



WebSense Web Security Gateway ThreatVision Setup Guide

v7.7.3

©1996–2013, Websense Inc.

All rights reserved.

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2013

Printed in the United States and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense is a registered trademark and TRITON is a trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation in the United States and/or other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

This product includes software distributed by the Apache Software Foundation (<http://www.apache.org>).

Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

Chapter 1	Introducing Web Security Gateway ThreatVision	1
	ThreatVision restrictions in this version	1
	Setup process overview	2
Chapter 2	Set Up the Appliance	5
	Step 1: Set up the appliance hardware	6
	Step 2: Run the firstboot script	7
	Step 3: Configure basic appliance settings	9
	Step 4: Configure network interfaces	10
	Step 5: Configure Web Security component interaction	11
	Step 6: Enable the ThreatVision hotfix	11
Chapter 3	Create a Management Server	13
	Step 1: Download the installer and start installation	13
	Step 2: Install TRITON Infrastructure	14
	Step 3a: Install Web Security management components	18
	Step 3b (optional): Install Data Security management components ...	19
	Step 4: Enter a key and download the Master Database	20
Chapter 4	Configure Monitor Mode	21
	Step 1: Configure Content Gateway analysis	21
	Step 2a: Customize Internet access policies	23
	Step 2b (optional): Configure Web DLP policies	24
	Step 3: Configure reporting behavior	25
	Step 4 (optional): Configure the monitor port	25

1

Introducing Web Security Gateway ThreatVision

Monitor Appliance Setup | Web Security Gateway | v7.7.3

In evaluation or proof of concept deployments, Websense® V10000 Appliances running Websense TRITON™ Web Security Gateway or Gateway Anywhere can be configured to monitor traffic using a span port.

This allows organizations to prove the advantages offered by Websense Content Gateway, Web DLP (in Gateway Anywhere deployments) and the Websense ACE analytics that it uses to evaluate Internet requests.

- ◆ Traffic (requests and responses) monitored by the solution is analyzed in real time by Content Gateway.
- ◆ The results of the analysis are logged, and appear in reports and Real-Time Monitor.
- ◆ Administrators can configure Web Security policies to find out how they would be applied, were the proxy deployed in enforcement mode.
- ◆ Administrators can configure suspicious activity alerts and usage alerts to allow them to respond to any troubling activity that is monitored.



Warning

Websense Content Gateway proxy authentication must **not** be enabled in Web Security Monitor deployments.

ThreatVision restrictions in this version

In version 7.7.3, Web Security Gateway ThreatVision has the following restrictions:

- ◆ No requests are blocked.
- ◆ If the administrator configures policies that include blocked categories, Web Security reporting tools show requests as blocked, even though no actual blocking has occurred.
- ◆ If the administrator sets up Web DLP policies that include blocking:
 - Data Security incident reports show blocked requests (even though no actual blocking occurred).
 - Web Security Real-Time Monitor shows the requests as permitted.

- Web Security investigative reports show the action applied to the requests as “Not Available” (neither permitted nor blocked).

Note that the forensics repository does store files associates with Web DLP incidents.

- ◆ In a standard Web Security Gateway deployment, if Filtering Service blocks a request based on its static (Master Database) category, the request does not go to Content Gateway for analysis. In other words, even with aggressive scanning enabled, URLs are only analyzed if they are permitted by the initial Filtering Service lookup.

As a result of this standard behavior, when Web Security Monitor is enabled, if a policy “blocks” a request before the request is sent to the analytics, subsequent requests by the user for content internal to that website (for example, clicking through content on the site) may not appear in reports.

This happens because Content Gateway does not know that the “block” is virtual. It acts as though a block page was sent, and closes its connection to the request.

- ◆ The Web Security Monitor option is available only for the V10000 Appliance.
- ◆ Disabling monitor mode requires reimaging the appliance.
- ◆ Only HTTP traffic is supported (not FTP or HTTPS).
- ◆ SSL decryption is not available in this mode.
- ◆ A single TRITON console **cannot** support both monitor mode and enforcement mode appliances.
- ◆ Network Agent protocol monitoring is not included at this time.
- ◆ VLAN tagging is not supported.

Setup process overview

The installation and deployment process for monitor mode has 3 basic stages, broken into a series of steps. Use this guide to ensure that you complete the entire process.

