



# Installation Guide

Websense<sup>®</sup> TRITON<sup>™</sup> Enterprise

**v7.8.x**

©1996–2014, Websense, Inc.  
All rights reserved.  
10240 Sorrento Valley Rd., San Diego, CA 92121, USA  
Published 2014

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.

# Contents

<b>Topic 1</b>	<b>Preparing for TRITON Enterprise Deployment . . . . .</b>	<b>1</b>
	Deployment overview . . . . .	1
	Remote office and off-site users . . . . .	4
	Hybrid services . . . . .	4
	Websense appliances . . . . .	4
	Data Security Protector . . . . .	4
	Components that may not be installed on Websense appliances . . . . .	5
	TRITON management server . . . . .	5
	Web Security and Email Security Log Server . . . . .	5
	Optional Web Security components . . . . .	5
	Data Security Agents . . . . .	5
	Data Endpoint (User Machine) . . . . .	5
	Third-party components . . . . .	5
	Microsoft SQL Server . . . . .	5
	Mail server . . . . .	6
	Deployment details by TRITON Enterprise module . . . . .	6
	Web Security Gateway Anywhere . . . . .	6
	Data Security . . . . .	6
	Email Security Gateway . . . . .	6
	Installation overview . . . . .	6
	Requirements . . . . .	7
	Reporting database . . . . .	7
	TRITON Management Server . . . . .	8
	Hardware requirements . . . . .	8
	TRITON console browser support . . . . .	9
	Virtualization systems . . . . .	9
	Directory services for administrator authentication . . . . .	10
	Preparing servers for TRITON Enterprise deployments . . . . .	10
	Windows . . . . .	10
	Linux . . . . .	11
<b>Topic 2</b>	<b>Installing TRITON Management Components . . . . .</b>	<b>13</b>
	Installing the Web Security policy source . . . . .	13
	Creating the TRITON Management Server . . . . .	14
	Step 1: Download the TRITON Unified Installer . . . . .	15
	Step 2: Select management components . . . . .	15
	Step 3: Install the TRITON Infrastructure . . . . .	17
	Step 4: Install Web Security management components . . . . .	22

	Policy Server Connection screen . . . . .	24
	Policy Broker Connection screen. . . . .	24
	Filtering Service Communication screen. . . . .	24
	Completing the installation . . . . .	25
	Step 5: Install Data Security management components . . . . .	25
	Step 6: Install Email Security management components . . . . .	28
<b>Topic 3</b>	<b>Installing Additional Components . . . . .</b>	<b>31</b>
	Installing Web Security components . . . . .	31
	Install Web Security Log Server. . . . .	31
	Installation steps. . . . .	32
	Install an instance of Filtering Service . . . . .	35
	Using a filtering only appliance. . . . .	35
	Installing Filtering Service on Windows . . . . .	37
	Installing Filtering Service on Linux . . . . .	39
	Install Websense Content Gateway. . . . .	41
	Installing other Web Security components . . . . .	42
	Installing Data Security components . . . . .	42
	Installing supplemental Data Security servers . . . . .	43
	Operating system requirements . . . . .	43
	Hardware requirements . . . . .	43
	Software requirements . . . . .	44
	Antivirus . . . . .	44
	Port requirements. . . . .	45
	Installation steps. . . . .	45
	Installing Email Security Log Server . . . . .	48
<b>Topic 4</b>	<b>Initial Configuration . . . . .</b>	<b>51</b>
	General configuration. . . . .	51
	Log on to the TRITON console . . . . .	52
	Web Security initial configuration . . . . .	53
	Getting started with Web Security solutions. . . . .	53
	Additional tips for working with Web Security solutions . . . . .	53
	Identifying Filtering Service by IP address. . . . .	54
	Additional configuration for Web Security Gateway Anywhere. . . . .	55
	Confirm Content Gateway registration with Data Security . . . . .	55
	Configuring the Content Gateway policy engine . . . . .	56
	Verifying Web and data security linking . . . . .	56
	Data Security initial configuration . . . . .	57
	Email Security Gateway initial configuration . . . . .	58
	Email Security Gateway initial configuration. . . . .	58
	Email Security Gateway Anywhere initial configuration . . . . .	59
	Content Gateway initial configuration . . . . .	59
	Network Agent and stealth mode NICs . . . . .	60

Windows .....	60
Linux .....	61



# 1

## Preparing for TRITON Enterprise Deployment

### In this topic:

---

- ◆ [Deployment overview, page 1](#)
  - ◆ [Installation overview, page 6](#)
  - ◆ [Requirements, page 7](#)
  - ◆ [Preparing servers for TRITON Enterprise deployments, page 10](#)
- 

This guide provides deployment and installation instructions for Websense® TRITON™ Enterprise.

## Deployment overview

---

Websense TRITON Enterprise includes Web Security Gateway Anywhere, Data Security, and Email Security Gateway Anywhere.

