Configuration Guide

Websense Web Security Solutions | Version 7.8.1

To help you make the transition to Websense Web Security or Web Security Gateway, this guide covers the basic steps involved in setting up your new solution in a network of up to 2500 users.

Important

Please refer to the Deployment and Installation Center detailed help in planning where and how to install Websense components.

This guide includes information about how to:

Complete product documentation is available in the Websense Technical Library.

Prepare for installation

This guide provides instructions for setting up a V-Series appliance to run Websense Web Security or Web Security Gateway.

- All core policy components reside on the V10000 G3 appliance.
- Management and reporting components reside on a Windows server.

✓ **Note**

If you are installing Websense software in a larger network, or if you want to learn how to integrate Websense Web Security with a third-party firewall, network appliance, or proxy server, see the Deployment and Installation Center.

Make sure that the machine that will host management and reporting components meets the following requirements before you begin.

Supported operating systems:

- Windows Server 2008 R2
- Windows Server 2012

Hardware requirements:

- 4 CPU cores (2.5 GHz)
- 12 GB RAM
- 150 GB Disk Space

Configuration prerequisites

- **Deployment**: Connect the V-Series appliance as directed on your appliance setup poster (V10000 G3 or V5000 G2)

  In Web Security Gateway deployments (V10000 or V5000):

  - Proxy interface P1 is used to proxy clients' Internet requests.
  - Network interface N may be connected to a span port so that Network Agent can be used to monitor non-HTTP activity in the network.
  - The remaining Web Security Gateway components use interface C for communication.

  In Web Security deployments (V5000 only):

  - Network interface N must be connected to a span port to allow Network Agent to monitor Internet traffic from all clients.
  - The remaining Web Security components use interface C for communication.

- **Internet access**: For the database download to occur after installation, the appliance C interface must be able to access:

  - a DNS server

  - all servers at **download.websense.com**

  Make sure that the download server address is permitted by all relevant external firewalls, proxy servers, and routers.

- **Reporting**: Websense Web Security solutions also require a Microsoft SQL Server database management system to host the reporting database (known as the Web Security Log Database). This database cannot reside on the Web Security management and reporting machine.

  Supported SQL Server versions include:

  - SQL Server 2008

    All editions except Web, Express, and Compact; all service packs, 32- and 64-bit, but not IA64

  - SQL Server 2008 R2

    All editions except Web and Compact; all service packs; not IA64

  - SQL Server 2012

    Standard, Business Intelligence, and Enterprise editions

Prepare to install the Websense V-Series appliance

The first time you start a Websense appliance, a brief script (**firstboot**) prompts you:

- select the security mode for the appliance
- supply settings for the network interface labeled C
- enter a few other general items, such as hostname and password

You are given the opportunity to review and change these settings before you exit the **firstboot** script. After you approve the settings, the appliance mode is configured.

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.

Security mode	**Web**
Which Web Security subscription?	*Choose one*: Websense Web Security Web Security Gateway

Hostname (example: appliance.domain.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 this is a Web Security Gateway appliance and 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 Content Gateway Manager Help.	
IP address for network interface C	
Subnet mask for network interface C	
Default gateway for network interface C (IP address)	
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 (8 to 15 characters, at least 1 letter and 1 number) This password is for the following: • Appliance manager • Content Gateway manager (*Web Security Gateway*)	
Integration method for this appliance (for sites using Web Security only [not Web Security Gateway]).	**Standalone** (Network Agent only)
Send usage statistics?	Usage statistics from appliance modules can optionally be sent to Websense to help improve the accuracy of categorization.

When you have finished gathering the information, you are ready to *Run the appliance configuration script*.

Run the appliance configuration script

Run the initial command-line configuration script (**firstboot**) as follows.