1. *Set Up the Appliance*
 - *Step 1: Set up the appliance hardware*
 - *Step 2: Run the firstboot script*
 - *Step 3: Configure basic appliance settings*
 - *Step 4: Configure network interfaces*
 - *Step 5: Configure Web Security component interaction*
 - *Step 6: Enable the ThreatVision hotfix*
2. *Create a Management Server*
 - *Step 1: Download the installer and start installation*
 - *Step 2: Install TRITON Infrastructure*
 - *Step 3a: Install Web Security management components*
 - *Step 3b (optional): Install Data Security management components*

- *Step 4: Enter a key and download the Master Database*
- 3. *Configure Monitor Mode*
 - *Step 1: Configure Content Gateway analysis*
 - *Step 2a: Customize Internet access policies*
 - *Step 2b (optional): Configure Web DLP policies*
 - *Step 3: Configure reporting behavior*
 - *Step 4 (optional): Configure the monitor port*

2

Set Up the Appliance

Monitor Appliance Setup | Web Security Gateway | v7.7.3

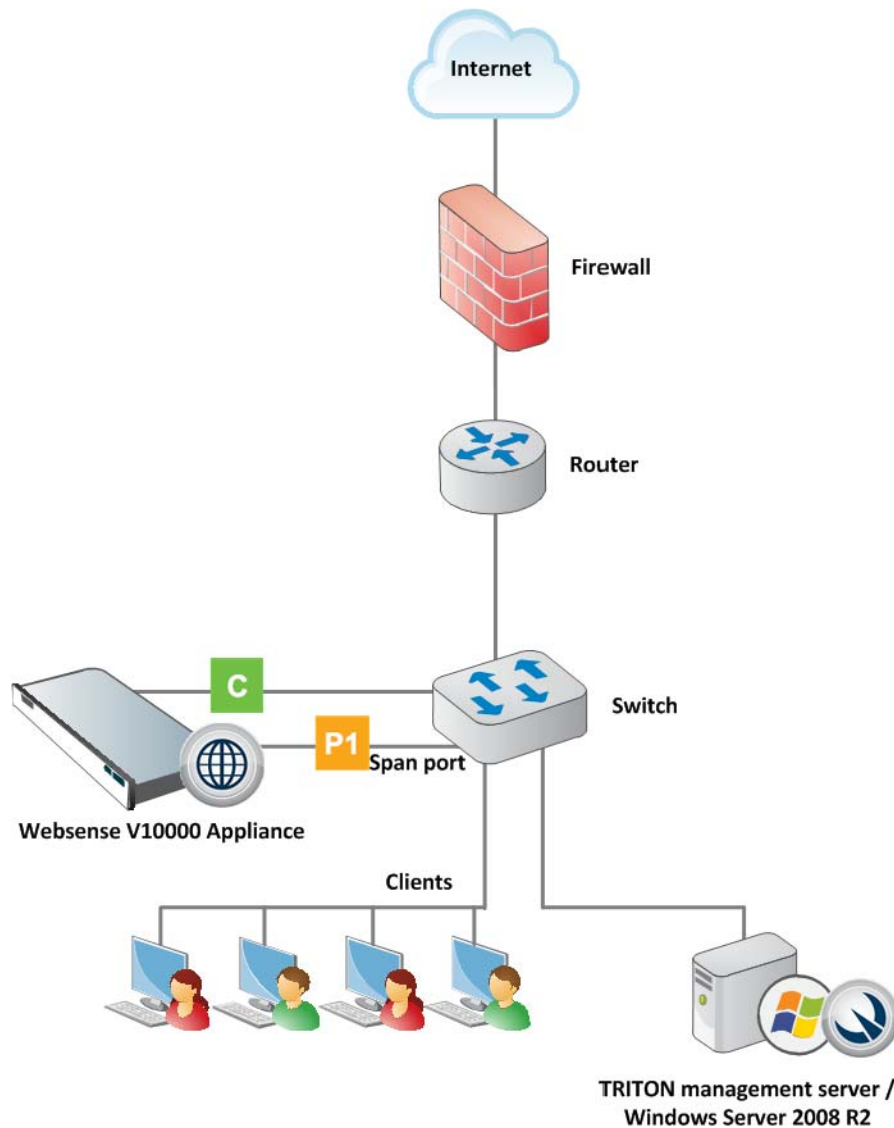
To deploy Websense® Web Security Gateway ThreatVision on a Websense V10000 Appliance, start by setting up the appliance hardware and performing basic appliance configuration, as outlined below.

- ◆ *Step 1: Set up the appliance hardware* (rack and cable the appliance).
- ◆ *Step 2: Run the firstboot script* (activates the appliance).
- ◆ *Step 3: Configure basic appliance settings* (set date and time, and add an appliance description).
- ◆ *Step 4: Configure network interfaces* (verify the settings for the C interface, and assign an IP address to the P1 interface).
- ◆ *Step 5: Configure Web Security component interaction* (verify which components run on the appliance).