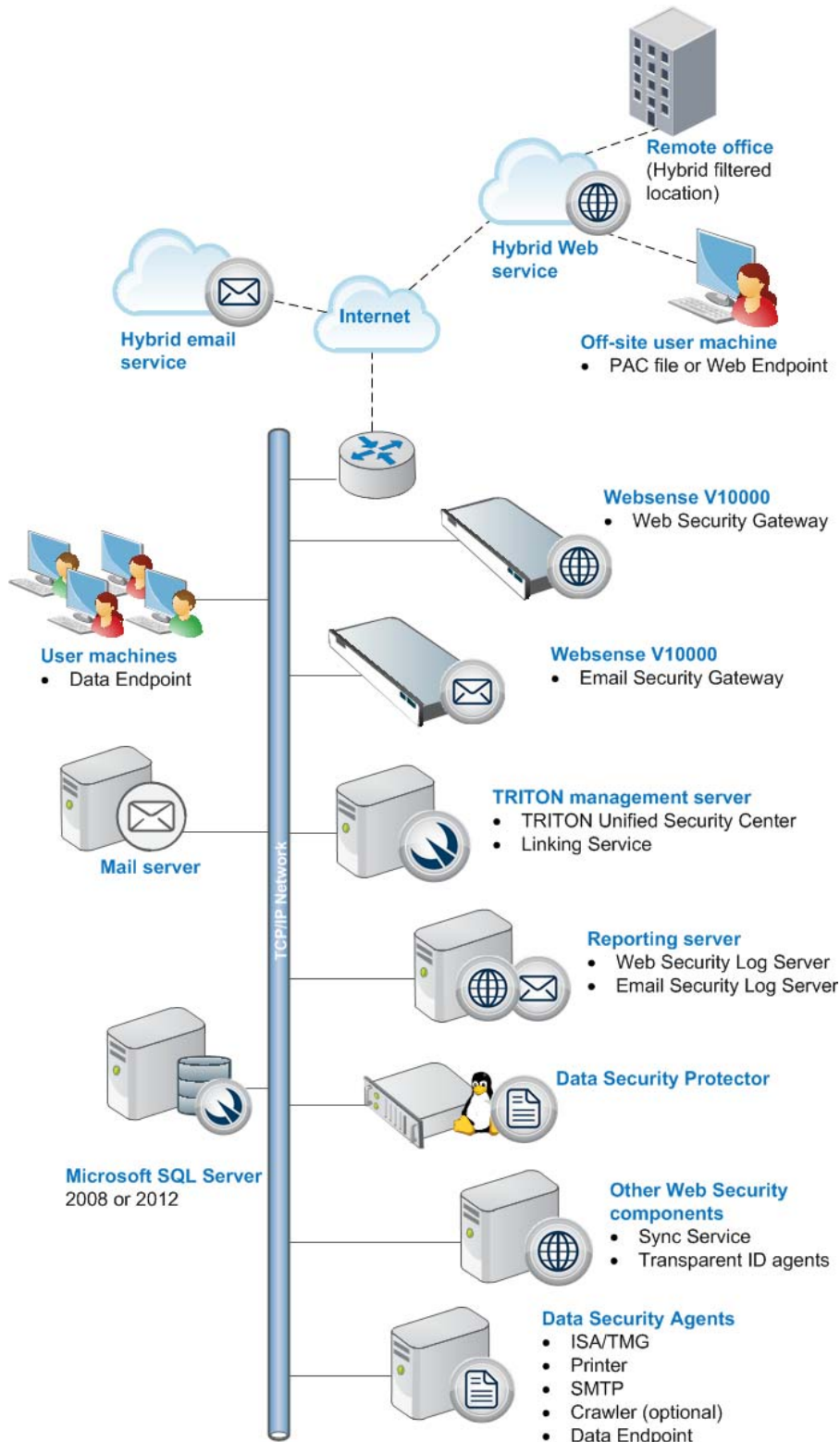
- ◆ The TRITON Unified Security Center, the management interface for Web, Email, and Data Security, resides on a Windows server.
- ◆ Web Security Gateway Anywhere may be deployed on Websense appliances, dedicated Windows or Linux servers, or a combination of platforms. This guide covers the following configuration:
  - The policy source (the standalone or primary Policy Broker and central Policy Server) reside separate from the TRITON management server, on another Windows or Linux server, or on a Websense appliance.

While this is not required and Policy Broker and Policy Server can reside on the TRITON management server machine, this configuration is recommended for TRITON Enterprise deployments to ensure optimum performance.
  - Web Security Log Server resides separate from the TRITON management server on a Windows machine.
- ◆ Data Security runs on Windows servers, optional Protector appliances, and elsewhere in the network.

- ◆ Email Security Gateway Anywhere enforcement components reside only on Websense appliances. Management and reporting components reside on Windows servers.



The following illustration is a high-level diagram of a basic appliance-based deployment of Websense TRITON Enterprise.



## Remote office and off-site users

You can use the hybrid Web service to provide web security for small remote offices. This is accomplished by designating a remote office as a hybrid filtered location. See [Initial Configuration](#), page 51, for more information.

Either the hybrid service or Websense remote filtering software can provide web filtering for off-site users (e.g., telecommuters or traveling personnel).