1. Access the appliance through a USB keyboard and monitor, or a serial port connection.

✓ **Note**

To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:

- 9600 baud rate
- 8 data bits
- no parity

1. Accept the subscription agreement when prompted.
2. When asked if you want to begin, enter **yes** to launch the **firstboot** activation script.
3. At the first prompt, select **Web** as the security mode.
   - On model V10000 G3, this activates Web Security Gateway.
   - On model V5000 G2, you are next prompted to select between Web Security or Web Security Gateway. Make sure to select the option that matches your subscription level.
4. Follow the on-screen instructions to provide the information collected in the previous section.

When the script is complete, continue with the next section, *Complete initial appliance configuration*.

Complete initial appliance configuration

Use the Appliance manager to perform key initial configuration tasks before you install management and reporting components on your Windows server.

1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP-address-of-C-interface>:9447/appmng
   ```

   Note that all Websense consoles support the following browsers:

   - Microsoft Internet Explorer 8 and 9, or 10 in desktop mode. (Compatibility View is not supported.)
   - Mozilla Firefox version 5 and later
   - Google Chrome 13 and later
2. Log on with the user name **admin** and the password set via the firstboot script.

3. In the left navigation pane, navigate to the **Configuration** section, then click **System**.
4. Under **Time and Date**:
   - Use the **Time zone** list to select the time zone to be used on this system.

     GMT (Greenwich Mean Time), the default, is also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.
   - Use the **Time and date** radio buttons to indicate how you want to set the date.

     Time is set and displayed using 24-hour notation.
     - To synchronize with an Internet Network Time Protocol (NTP) server (www.ntp.org.), select the **Automatically synchronize** option and enter the address of a primary NTP server. The secondary and tertiary fields are optional.

Important

If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between the appliance and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server.

If interface C on this appliance is not connected to the Internet, you must provide a way for interface C to reach an NTP server. One solution is to install an NTP server on the local network where interface C can reach it.

- To set the time yourself, select the **Manually set** option and change the value in the Date and Time fields. Use the format indicated below the entry field.

5. Create or edit a unique **appliance description** to help you identify and manage the system, particularly when there will be multiple appliances deployed, then Click **OK** to save your changes.

   The description is displayed in the Appliance list in the TRITON console.
6. Navigate to the **Configuration** > **Network Interfaces IPv4** and **IPv6** pages to specify the IP address, subnet mask, default gateway, and DNS addresses for the Content Gateway interface (P1) on the appliance, using the guidelines below. Be sure to click **OK** to save your changes.

General guideline	Ensure that outbound packets can reach the Internet.
IP address (P1 or P2 interface)	Required.
Subnet mask	Required.

Default gateway	Required. The gateway must be in the same subnet as the IP address of the P1 interface. Ensure that outbound packets can reach the Internet.
Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

7. Also use the **Configuration > Network Interfaces IPv4** and **IPv6** pages to specify the IP address, subnet mask, default gateway, and DNS addresses for the Network Agent interface (N) on the appliance. Be sure to click **OK** to save your changes.

   Network Agent continually monitors overall network usage, including bytes transferred over the network. The agent sends usage summaries to other Websense components at predefined intervals.

   Network Agent is typically configured to see both inbound and outbound traffic in your network. The agent distinguishes between:

   - Requests sent from internal machines to internal machines (hits to an intranet server, for example)
   - Requests sent from internal machines to external machines such as web servers (user Internet requests, for example)

   You choose whether blocking information for non-HTTP protocols is routed through interface C or interface N.

Select an interface to use to send blocking information for non-HTTP and HTTPS traffic	- Select **Interface C** only if you want to use interface C to send blocking information. - Select **Interface N** if network interface N is connected to a bidirectional span port, and you want to use N to transport blocking information. Blocking NIC settings configured in the Web Security manager do **not** override the settings you enter in this pane. The settings in Appliance manager take precedence.
IP address of interface N	Required. Network Agent should be able to see the outbound and inbound traffic in your network. Network Agent ignores ports 80, 443, 8070, and 8080.
Subnet mask	Required if interface N is selected for blocking. Otherwise the subnet mask has a fixed value of 255.255.255.255.
Default gateway	Required if interface N is selected for blocking. Otherwise, the field is disabled.

Primary DNS	Required. IP address of the domain name server.
Secondary DNS	Optional. Serves as a backup in case the primary DNS is unavailable.
Tertiary DNS	Optional. Serves as a backup in case the primary and secondary DNSes are unavailable.

8. On the **Configuration** > **Web Security Components** page:
   - Under **Policy Source**, select **Full policy source**. This means that the appliance hosts Policy Broker and Policy Server.
   - Provide the IP address of the Windows server that you will use to host management and reporting components, including the TRITON Unified Security Center.

   When you are finished, click **OK** to save and apply your changes.

Continue with the next section, *Prepare the management and reporting server*.

Prepare the management and reporting server

On the Windows machine that will host your management and reporting components (the TRITON management server):

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. You can use Server Manager to install the appropriate version of .NET Framework.
   - Windows Server 2008 R2: Use version 2.0 or higher.
   - Windows Server 2012: Version 3.5 is required.

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: http://download.microsoft.com/download/D/1/0/D105DCF6-AC6C-439D-8046-50C5777F3E2F/microsoft-.net-3.5-deployment-considerations.docx).

5. Synchronize the clocks on all machines (including appliances) where a Websense 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 Excluding Websense software from antivirus scans.
7. Disable any firewall on the machine before starting the Websense installer and then re-enable it after installation. Open ports as required by the Websense 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 Web Security Default Ports 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.