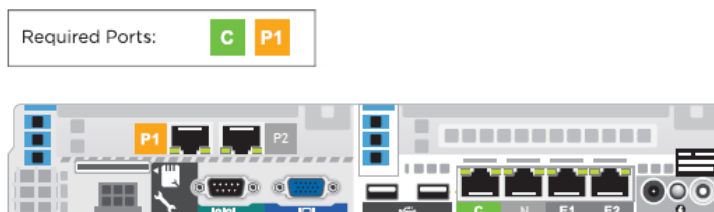
Once the appliance is racked, connected, and configured, continue to the next sections of this guide to *Create a Management Server* and *Configure Monitor Mode*.

Step 1: Set up the appliance hardware

The diagram below gives a simple overview of a Web Security Gateway ThreatVision deployment. In addition to the V10000 Appliance, a Windows Server 2008 R2 machine is required to host management and reporting components.



Connect the C and P appliance interfaces as described below. Cat 5E cables (or better) are required. Do not use crossover network cables.



Network **interface C** provides communication for appliance modules and handles database downloads. The interface:

- ◆ Must be able to access a DNS server
- ◆ Has continuous access to the Internet

Ensure that interface C is able to access the download servers at **download.websense.com**. This URL must be permitted by all firewalls, proxy servers, routers, or host files controlling the URLs that the C interface can access.

Network **interface P1** connects to a span port on the switch to allow Websense Content Gateway to monitor client Internet requests.

Step 2: Run the firstboot script

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports.



An activation script, called **firstboot**, runs when you start the appliance. The firstboot script prompts you to:

- ◆ 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.

Later, if you want to change settings (except the security mode), you can do so through the Appliance Manager user interface.

To change the security mode, re-image the appliance with the image from the Websense Downloads site, and then run the **firstboot** script again.

Gather the following information before running the script.

Security mode	Web
Which Web Security subscription?	Choose one: Web Security Gateway Web Security Gateway Anywhere
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.	
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) <i>Optional</i>	
Tertiary DNS server for network interface C (IP address) <i>Optional</i>	
Password (8 to 15 characters, at least 1 letter and 1 number) This password is for the following: <ul style="list-style-type: none"> • Appliance Manager • Content Gateway Manager 	
Send usage statistics?	Usage statistics from appliance modules can optionally be sent to Websense to help improve the accuracy of filtering and categorization.

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**

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 launch the **firstboot** activation script.
To rerun the script manually, enter the following command:

```
firstboot
```
4. At the first prompt, select **Web** as the security mode.
5. Follow the on-screen instructions to provide the information collected in the table above.

After the script finishes running, continue with the next section,

Step 3: Configure basic appliance settings

Appliance Manager is a Web-based interface for the appliance. Use it to view system status, configure network and communication settings, and perform general appliance administration.

1. Open a supported browser (Internet Explorer 8 or 9, Firefox 5 and later, or Google Chrome 13 and later), and enter the following URL in the address bar:

```
https://<IP-address-of-C-interface>:9447/appmng
```
2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. Use the left navigation pane to go to the **Configuration > System** page.
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.

- 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.
The description is displayed in the appliance list in the TRITON Unified Security Center when the appliance is added there.
 6. Click **OK** to save your changes.

Step 4: Configure network interfaces

Still in Appliance Manager:

1. Navigate to the **Configuration > Network Interfaces IPv4 and IPv6** pages.
2. Specify the IP address, subnet mask, default gateway, and DNS address for the P1 interface.
 - Correct DNS settings are essential for the Web Security Monitor to function.
 - While entries for the IP address, mask, and default gateway fields are required by the user interface, you can enter any valid settings. Because the NIC is used only for monitoring, the IP address settings are not functionally important.
3. **Disable** the P2 interface.



Important

Do **not** make configuration changes on the Network Interfaces pages after enabling Web Security Monitor. Once monitoring is enabled, changes to your NIC configuration will prevent the product from functioning correctly.

Step 5: Configure Web Security component interaction

Still in Appliance Manager:

1. Navigate to the **Configuration > Web Security Components** page to specify which Web Security components are active on the appliance, and where the appliance gets Web Security global configuration and Internet access policy information.
2. Under Policy Source, select **Full policy source**.
This means that it hosts Websense Policy Broker, which is responsible for global configuration and policy management information.
3. Click **OK** to save and apply your changes.
4. Under **TRITON - Web Security**, specify that the TRITON console is installed **Off** the appliance (on a separate Windows machine).
5. Click **OK** to save and apply your changes.