- ◆ To direct user requests to the hybrid service, you can install a PAC file or Websense Web Endpoint on the user's machine. Web requests from that machine are then directed to the hybrid service for policy enforcement.
- ◆ To use remote filtering software, an optional component, Remote Filtering Server, is installed in your network DMZ, and Remote Filtering Client is installed on user machines. Web requests from the machine are sent to Remote Filtering Server, which connects to Filtering Service for policy enforcement. See [Deploying Remote Filtering Server and Client](#).

## Hybrid services

If your subscription includes Web Security Gateway Anywhere and Email Security Gateway Anywhere:

- ◆ The cloud-based hybrid web service can provide Internet security for remote offices and off-site users.
- ◆ The cloud-based email hybrid service provides an extra layer of email scanning, stopping spam, virus, phishing, and other malware attacks before they reach your network and possibly reducing email bandwidth and storage requirements. You can also use the hybrid service to encrypt outbound email before delivery to its recipient.

## Websense appliances

Websense appliances may be used to deploy core Web and Email Security Gateway functionality.

- ◆ The Content Gateway proxy on the appliance manages web traffic.
- ◆ Incoming email flows from the email hybrid service (if enabled) to the Websense appliance and to your mail server. The Websense appliance also provides the Personal Email Manager facility for end users to manage quarantined email.

## Data Security Protector

The protector is a Linux-based soft-appliance, providing monitoring and blocking capabilities, preventing data loss and leaks of sensitive information. Using PreciseID technology, the protector can be configured to accurately monitor sensitive information-in-transit on any port.

## Components that may not be installed on Websense appliances

### TRITON management server

The TRITON management server is the Windows server on which the TRITON Unified Security Center (TRITON console) is installed. The TRITON console is the management and reporting interface for Websense Web, Data, and Email Security solutions.

The Data Security Management Server and, typically, Crawler also reside on the TRITON management server machine to provide key Data Security functions, including web and email DLP (data loss prevention) features.

Linking Service also usually resides on the management server.

### Web Security and Email Security Log Server

A separate Windows machine hosts Web Security Log Server and Email Security Log Server. These services receive information about Web Security and Email Security activity and process it into their respective Log Database.

### Optional Web Security components

Remote Filtering Server, Sync Service, and transparent identification agents (DC Agent, Logon Agent, eDirectory Agent, and RADIUS Agent) cannot reside on V-Series appliances.

Also, you can install additional instances of several Web Security components on Windows or Linux servers, if needed.

### Data Security Agents

Microsoft ISA/TMG agent, Printer agent, SMTP agent, Crawler, and Data Endpoint are installed on appropriate machines.

See the [Data Security Installation Guide](#) for installation instructions.

### Data Endpoint (User Machine)

The Data Endpoint can be installed on any machine.

## Third-party components

### Microsoft SQL Server

Microsoft SQL Server, running on a Windows server in your network, is used to store Websense TRITON logging and reporting data. Quarantined email messages are also stored here.

When Websense TRITON components are installed, SQL Server must be installed and running, typically on its own machine as shown in the diagram above.

## Mail server

Your internal mail server.

## Deployment details by TRITON Enterprise module

---

Use the links in this section to read about further deployment details and recommendations for the individual TRITON Enterprise modules.



### Note

The links in this section take you to pages in the Websense Technical Library. You can also download deployment guides for individual TRITON Enterprise modules in PDF format from the Technical Library.

## Web Security Gateway Anywhere

- ◆ [Web Security Deployment Recommendations](#)
- ◆ [Deploying Web Security for a distributed enterprise](#)

## Data Security

- ◆ [Planning Data Security Deployment](#)
- ◆ [Installing Data Security Components](#)
- ◆ [Integrating Data Security with Existing Infrastructure](#)
- ◆ [Scaling Data Security](#)

## Email Security Gateway

- ◆ [Email Security Gateway Deployment](#)

## Installation overview

---

To install Websense TRITON Enterprise components:

1. Make sure that a supported version of Microsoft SQL Server (not Express) is installed and running in your network. See [Requirements, page 7](#).
2. The machine with the standalone or primary Websense Policy Broker and its companion Policy Server instance must be configured first. These Web Security components must be running before any other Web Security components can be installed:
  - If Policy Broker will reside on a full policy source appliance, configure that appliance first. See [Setting Up Websense V-Series Appliances](#).

- If you wish to install the software version of Policy Broker and Policy Server, you must do this **before** the TRITON management server installation. Install the software version if you plan to use Policy Broker replication. See [Installing the Web Security policy source, page 13](#).

It is also recommended that you install an instance of Websense Filtering Service on this machine.

3. Install and run the firstboot script on your appliances. See [Setting Up Websense V-Series Appliances](#).
4. Install TRITON management and core Data Security components on a Windows Server 2008 R2 or Windows Server 2012 Standard Edition machine. For the machine requirements see [Requirements, page 7](#), and for the installation steps see [Installing TRITON Management Components, page 13](#).