Create the TRITON management server

The Windows Server 2008 R2 or Windows Server 2012 machine that hosts core management components is called the TRITON management server.

To create your management server:

1. Log on to the machine that you want to use with **local** and **domain** administrator privileges.
2. Stop any antivirus software and close unnecessary applications.
3. Download the TRITON Unified Installer from the Downloads tab of www.mywebsense.com.
4. Right-click the installer executable and select **Run as administrator** to extract the installer files.

   After the files are decompressed, **setup.exe** runs automatically.
5. Click **Next** on the welcome screen, and then accept the subscription agreement.
6. On the Installation Type screen, select **TRITON Unified Security Center**, then mark the **Web Security** check box and click **Next**.
7. On the **Summary** screen, click **Next** to continue the installation.

   TRITON Infrastructure Setup launches.

Install the management components

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

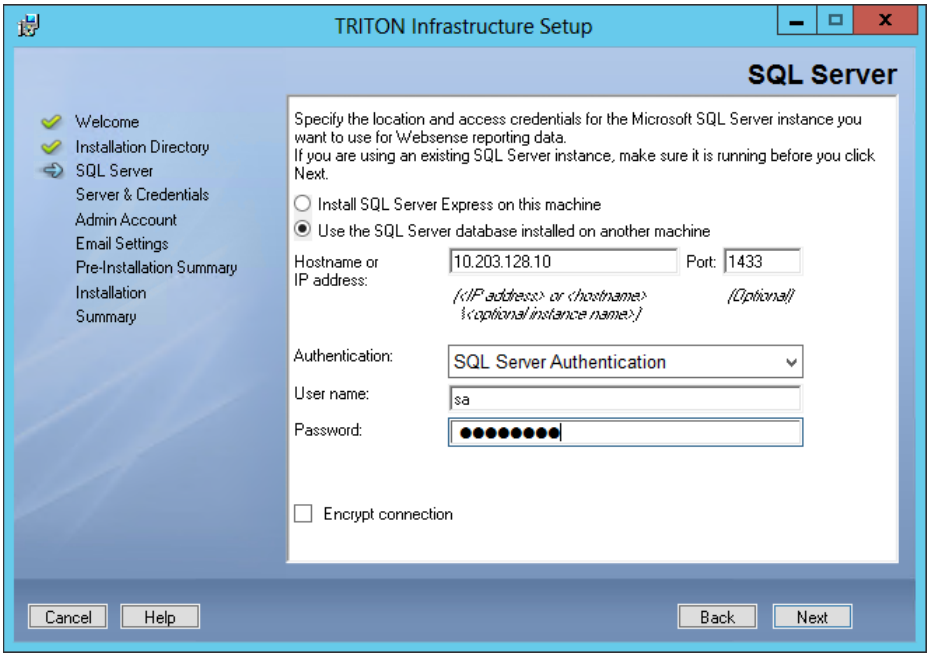
The Web Security module includes configuration, policy management, and reporting tools for Websense Web Security solutions.

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 existing SQL Server on another machine**, then specify the location and connection credentials for a database server located elsewhere in the network.



TRITON Infrastructure Setup

SQL Server

Specify the location and access credentials for the Microsoft SQL Server instance you want to use for Websense reporting data.
If you are using an existing SQL Server instance, make sure it is running before you click Next.

○ Install SQL Server Express on this machine

● Use the SQL Server database installed on another machine

Hostname or IP address: 10.203.128.10 Port: 1433

(<IP address> or <hostname> \<optional instance name>) (Optional)

Authentication: SQL Server Authentication

User name: sa

Password: ●●●●●●●●●

□ Encrypt connection

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 Security manager. See Configuring Websense Apache services to use a trusted connection.

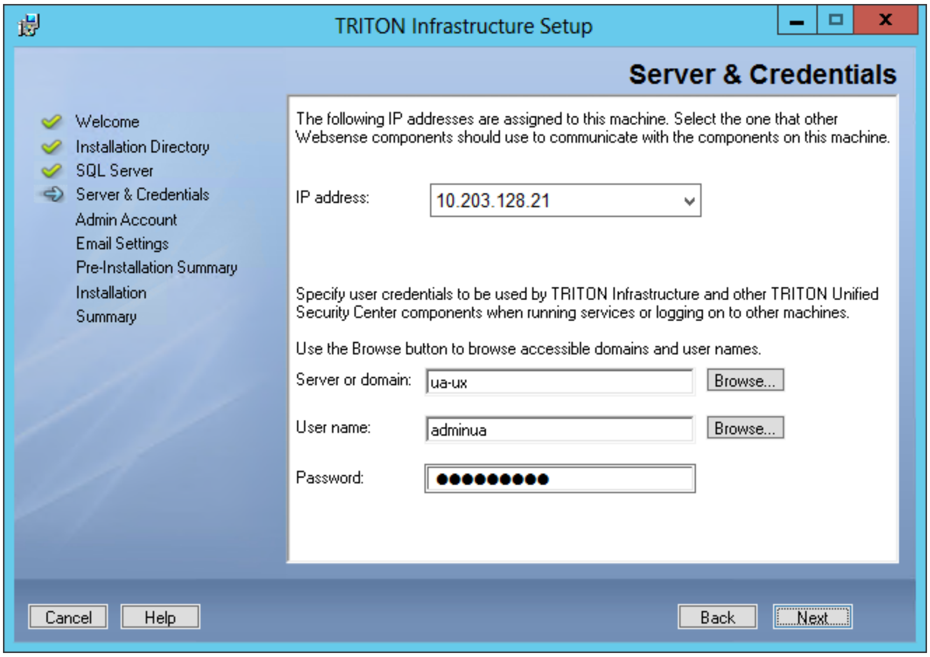
c. Click **Next**. The installer verifies the connection to the database engine. If the connection test is successful, the next installer screen appears.

If the test is unsuccessful, the following message appears:

Unable to connect to SQL
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 Unified Security Center.



Server & Credentials

The following IP addresses are assigned to this machine. Select the one that other Websense components should use to communicate with the components on this machine.

IP address: 10.203.128.21

Specify user credentials to be used by TRITON Infrastructure and other TRITON Unified Security Center components when running services or logging on to other machines.

Use the Browse button to browse accessible domains and user names.

Server or domain: ua-ux

User name: adminua

Password: ●●●●●●●●●

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

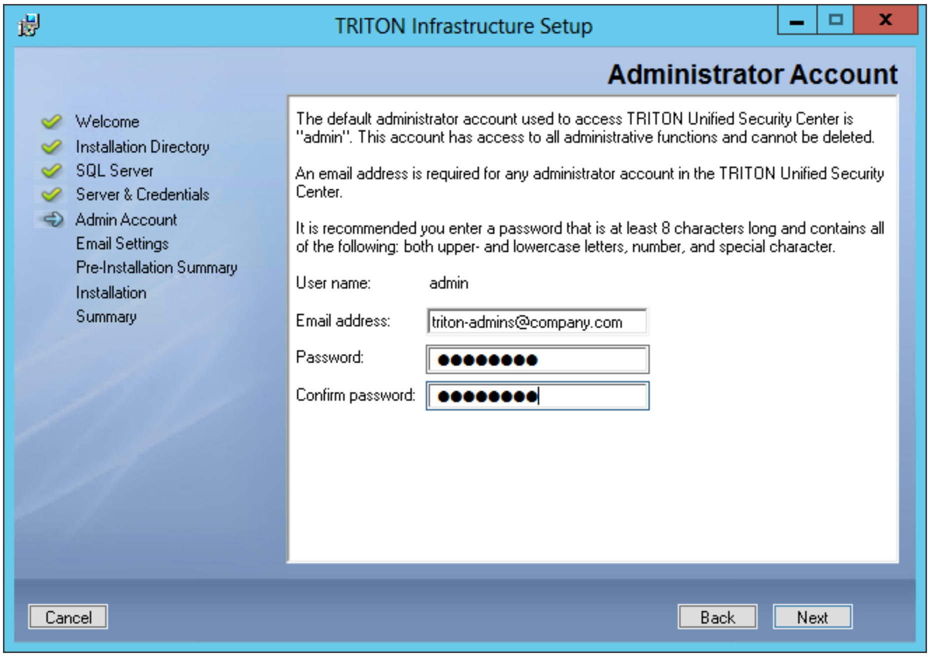
  Administrators will use this address to access the TRITON console (via a web browser), and Websense component on other machines will use the address to connect to the TRITON management server.