Step 6: Enable the ThreatVision hotfix

To enable Web Security Gateway ThreatVision, upload the hotfix to the appliance and enable “monitor mode” as follows:

1. Open Appliance Manager in a supported browser. The URL is:
`https://<IP-address-of-C-interface>:9447/appmng`
2. Navigate to the **Administration > Patches / Hotfixes > Hotfixes** page.
3. Click **Upload Hotfix Manually** to retrieve the hotfix file from a network location.
4. Click **Install** to initiate hotfix installation.
5. Wait until hotfix application is complete.
6. Connect the **appliance P1 interface** to a span port on the switch that mirrors the client traffic that you want to monitor during the evaluation or proof of concept period.
7. Use SSH to connect to the **appliance C interface** and log on using your Appliance Manager logon credentials when prompted.
8. Enter the following command:
`monitor enable`
9. Close the SSH session, then use SSH to open a new connection to the appliance C interface.
10. To verify that the appliance has successfully enabled monitor mode, enter the following command:

`monitor status`

If the status does not show that monitor mode has been enabled, you may need to restart the appliance and try again.

After enabling monitor mode, continue to the next section to create a TRITON management server.



Important

Do **not** make configuration changes on the Network Interfaces pages after enabling Web Security Monitor. Once monitoring is enabled, changes to your NIC configuration will prevent the product from functioning correctly.

3

Create a Management Server

Monitor Appliance Setup | Web Security Gateway | v7.7.3

After performing initial appliance configuration, install management and reporting components on a Windows Server 2008 R2 machine. There are 4 steps involved in the process:

- ◆ *Step 1: Download the installer and start installation*
- ◆ *Step 2: Install TRITON Infrastructure*
- ◆ *Step 3a: Install Web Security management components*
- ◆ *Step 3b (optional): Install Data Security management components*
- ◆ *Step 4: Enter a key and download the Master Database*

Before you begin:

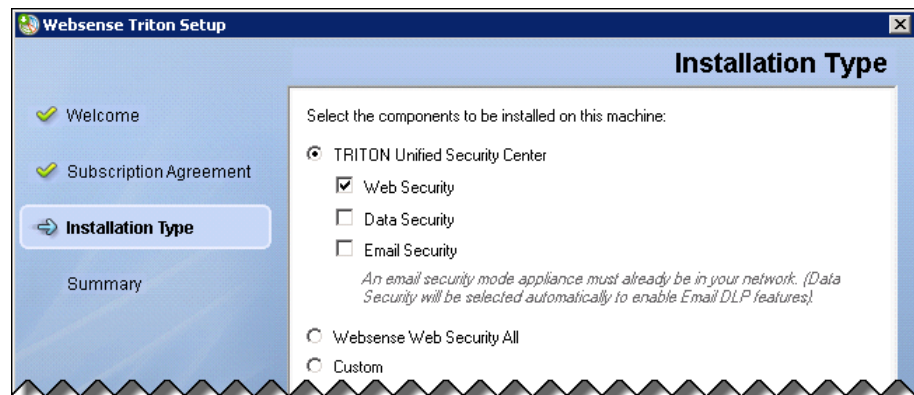
- ◆ Make sure all Microsoft updates have been applied on the Windows Server 2008 R2 machine. There should be no pending updates, especially any requiring a restart of the system.
- ◆ .NET Framework version 2.0 or higher is required to run the Windows installer. If .NET 2.0 is not already installed, it is available from www.microsoft.com.
- ◆ Disable any antivirus software on the machine prior to installing Websense components. Be sure to re-enable antivirus after installation.
- ◆ Synchronize the clocks on all machines where a Websense component is installed. It is a good practice to point the machines to the same Network Time Protocol server.

Once the management server has been created, continue to the final section of this guide to *Configure Monitor Mode*.