On the **Installation Type** screen, select all three modules (**Web Security, Data Security, and Email Security**) under TRITON Unified Security Center.

5. Install Web and Email Security Log Server. See [Install Web Security Log Server, page 31](#) and [Installing Email Security Log Server, page 48](#).

If you plan to enable hybrid Web Security, note that Sync Service is typically installed with Web Security Log Server.

6. Install additional components (such as Web Security transparent identification agents or Data Security agents) as needed. See:
  - the section “Install additional Web Security components” in the installation instructions for [Web Security Gateway Anywhere](#).
  - the section “Adding, Modifying, or Removing Components” in the [Data Security Installation Guide](#)

## Requirements

This section lists the requirements for the TRITON Management Server and the reporting database.

### Reporting database

For all Websense TRITON solutions, Microsoft SQL Server is used to host the reporting database.

TRITON Enterprise deployments are advised to use Microsoft SQL Server Standard or Enterprise. These SQL Server editions cannot reside on the TRITON management server.

SQL Server clustering may be used with all supported standard and enterprise versions of Microsoft SQL Server for failover or high availability.

The supported database engines for Websense Web Security, Data Security, and Email Security solutions are:

- ◆ SQL Server 2008

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

- ◆ SQL Server 2008 R2 Express (installed by the TRITON Unified Installer)
- ◆ SQL Server 2008 R2

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

- ◆ SQL Server 2012

## TRITON Management Server

The machine that hosts core management components for all Websense security solutions is referred to as the **TRITON management server**. This machine hosts the TRITON Unified Security Center (TRITON console), which includes:

- ◆ The infrastructure uniting all management components
- ◆ A settings database, holding administrator account information and other data shared by all management components
- ◆ One or more management modules, used to access configuration, policy management, and reporting tools for a Websense security solution. Available modules include:
  - Web Security manager
  - Data Security manager
  - Email Security manager

Additional components may also reside on the TRITON management server.

The TRITON management server must be hosted on one of the following 64-bit Windows operating systems:

- ◆ Windows Server 2008 Standard or Enterprise R2
- ◆ Windows Server 2012 Standard Edition
- ◆ Windows Server 2012 Standard or Enterprise R2

Typically, there is only one TRITON management server in a deployment. It serves as the central point for management, configuration, and reporting.

## Hardware requirements

The following are minimum hardware recommendations for a TRITON management server.

Notes:

- ◆ Data Security allows for either local or remote installation of the forensics repository. If the repository is hosted remotely, deduct 90GB from the Data Security disk space requirements.
- ◆ It is strongly recommended you allocate more than the minimum listed disk space to allow for scaling with use.

- ◆ If you choose to install the Websense product on a drive other than the main Windows drive (typically C drive), then you must have at least 2GB free on the main Windows drive to accommodate for files to be extracted to this drive.

TRITON console modules	Recommended requirements	Minimum requirements
Web Security manager	4 CPU cores (2.5 GHz), 8 GB RAM, 150 GB Disk Space	4 CPU cores (2.5 GHz), 4 GB RAM, 7 GB Disk Space
Data Security manager	4 CPU cores (2.5 GHz), 8 GB RAM, 140 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB RAM, 140 GB Disk Space
Web Security and Data Security managers	8 CPU cores (2.5 GHz), 12 GB RAM, 300 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB Disk Space
Email Security and Data Security managers	8 CPU cores (2.5 GHz), 12 GB RAM, 300 GB Disk Space	4 CPU cores (2.5 GHz), 8 GB RAM, 146 GB Disk Space
Web Security, Data Security, and Email Security managers	8 CPU cores (2.5 GHz), 16 GB RAM, 500 GB Disk Space	8 CPU cores (2.5 GHz), 16 GB RAM, 146 GB Disk Space

## TRITON console browser support

Use any of the following browsers to access the TRITON Unified Security Center.

Browser	Versions
Microsoft Internet Explorer*	8, 9, and 10, and 11
Mozilla Firefox	4.4 and later
Google Chrome	13 and later

\* Do not use Compatibility View.

## Virtualization systems

All TRITON Unified Security Center components are supported on these virtualization systems:

- ◆ Hyper-V over Windows Server 2008 R2 or Windows Server 2012 Standard Edition
- ◆ VMware over Windows Server 2008 R2 or Windows Server 2012 Standard Edition

Note that this support is for the TRITON console only. Other components (used for filtering, analysis, reporting, or enforcement) may have additional requirements that are not supported by these virtualization environments.

## Directory services for administrator authentication

If you allow users to log on to the TRITON console using their network accounts, the following directory services can be used to authenticate administrator logons:

- Microsoft Active Directory
- Lotus Notes
- Generic LDAP directories
- Novell eDirectory
- Oracle Directory Services

## Preparing servers for TRITON Enterprise deployments

---

Follow the instructions in this section to ensure your servers are ready for the v7.8 installation.

### Windows

On Windows machines that will host either the TRITON management server or other TRITON components:

- ◆ 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.