- Specify the **Server or domain** of the user account to be used by TRITON Infrastructure and TRITON Unified Security Center. The name cannot exceed 15 characters.

- Specify the **User name** of the account to be used by TRITON Unified Security Center.

- 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**.



Administrator Account

The default administrator account used to access TRITON Unified Security Center is "admin". This account has access to all administrative functions and cannot be deleted.

An email address is required for any administrator account in the TRITON Unified Security Center.

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.

User name: admin

Email address: triton-admins@company.com

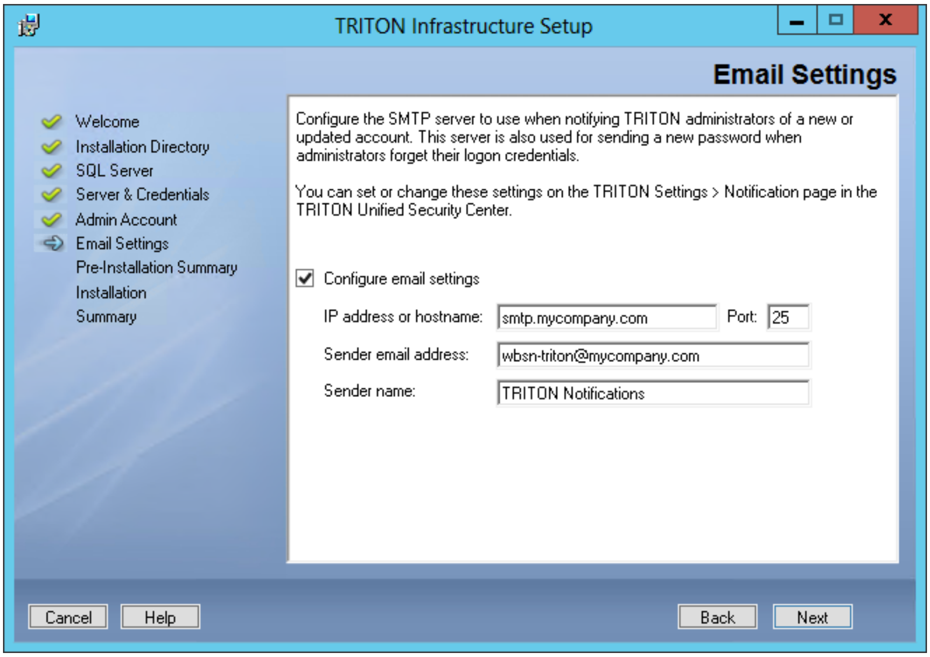
Password: ●●●●●●●●

Confirm password: ●●●●●●●●

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.



Email Settings

Configure the SMTP server to use when notifying TRITON administrators of a new or updated account. This server is also used for sending a new password when administrators forget their logon credentials.

You can set or change these settings on the TRITON Settings > Notification page in the TRITON Unified Security Center.

☑ Configure email settings

IP address or hostname: smtp.mycompany.com Port: 25

Sender email address: wbsn-triton@mycompany.com

Sender name: TRITON Notifications

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 Unified Security Center.

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 ’Websense TRITON Central Access’ (EIPManagerProxy) failed to start. Verify that you have sufficient privileges to start system services.

If port 9443 is in use, release it and then click **Retry** to continue installation.

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

   You are returned to the Installer Dashboard and, after a few seconds, the Web Security component installer launches.

10. On the Select Components screen, select:
    - TRITON - Web Security (selected by default)
    - Real-Time Manager
11. 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.
12. On the Pre-Installation Summary screen, verify the information shown, then click **Next**.
13. A progress screen is displayed. Wait for installation to complete.
14. On the Installation Complete screen, click **Next**.

After the management component have been installed, continue with *Install Websense Log Server*.

Install Websense Log Server

Websense Log Server is the tool that records monitored Internet activity for use by several graphical reporting tools.

In larger deployment, Log Server typically resides on a dedicated Windows server, but smaller sites can install it on the TRITON management server, as described in this section.

Note that before installing Log Server, you must have a supported version of Microsoft SQL Server installed and running in your network, as described in *Prepare for installation*.

1. Relaunch the installer on the machine you just used to install management components.

   Launch the installer from the Start menu (Start > All Programs > Websense > Websense TRITON Setup) or Start screen (Websense TRITON Setup) to save time and avoid having to re-extract the installation files.

2. On the **Modify Installation** screen, click the **Modify** link next to **Web Security**.
3. On the **Add Components** screen, select **Install additional components on this machine** and click **Next**.
4. On the **Select Components** screen, select **Log Server**, and then click **Next**.

5. On the **Policy Server Connection** screen, enter the IP address of the appliance C interface and the Policy Server communication port (55806), then click **Next**.
6. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that Log Server should use for communication, and then click **Next**.
7. 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 Websense 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 Security manager. See Configuring Websense Apache services to use a trusted connection.

   - Select **Database account** 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.

8. 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.

9. 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.websense.com)
     - Category
     - Keyword
     - Action (for example: Category Blocked)
     - User/workstation

10. 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 (x86)\Websense\Web Security\.

Important

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

11. 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.

12. A progress screen is displayed. Wait for the installation to complete.
13. On the Installation Complete screen, click **Next**.
14. After installing Log Server, restart the follow services on the management and reporting 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.

Next, *Enter your subscription key and get started*.

Enter your subscription key and get started

The TRITON Unified Security Center (TRITON console) is the management interface to all Websense TRITON security solutions. Its Web Security module (the Web Security manager) is used to update configuration, manage policies, and generate reports for Websense Web Security solutions. You can access the TRITON console from anywhere in the network.

Each time you open the Web Security manager, you connect to **Policy Server**, the component that handles status communication between Web Security components. Initially, you use a default administrative account, **admin**, to connect to Policy Server.

1. To launch the Web Security manager, launch a supported browser anywhere in the network and go to:

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

    Access to the TRITON console is secured with an SSL security certificate issued by Websense, Inc. Because the browser does not recognize Websense, Inc., as a known Certificate Authority (CA), a security warning is displayed.

    Create an exception or accept the certificate (depending on browser type) to continue to the logon page.

2. On the logon page, enter the user name **admin** and the password that you created during installation, then click **Log On**.
3. The Web Security manager opens, showing the **Initial Setup Checklist**, which prompts you to enter your subscription key as step one.
4. Enter your **Subscription key** exactly as you received it, provide any necessary proxy settings, and then click **Apply**.

   If you have Web Security Gateway, this subscription information is automatically shared with Content Gateway to enable content analysis.
5. Your subscription information is validated and Websense Filtering Service begins to download the Master Database, used to enable policy enforcement.
6. Wait for the first Master Database download to complete, then log off of the TRITON console and log on again.

   Because this initial download results in several updates to the Web Security manager, logging off and logging on again ensures that you are able to access all appropriate configuration options.
7. After the database download is complete, and you have logged back on to the TRITON console, use the Initial Setup Checklist to perform initial policy management tasks, including customizing the Default policy.