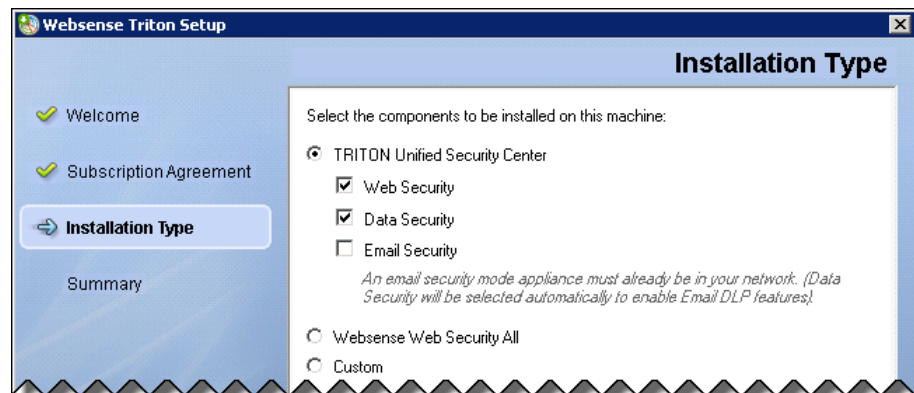
Step 1: Download the installer and start installation

1. Download the **Websense Web Security Gateway - Windows** installer from the **Downloads** tab of mywebsense.com.
 - The file name is **WebsenseTRITON773Setup.exe**.
 - The version is **7.7.3**.
 - When extracted, the installation files occupy about 2 GB of disk space.

2. Double-click the installer executable to launch the **Websense TRITON Setup** program.
A progress dialog box is displayed as files are extracted. This may take a few minutes.
3. On the **Welcome** screen, click **Start**.
4. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.
5. On the **Installation Type** screen, select **TRITON Unified Security Center**, then:
 - **Web Security Gateway**: Mark the **Web Security** check box.



- **Web Security Gateway Anywhere**: Mark the **Web Security** and **Data Security** check boxes.



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

6. On the **Summary** screen, click **Next** to continue the installation.
The TRITON Infrastructure Setup program launches. Continue with the next section.

Step 2: Install TRITON Infrastructure

TRITON Infrastructure is the platform on which Websense TRITON management components are built. When the infrastructure components have been installed, the

Web Security installer launches automatically to install the Web Security management components.

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**.



Important

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

3. On the **SQL Server** screen, specify the location of your database engine and the type of authentication to use for the connection. Also specify whether to encrypt communication with the database.
 - Select **Use existing SQL Server on this machine** if the Websense installer has already been used to install SQL Server 2008 R2 Express on this machine.
 - Select **Install SQL Server Express on this machine** to install SQL Server 2008 R2 Express on this machine.

When this option is selected, .NET 3.5 SP1, Powershell 1.0, and Windows Installer 4.5 are installed automatically if they are not found on the machine. These are required for SQL Server 2008 R2 Express.

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

In some cases, you are prompted to reboot the machine after installing SQL Server Express. If you do, go to **Start > All Programs > Websense > Websense TRITON Setup** to restart the installer.

- Select **Use existing SQL Server on another machine** to specify the location and connection credentials for a database server located elsewhere in the network.

Enter the **Hostname or IP address** of the SQL Server machine, including the instance name, if any.

- If you are using a named instance, the instance must already exist.
- If you are using SQL Server clustering, enter the virtual IP address of the cluster.

Also provide the **Port** used to connect to the database (1433, by default).

After selecting one of the above options, specify an authentication method and account information:

- Select the **Authentication** method to use for database connections: **SQL Server Authentication** (to use a SQL Server account) or **Windows Authentication** (to use a Windows trusted connection).

Next, provide the **User Name** or **Account** and its **Password**. This account must be configured to have system administrator rights in SQL Server. If you are using SQL Server Express, **sa** (the default system administrator account) is automatically specified (this is the default system administrator account).

When you click **Next**, connection to the database engine is verified. 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.
 - Select an **IP address** for this machine. If this machine has a single network interface card (NIC), only one address is listed.
 - Specify the **Server or domain** of the user account that you want to use to run the TRITON Infrastructure and TRITON Unified Security Center services. The server/host name cannot exceed 15 characters.
 - Specify the **User name** of the account that you want to use to run the TRITON Unified Security Center services.
 - 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**.

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

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

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

**Warning**

If you chose to install SQL Server Express, depending on whether certain Windows prerequisites are installed, your machine may be automatically restarted up to two times during the installation process. Restarts are not required if the prerequisites are already installed.

**Note**

When you click **Next**, if you chose to install SQL Server Express on this machine, it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

8. If you chose to install SQL Server Express, .NET Framework 3.5 SP1, PowerShell 1.0, and Windows Installer 4.5 will be installed if not already present. Wait for Windows to configure components.
 - a. If the following message appears during this process, click **OK**:

Setup could not restart the machine. Possible causes are insufficient privileges, or an application rejected the restart. Please restart the machine manually and setup will restart.
 - b. Websense installer starts again. In the TRITON Infrastructure Setup **Welcome** screen, click **Next**.
 - c. The **Ready to Resume EIP Infra installation** screen appears. Click **Next**.

