatically applied to Content Gateway, as well.
   - If you have purchased the Web DLP module, the Data module of the TRITON Manager also displays a subscription key page.

   Enter your subscription key and save the change in both consoles.

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. Once the Web and (optionally) Data modules of the TRITON Manager show that your key has been verified, log off of the TRITON Manager and log back on to see all of your subscribed features.

Confirm Content Gateway registration with TRITON AP-DATA

If you have purchased the Web DLP module, Content Gateway registers with TRITON AP-DATA automatically. To ensure that registration is successful:

- Synchronize the date and time on the Content Gateway and TRITON management server machines to within a few minutes.
- If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the appliance management interface (C) is not subject to transparent routing. If it is, the registration process will be intercepted by the transparent routing and will not complete properly.
- Make sure that the IPv4 address of the eth0 NIC on the Content Gateway machine is available (not required if Content Gateway is located on a TRITON appliance).

This is the NIC used by the TRITON management server during the registration process.

After registration, the IP address can move to another network interface.

If registration fails an alarm displays in Content Gateway Manager.

1. Verify connectivity between Content Gateway and the TRITON management server.

2. In Content Gateway Manager, in the **Networking** section of the **Configure > My Proxy > Basic > General** page, confirm that **Web DLP > Integrated on-box** is enabled.

3. Restart Content Gateway to initiate another registration attempt.

   Alternatively:

   a. Go to **Configure > Security > Web DLP** and enter the IP address of the management server.

   b. Enter a user name and password for a Data module administrator with Deploy Settings privileges.

   c. Click **Register**.

After Content Gateway has registered with TRITON AP-DATA, in Content Gateway Manager go to **Configure > Security > Web DLP** and set the following options:

1. **Analyze FTP Uploads**: Enable this option to send FTP uploads to Web DLP components for analysis and policy enforcement.

2. **Analyze HTTPS Content**: Enable this option to send decrypted HTTPS posts to Web DLP components for analysis and policy enforcement. SSL Manager must be enabled on Content Gateway.

3. Click **Apply** and restart Content Gateway.

Web DLP components communicate with the Content Gateway proxy over ports 17000-17014.

Configure the Content Gateway policy engine

When Content Gateway is registered with Web DLP components, a Content Gateway module appears on the System Modules page of the Data module of the TRITON Manager.

By default, this agent is configured to monitor web traffic, not block it, and for a default violation message to appear when an incident is triggered. If this is acceptable, you do not need to make changes to the Content Gateway configuration. Simply deploy the new settings.

If you want to block web traffic that breaches policy and customize the violation message, do the following:

1. In the Data module of the the TRITON Manager, go to the **Settings > Deployment > System Modules** page.

2. Select the Content Gateway module in the tree view (click the module name itself, not the plus sign next to it).

   It will be listed as **Content Gateway on** *<FQDN>* **(***<PE_version>***)**, where *<FQDN>* is the fully-qualified domain name of the Content Gateway machine and *<PE_version>* is the version of the Content Gateway policy engine.

3. Select the **HTTP/HTTPS** tab and configure the blocking behavior you want.

   Select **Help** > **Explain This Page** for instructions for each option.

4. Select the **FTP** tab and configure the blocking behavior you want.

   Select **Help** > **Explain This Page** for instructions for each option.

5. Click **Save** to save your changes.

6. Click **Deploy** to deploy your settings.

> **Important**
>
> Even if you do not change the default configuration, you must click **Deploy** to finalize your Content Gateway deployment process.

> **Important**
>
> Forcepoint Web Security customers using Red Hat Enterprise Linux or CentOS 7.x must disable firewalld prior to installing Content Gateway.
>
> On the machine where Content Gateway will be installed, execute the following:
>
> ```
> systemctl stop firewalld
> systemctl disable firewalld
> ```
>
> To successfully deploy Policy Engine, you must also execute the following:
>
> ```
> sysctl -w net.ipv4.tcp_tw_recycle=0
> ```

Verify that web and data protection components are linked

When Linking Service is installed, it allows Web DLP components to access user identification and URL categorization data. To verify that it is working:

1. Log onto the Data module of the TRITON Manager.

2. Select **Settings > General > Linking Service**.

3. Verify settings and test the connection.

   Select **Help** > **Explain This Page** for detailed information about the settings on this screen.

4. Click **OK** to save any changes.

5. Click **Deploy** to deploy your settings.

Set Up Content Gateway

- Log onto Content Gateway Manager and run a basic test (Getting Started)
- If there are multiple instances of Content Gateway, consider configuring a managed cluster.
- Configure protocols to proxy in addition to HTTP: HTTP (SSL Manager), FTP
- Complete your explicit or transparent proxy deployment
    - Content Gateway explicit and transparent proxy deployments
    - In Content Gateway Manager Help: Explicit proxy, Transparent proxy
- If proxy user authentication will be used, configure user authentication. Alternatively, if Content Gateway is installed as a component of TRITON AP-WEB, configure TRITON AP-WEB user identification.
- If Content Gateway is installed as a component of TRITON AP-WEB, configure the real-time Scanning Options in the Web module of the TRITON Manager.
- If you enabled content caching during installation, configure content caching.

After the base configuration has been tested, consider these additional activities:

- If Content Gateway is installed as a component of TRITON AP-WEB and you are using HTTPS (SSL Manager), use the Web module of the TRITON Manager to configure categories, clients, and destination servers for **SSL decryption bypass**
- Create Content Gateway filtering rules to:
    - Deny or allow URL requests
    - Insert custom headers
    - Allow specified applications, or requests to specified Web sites to bypass authentication
    - Keep or strip header information from client requests
    - Prevent specified applications from transiting the proxy
- In explicit proxy deployments, customize the PAC file
- In transparent proxy deployments, use **ARM dynamic and static bypass**, or use router ACL lists to bypass Content Gateway (see your router documentation).
- The ARM (Adaptive Redirection Module) module of Content Gateway uses a firewall. To facilitate interception and redirection of traffic:
    - IPTables rules are configured during installation of Content Gateway.
        - Forcepint IPTables chains are inserted.
        - Forcepoint IPTables rules are also inserted into existing chains.
        - Forcepoint chains and rules use "NC_" as a prefix for identification purposes.
    - IPTables rules configured outside of Content Gateway Manager must
        - Be inserted after Forecepoint rules.
        - Never be added to Forcepoint chains.

- Forcepoint chains and rules should never be edited.
- If customized chains or rules impact the Forcepoint configuration, navigate to /opt/wcg/bin and execute the following to re-establish the Forcepoint IPTables chains and rules.:

```
netcontrol.sh -r
```