---

- ◆ Make sure all Microsoft updates have been applied. There should be no pending updates, especially any requiring a restart of the system.
- ◆ 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).
- ◆ Make sure that .NET Framework version 2.0 or higher (available from [www.microsoft.com](http://www.microsoft.com)) is installed.
- ◆ 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.
- ◆ Disable the antivirus software on the machine before installation. After installation, before restarting your antivirus software, see [Excluding Websense software from antivirus scans](#).
- ◆ 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. See [Websense TRITON Enterprise default ports](#).



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

## Linux

On Linux machines that will host supported TRITON components:

- ◆ If SELinux is enabled, disable it or set it to permissive.
- ◆ 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 Websense components installed on this machine.



### Important

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

- ◆ For v7.8.2, if you receive an error during installation regarding the **/etc/hosts** file, use the following information to correct the problem. For v7.8.1, use this information to edit your **/etc/hosts** file prior to running the installer.

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.

- ◆ Websense 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

## Installing TRITON Management Components

### In this topic:

---

- ◆ [Installing the Web Security policy source, page 13](#)
  - ◆ [Creating the TRITON Management Server, page 14](#)
- 

Follow the instructions in this section to install:

- ◆ The Web Security policy source
- ◆ The TRITON Unified Security Center and management components on the TRITON management server

### Installing the Web Security policy source

---

This section describes the steps required to install the primary or standalone Policy Broker and the associated Policy Server instance on a Windows machine. If Policy Broker will reside on a full policy source appliance, see [Setting Up Websense V-Series Appliances](#) and [Configuring Web Security components](#).

It is recommended that you install Websense Filtering Service at the same time. If you choose to install the first instance of Filtering Service on a different machine, it must connect to the central Policy Server on this machine. See [Install an instance of Filtering Service, page 35](#).

You can also install other components on this machine, for example User Service, Usage Monitor, and Directory Agent.

On the machine that will host the policy source:

1. Ensure you have prepared the machine as described in [Preparing servers for TRITON Enterprise deployments, page 10](#).
2. Log on to the machine with domain admin privileges.
3. Download or copy the TRITON Unified Installer (the Windows installer) to this machine. The installer is available from [mywebsense.com](http://mywebsense.com), and the installer file is **WebsenseTRITON782Setup.exe**.
4. Double-click **WebsenseTRITON782Setup.exe** to launch the installer.

A progress dialog box appears, as files are extracted. It may take some time to extract all of the installer files and launch the setup program.

5. On the **Welcome** screen, click **Start**.  
The Installer Dashboard stays on-screen during installation. Various subinstallers and dialog boxes are displayed over it.
6. On the **Subscription Agreement** screen, select **I accept this agreement**, then click **Next**.
7. On the **Installation Type** screen, select **Custom**.
8. On the Custom Installation dashboard, click the Web Security **Install** link.
9. On the **Select Components** screen, select Policy Broker, Policy Server, and Filtering Service. Note that these components must be installed in the order listed, and before any other Web Security components. (If you select all 3 at the same time, they are installed in the correct order.)
10. 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.



#### **Important**

Be sure to record the synchronization password. You must provide this password each time you create a Policy Broker replica.

It is recommended that you create no more than 2 or 3 Policy Brokers in your deployment.

---

11. On the Integration Option screen, select **Integrated with another application or device**, then click **Next**.
12. On the Select Integration screen, select **Websense Content Gateway**, then click **Next**.
13. 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.
14. On the Pre-Installation Summary screen, verify the information shown, then click **Next**.
15. A progress screen is displayed. Wait for installation to complete.

## **Creating the TRITON Management Server**

---

The installation procedure for the TRITON management server includes the following steps:

- ◆ *Step 1: Download the TRITON Unified Installer, page 15*
- ◆ *Step 2: Select management components, page 15*
- ◆ *Step 3: Install the TRITON Infrastructure, page 17*
- ◆ *Step 4: Install Web Security management components, page 22*
- ◆ *Step 5: Install Data Security management components, page 25*
- ◆ *Step 6: Install Email Security management components, page 28*

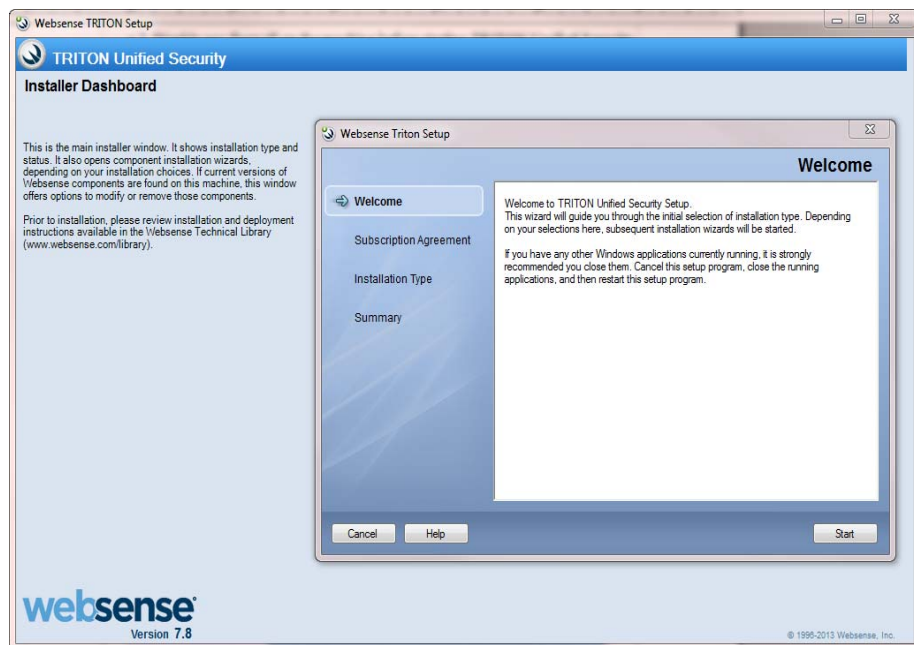
Ensure you have prepared the machine as described in *Preparing servers for TRITON Enterprise deployments*, page 10.