**Note**

When you click **Next**, if you chose to install SQL Server it may take a couple minutes for the next screen to appear. Wait for the next screen, then see the next step below.

9. If you chose to install SQL Server Express on this machine, SQL Server 2008 R2 Setup is launched. Wait for it to complete.

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

Note that it may take approximately 10-15 minutes for the SQL Server 2008 R2 Express installation to complete.
10. Next, the **Installation** screen appears. Wait until all files have been installed.

If the following message appears, check whether 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.

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

The TRITON Infrastructure Setup program closes and the Web Security component installer launches. Continue with the next section.

Step 3a: Install Web Security management components

1. On the **Select Components** screen, select the following components to install, and then click **Next**.
 - **TRITON - Web Security**
 - **Web Security Log Server**
 - *Web Security Gateway Anywhere only* (optional): **Sync Service**
 - *Web Security Gateway Anywhere only*: **Linking Service**
 - **Real-Time Monitor**
2. On **Policy Server Connection** screen, enter the IP address and port used by Policy Server (the IP address of the **appliance C interface** and **55806**, by default). When you are finished, click **Next**.
3. If you selected Sync Service for installation, use the **Policy Broker Connection** screen to enter the IP address and port used by Policy Broker (the IP address of the **appliance C interface** and **55880**, by default). When you are finished, click **Next**.
4. Use the **Log Database Location** screen to specify the IP address or hostname of the SQL Server instance that will host the Log (reporting) Database (if necessary), and provide a path for the database files. When you are finished, click **Next**.
5. On the **Optimize Log Database Size** screen, select **Log Web page visits**.

This results in fewer log records for each URL by combining information for secondary elements on a website (like graphics) into a single record. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities.

When you are finished, click **Next**.
6. If you selected Linking Service for installation, on the **Filtering Service Communication** screen, provide the IP address and port used by Filtering Service (the IP address of the **appliance C interface** and **15868**, by default). When you are finished, click **Next**.
7. On the **Pre-Installation Summary** screen, verify the information shown.

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

8. Click **Next** to start the installation. The **Installing Websense** progress screen is displayed. Wait for installation to complete.
9. On the **Installation Complete** screen, click **Next**.

For Web Security Gateway, installation of off-appliance components is complete. Continue with [Step 4: Enter a key and download the Master Database](#), page 20.

For Web Security Gateway Anywhere, continue with the next section to install Data Security management components.

Step 3b (optional): Install Data Security management components

Web Security Gateway Anywhere subscriptions include data loss prevention over web channels (Web DLP), configured in the Data Security module of the TRITON console.

To install the Data Security management components:

1. When the Data Security component installer launches, and the Welcome screen is displayed click **Next**.
2. On the Select Components screen, accept the defaults and click **Next**.
3. If prompted, click **OK** to accept that services such as ASP.NET and SMTP will be enabled.
4. On the Fingerprinting Database screen, accept the default location or click **Browse** to specify a different location (local path only).
5. If your SQL Server database is on a remote machine, use the Temporary Folder Location Screen to provide the name of a folder to use for temporary files created during archive processing and system backup and restore. Also indicate:
 - Whether to **Enable incident archiving and system backup** to archive old or aging incidents and perform system backup or restore.
 - Use the **From SQL Server** field to enter the UNC path that the SQL Server should use to access the temporary folder. Make sure the account used to run SQL has write access to this folder.
 - Use the **From TRITON Management Server** field to enter the UNC path the management server should use to access the temporary folder. Enter a user name and password for a user who is authorized to access this location.
6. In the Installation Confirmation screen, click **Install** to begin installing Data Security components.
7. If the following message appears, click **Yes** to continue the installation:

Data Security needs port 80 free.
In order to proceed with this installation, DSS will free up this port.
Click Yes to proceed OR click No to preserve your settings.

A similar message for port 443 may appear. Click **Yes** to continue.

8. The Installation progress screen appears. Wait for the installation to complete.
When the Installation Complete screen appears, click **Finish** to close the Data Security installer.

You have completed installation of the TRITON management server. Continue with the next section to enter a subscription key and activate your Web Security software.

Step 4: Enter a key and download the Master Database

After the management server installation is complete, log on to the TRITON console and enter your Web Security Gateway or Gateway Anywhere subscription key.

1. Open a supported browser (Internet Explorer 8 or 9, Firefox 5 and later, or Google Chrome 13 and later), and enter the following URL in the address bar:

`https://<IP-address-of-management server>:9443/triton/`

2. Enter the user name **admin** and the password set during installation, then click **Log On**.

You are logged on to the TRITON console and automatically connected to the Web Security management module.