   Refer to the *Transition Guide* and its associated worksheets to help in completing these tasks.

Once you have created policies and assigned them to clients, use the tools described in *Assess your implementation* to ensure that Internet requests are being monitored, analyzed, and managed as expected.

Assess your implementation

Websense reporting tools can help you to evaluate the results and overall effectiveness of your filtering policies.

- Identify Internet usage patterns for your organization.
- Investigate unexpected surges or dips in Internet usage.
- Verify that policies are being enforced correctly.
- Identify high-traffic uncategorized sites for investigation and possible recategorization.

Status overview

When you initially log on to the Web Security manager, the **Status** > **Dashboard** page shows charts and tables that provide an overview of Web Security activity in your network.

- Use the **Threats** dashboard to investigate suspicious activity that may be related to malware threats in your network.

- Use the **Risks** dashboard to find information about requests for websites classified as security risks.
- Use the **Usage** dashboard to understand traffic patterns in your network.
- Use the **System** dashboard to review alert messages, status information, and graphical charts showing the current state of your deployment.

Traffic monitor

To visualize current traffic flow through your Web Security solution, use the **Reporting** > **Real-Time Monitor** page. Real-Time Monitor lists URLs with information about:

- The client making the request
- Whether the site was recategorized based on Content Gateway analysis
- Which category was assigned to the site
- Whether the request was permitted or blocked
- The time the request was made

Find detailed information about using Real-Time Monitor in the Web Security Help.

Interactive, drill-down reporting

To drill into reporting data, use the **Reporting** > **Investigative Reports** page. This interactive interface provides summaries of current Internet usage, as well as tools for performing detailed usage analysis. You can:

- Drill down from overviews to more detailed information on Internet activity of particular interest or concern.
- Generate customizable detail reports on specific areas of interest.
- Save and schedule Favorite Reports to run at your convenience.

Find detailed instructions for creating investigative reports in the Investigative Reporting Quick Start.

Graphical and tabular reports

For tables and graphical charts that you can share with other members of your organization, use the **Reporting** > **Presentation Reports** page. Predefined reports make it easy to generate a consistent presentation of data on a particular topic. You can:

- Run reports for specific time frames.
- Copy predefined reports, and edit the filter that determines which clients, categories, protocols, and actions are reported.
- Schedule reports to run at a specific time or on a repeating schedule.

Find detailed instructions for creating presentation reports in the Presentation Reporting Quick Start.

Conclusion

This completes your initial configuration of Websense Web Security or Web Security Gateway. Please refer to the Web Security Help for detailed information about continuing to configure and manage your solution.

Also see Websense Knowledge Base for access to articles, technical papers, video tutorials, and other resources that you can use to make the most of your Websense software.