## Step 1: Download the TRITON Unified Installer

1. Log on to the machine with domain admin privileges.
2. Download or copy the TRITON Unified Installer (the Windows installer) to this machine. The installer is available from [mywebsense.com](http://mywebsense.com), and the installer file is **WebsenseTRITON782Setup.exe**.

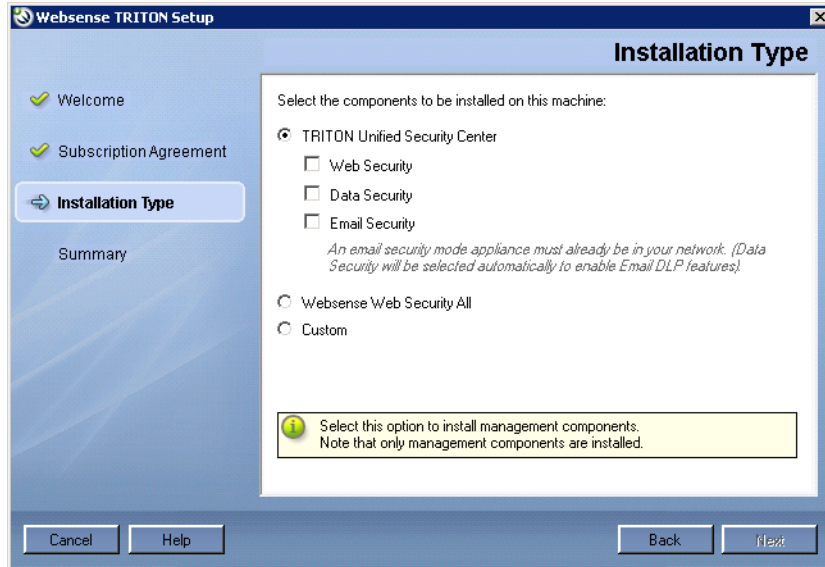
## Step 2: Select management components

1. On the TRITON Management Server, double-click **WebsenseTRITON782Setup.exe** to launch the installer.  
After a few seconds a progress dialog box appears, as files are extracted.
2. On the **Welcome** screen, click **Start**.



3. On the **Subscription Agreement** screen, select **I accept this agreement** and then click **Next**.

- On the **Installation Type** screen, select **TRITON Unified Security Center** and the modules you want to install (Web Security, Data Security, and Email Security).



**Note**

The TRITON Unified Security Center modules are management consoles. Selecting them does not install other security or filtering components. Non-management components are installed using the **Websense Web Security All** or **Custom** options.

See the following table for information about which modules you should select for installation.

Solution	TRITON Unified Security module		
	Web Security	Data Security	Email Security
Web Filter, Web Security, and Web Security Gateway	X		
Web Security Gateway Anywhere	X	X	
Data Security		X	
Email Security Gateway (Anywhere)		X	X

Note: If your subscription includes a combination of these solutions, install all of the modules required by them. For example, if your subscription includes both Web Security Gateway Anywhere and Email Security Gateway, install all 3 modules.

When you select **Email Security**, **Data Security** is also selected. The Data Security module is required for email DLP (data loss prevention) features, included with Email Security Gateway (Anywhere).



---

**Important**

To install the Email Security module of the TRITON Unified Security Center, an Email Security Gateway appliance must already be running. You will need to provide the appliance C interface IP address during console installation.

The appliance E1 (and E2, if used) interface must also be configured in the Appliance Manager before you install Email Security management components.