3. A pop-up window prompts you to enter your subscription key. If Internet requests originating from the **appliance C interface** must go through a proxy to reach the Internet, provide the proxy details at the same time you enter the key, and before clicking **OK**.
4. Go to the **System** tab of the **Status > Dashboard** page to monitor the progress of the Master Database download.
5. When the download is complete, log off of the TRITON console and continue with the next section of this document.

4

Configure Monitor Mode

Monitor Appliance Setup | Web Security Gateway | v7.7.3

After setting up the Websense® V10000 Appliance and creating a TRITON™ management server, you are ready to use ThreatVision to begin monitoring traffic. This involves the following steps:

- ◆ *Step 1: Configure Content Gateway analysis*
- ◆ *Step 2a: Customize Internet access policies*
- ◆ *Step 2b (optional): Configure Web DLP policies*
- ◆ *Step 3: Configure reporting behavior*
- ◆ *Step 4 (optional): Configure the monitor port*

Step 1: Configure Content Gateway analysis

This section describes which analysis options to enable to best demonstrate the capabilities offered by Content Gateway and its analytics. Note, however, that even in this configuration, not all traffic may be sent to the proxy for analysis.

- ◆ If any policies that you configure (including the Default policy) use only the Monitor Only filters, all traffic will go to the proxy, but reports will not show any blocked requests.

This means that you will not be able to see the blocking capabilities of the full (enforcement mode) solution.

- ◆ If your policies enforce filters that block categories (as instructed in the next section), any requests blocked **before analysis** (that is, any requests for URLs assigned to Master Database categories blocked by the filter) are not forwarded to the proxy (just as in enforcement mode).

In other words, even though no actual block occurs, the request is treated **as if it had been blocked** based on Master Database categorization, and no further analysis is performed.

This mirrors the way that Web Security Gateway (Anywhere) functions in enforcement mode.

To configure how Content Gateway analyzes traffic:

1. Log on to the TRITON console as **admin**, using the password created during installation and select the Web Security module (if needed).

2. Select the **Settings** tab of the left navigation page, then navigate to the **Scanning > Scanning Options** page.
3. Under Content Categorization, make sure that the **On** radio button is selected, and that the **Analyze links embedded in Web content...** check box is marked.

Content Categorization

Analyze content to categorize sites not in the Master Database and dynamic Web 2.0 sites identified by Websense Security Labs.

☐ Off
☒ On (default)

☒ Analyze links embedded in Web content as part of content categorization

Content categorization sensitivity can be controlled under Advanced Options below

4. Under Tunneled Protocol Detection, make sure that the **On** radio button is selected.
5. Under Security Threats: Content Security, make sure that the **On** radio button is selected, and the **Aggressive analysis...** check box is marked.

Security Threats: Content Security

Analyze Web content in incoming traffic and block malicious content, such as phishing, malware, and viruses.

☐ Off
☒ On - Perform advanced security analysis on content from sites with elevated risk profiles (recommended by Websense Security Labs) (default)

☒ Aggressive analysis - Perform advanced security analysis for sites with elevated risk profiles and sites with lower risk profiles (may consume additional system resources)

Analytic sensitivity can be controlled under Advanced Options below

6. Under Security Threats: File Analysis:
 - Under Advanced Detection, make sure that the **On** radio button is checked, and the **Aggressive analysis...** check box is marked.
 - Under Antivirus Scanning, make sure that the **On** radio button is checked, and the **Aggressive analysis...** check box is marked.

Security Threats: File Analysis

Advanced Detection

Analyze files that users attempt to download or open remotely and block malicious files.

☐ Off
☒ On - Perform advanced security analysis on files from sites with elevated risk profiles (recommended by Websense Security Labs) (default)

☒ Aggressive analysis - Perform advanced security analysis for sites with elevated risk profiles and sites with lower risk profiles (may consume additional system resources)

Specific file types to scan can be configured under File Type Options

Antivirus Scanning

Analyze files that users attempt to download or open remotely and block virus-infected files.

☐ Off
☒ On - Perform advanced security analysis on files from sites with elevated risk profiles (recommended by Websense Security Labs) (default)

☒ Aggressive analysis - Perform advanced security analysis for sites with elevated risk profiles and sites with lower risk profiles (may consume additional system resources)

Specific file types to scan can be configured under File Type Options

- Expand the **File Type Options** button, then mark all of the file type check boxes.