---

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

## Step 3: 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**.



---

**Important**

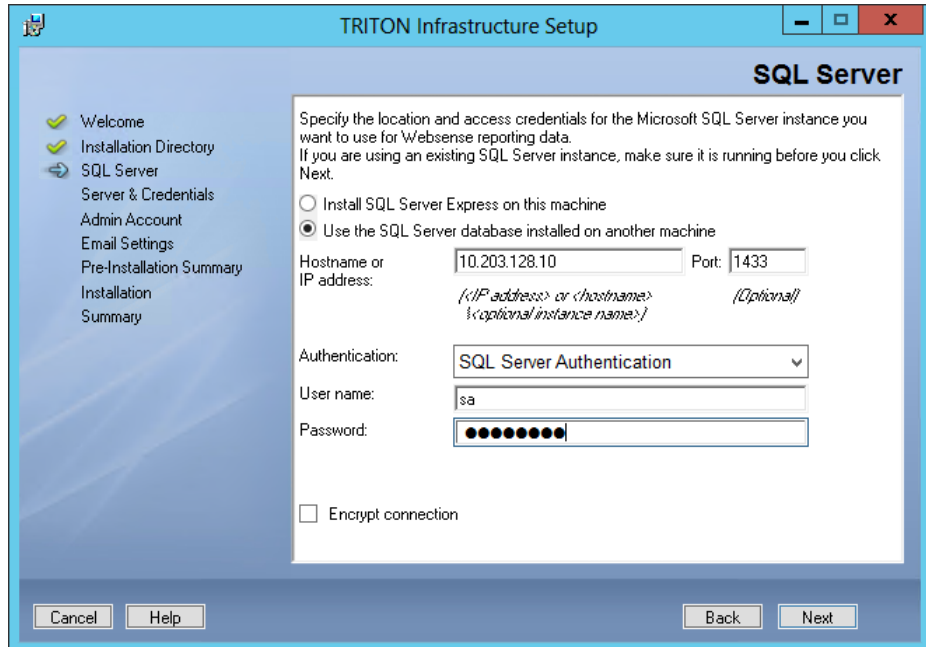
The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

---

- To accept the default location (recommended), simply click **Next**.
  - To specify a different location, click **Browse**.
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.

The information entered here is also used by the Web, Data, and Email Security component installers, by default. The Web Security component installer can be

used to specify a different database; the Data and Email Security component installers cannot.



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).

See [Requirements, page 7](#), to verify your version of SQL Server is supported.

After entering the above information, 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 Windows authentication with Data Security, Web Security Gateway Anywhere or Email Security Gateway/Anywhere, use an account with the



sysadmin role. If you are using SQL Server Express, **sa** (the default system administrator account) is automatically specified (this is the default system administrator account).



#### Note

The system administrator account password cannot contain single or double quotes.

For more information about permissions required for the connection account, see [Installing with SQL Server](#).

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](#).

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.*

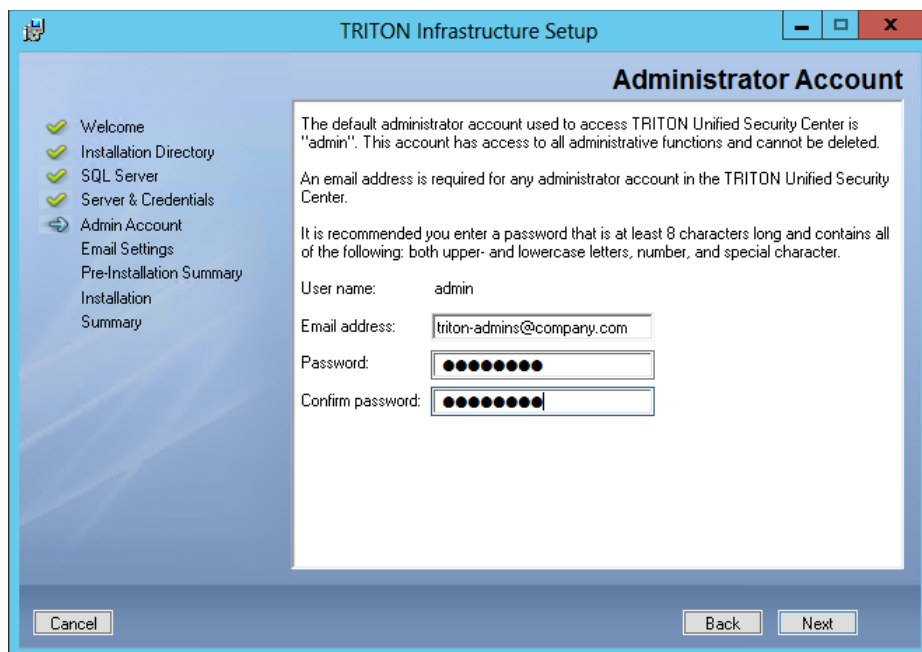
Click **OK** to dismiss the message, verify the information you entered, and click **Next** to try again.

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.

Use the IP address selected to access the TRITON Unified Security Center (via Web browser). Also specify this IP address to any Websense component that needs 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 server/host 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**.



The screenshot shows a window titled "TRITON Infrastructure Setup" with a sub-header "Administrator Account". On the left is a navigation pane with the following items: Welcome, Installation Directory, SQL Server, Server & Credentials, Admin Account (highlighted with a mouse cursor), Email Settings, Pre-Installation Summary, Installation, and Summary. The main content area contains the following text and form fields:

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:

Password:

Confirm password:

At the bottom of the window are three buttons: "Cancel", "Back", and "Next".