File Type Options

Specify the types of files to scan:

- ☒ Suspicious files, as identified by Websense Security Labs (default)
- ☒ Executable files (default)
- ☒ Unrecognized files (default)
- ☒ Image files (this option is resource intensive)
- ☒ Multimedia files (MPEG, RealMedia)
- ☒ Documents and office-related files (spreadsheets, word processing files, PDFs)
- ☒ Files with the following extensions:

Add

Enter extensions separated by commas. For example: gz, cad, js

.ex_


.1

Delete

- Under Outbound Scanning, make sure that both the **Analyze for and block outbound security threats...** and **Data theft protection** check boxes are marked.

Outbound Scanning

- ☒ Analyze for and block outbound security threats (and enable Social Web Controls if Content Security is enabled) (default)
For each Security Threats scanning option enabled above, outbound security will also be enabled. Does not apply to rich Internet applications embedded in Web content.
- ☒ Data theft protection (default)
Analyzes outbound content for sensitive data (for example, encrypted files or password files) and blocks sensitive content. Information from this scan is used in the Threats dashboard, and in logs and reports.

Advanced Options 

- Click **OK** to cache your changes, then click **Save and Deploy** to implement them.
- Next, optionally customize your Web Security policies.

Step 2a: Customize Internet access policies

In monitor mode, creating custom policies enables reporting tools to show how requests would be handled by Websense Web Security Gateway (Anywhere) in enforcement mode. Regardless of how strict the policies are that you create, no requests are blocked while the deployment is in monitor mode.

Web Security Gateway includes a **Default** policy, in effect 24 hours a day, 7 days a week. This policy is applied to all requests from clients that do not have any other policy assigned. Initially, this policy is configured to use the **Monitor Only** category filter, which permits all Internet requests.

As a best practice, configure the Default policy to enforce the **Basic** category filter, then update the filter to block 4 additional categories, as described below:

1. In the Web Security module of the TRITON console, navigate to the **Policy Management > Policies** page.
2. Click the **Default** link to open the Default policy for editing.
3. Expand the Category / Limited Access Filter list and select **Basic**.
The Category Filter box (under the Policy Definition box) updates to show which categories the Basic category filter blocks and permits.
4. Scroll down to the **Extended Protection** parent category in the category list and expand it to see its child categories.
5. Select **Dynamic DNS**, then click **Block**.
6. Scroll down to the **Productivity** parent category and expand it, then select **Freeware and Software Download** and click **Block**.
7. Scroll down to the **Security** parent category and expand it, then:
 - Select **Malicious Embedded Link** and click **Block**.
 - Select **Suspicious Embedded Link** and click **Block**.
8. Click **OK** to cache your changes, then click **Save and Deploy** to implement them.

In addition to modifying the Default policy, you can:

- ◆ Create additional, custom policies.
- ◆ Define specific clients (IP addresses or IP address ranges) and apply different policies to different clients or groups of clients.

Step 2b (optional): Configure Web DLP policies

If you have installed Websense Web Security Gateway Anywhere, configure Web DLP policies in the Data Security manager to compliment your Web Security policies.

1. Select the Data Security module of the TRITON console.
2. On the Main tab, navigate to the **Policy Management > DLP Policies > Web DLP Policy** page. A quick-start Web DLP policy is provided.
3. On the Attributes tab, select and enable the attributes to monitor—for example uploaded file type. Configure properties for those attributes. When the settings you configure are matched, the policy is triggered.
See the Data Security Help for instructions.
4. Select the **Destination** tab, then specify the websites where you do not want your data sent. See the Data Security Help for instructions.
5. Select the **Policy Owners** tab, then identify an owner for the policy. See the Data Security Help for instructions.
5. Click **OK**.

Step 3: Configure reporting behavior

To record detailed information about the URLs that users request, enable full URL logging.

1. In the Web Security module of the TRITON console, navigate to the **Settings > Reporting > Log Database** page.
2. Scroll down to the **Full URL Logging** section.
3. Select the **Record domain and full URL of each site requested** radio button.
4. Click **OK** to cache your changes, then click **Save and Deploy** to implement them.

Step 4 (optional): Configure the monitor port

If you need to monitor traffic on a port other than the default (port 80), configure the custom port in Content Gateway Manager. This is not a recommended configuration in this version.

1. Log on to Content Gateway Manager.
2. Select the **Configure** tab and navigate to the **Networking > ARM** page.
3. Click **Edit File**.
4. In the selection box at the top of the page, select the connection that you want to change (the rule using port 80).
5. Change the **Destination Port** value to the port you want to use.
6. Click **Apply**, then click **Close** to return to the ARM page.
7. Click **Apply** again to implement the change.