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

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

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

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

When you click **Finish** in TRITON Infrastructure Setup, component installers for each module selected in the Module Selection screen are launched in succession.

Only the component installers for the modules you have selected are launched. For example, if you select only Web Security and Data Security, the Email Security installer is not launched.

Complete the following procedures for the modules you have selected. For each module, a component installer will launch. The component installers launch in the order shown here.

- ◆ [Step 4: Install Web Security management components](#)
- ◆ [Step 5: Install Data Security management components](#)
- ◆ [Step 6: Install Email Security management components](#)

## Step 4: Install Web Security management components

In the recommended software installation for TRITON Enterprise deployments, the TRITON management server hosts management components while the primary or standalone Policy Broker and central Policy Server reside on a separate machine (the policy source machine), as described in [Installing the Web Security policy source](#).

Note that if Linking Service will run on the management server, the Filtering Service that connects to the central Policy Server must be installed and running before Linking Service is installed.



### Important

If you have a **full policy source** Web Security appliance, Policy Broker, Policy Server, and Filtering Service, among other components, reside there.

---

Follow these instructions to install Web Security management components on a TRITON management server.

1. It is assumed you have reached this point by starting a TRITON Unified Security Center installation. If not, see [Step 2: Select management components, page 15](#).
2. In the **Select Components** screen, select the components you want to install on this machine and then click **Next**.

The following Web Security components are available for installation on a TRITON management server:

- **TRITON - Web Security** (the component that activates the Web Security module in the TRITON Unified Security Center) must be installed. It is selected by default and cannot be deselected. The other components shown are optional for this machine.
- **Sync Service** typically does not run on the management server. It is a required component of Web Security Gateway Anywhere, but it typically resides on the Web Security Log Server machine.

**Note**

Although Sync Service and the Web Security Log Server may be installed on the TRITON management server, they consume considerable system resources. For TRITON Enterprise deployments, it is recommended to install these components on another machine. See [Install Web Security Log Server, page 31](#).

---

- Select **Linking Service** if your subscription includes both a Web Security solution and Data Security.

**Important**

Filtering Service must be installed in your network before you install Linking Service. In an appliance-based deployment, Filtering Service is installed on all Web Security appliances (full policy source, user directory and filtering, and filtering only). In a software-based deployment, it is recommended that you install Filtering Service with Policy Broker and Policy Server on another separate machine from the TRITON management server, as Filtering Service can consume considerable system resources and may have a performance impact on the TRITON management server. Large or distributed environments may include multiple Filtering Service instances.

You can return to the TRITON management server at a later time and install Linking Service if required.

---

- **Real-Time Monitor** is optional. It is typically installed on the TRITON management server, but can be located elsewhere. Install no more than one instance of Real-Time Monitor for a Policy Server instance. In most cases, only one instance of Real-Time Monitor is required per deployment.
- **Policy Broker and Policy Server** are typically already installed on a separate machine, and should not be selected again.

## Policy Server Connection screen

If Policy Server does not reside on the management server, on the Policy Server Connection screen, enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.

The Policy Broker communication port must be in the range 1024-65535. During installation, Policy Broker may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Broker instances.) To verify the port:

1. Navigate to the Websense **bin** directory on the Policy Server machine (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/, by default).
2. Open the **BrokerService.cfg** file in a text editor.
3. Locate the **listen\_port** value.
4. When you are finished, close the file without saving. Do **not** modify the file.

## Policy Broker Connection screen

If Policy Broker does not reside on the management server, and you selected Sync Service for installation, the **Policy Broker Connection** screen appears. Enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.

The Policy Broker communication port must be in the range 1024-65535. During installation, Policy Broker may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Policy Broker instances.) To verify the port:

1. Navigate to the Websense **bin** directory on the Policy Server machine (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/, by default).
2. Open the **BrokerService.cfg** file in a text editor.
3. Locate the **listen\_port** value.
4. When you are finished, close the file without saving. Do **not** modify the file.

## Filtering Service Communication screen

If you select Linking Service for installation, the **Filtering Service Communication** screen appears.

Enter the IP address of the Filtering Service machine and the port Filtering Service uses to communicate with Network Agent, Content Gateway, or third-party integration products (default is 15868).

- ◆ In an appliance-based deployment, Filtering Service is installed on all Web Security appliances (full policy source, user directory and filtering, and filtering only).
  - Enter the IP address of the appliance's C interface and use the default port (15868).
  - If you have multiple appliances, be sure to select the one you want Network Agent, the filtering plug-in, or Linking Service to use.
- ◆ The Filtering Service communication port must be in the range 1024-65535. During installation, Filtering Service may have been automatically configured to use a port other than the default. (This does not apply to appliance-based Filtering Service instances.) To verify the port:
  - a. Navigate to the Websense **bin** directory on the Policy Server machine (C:\Program Files\Websense\Web Security\bin or /opt/Websense/bin/, by default).
  - b. Open the **eimserver.ini** file in a text editor.
  - c. Locate the **WebsenseServerPort** value.
  - d. When you are finished, close the file without saving. Do **not** modify the file.

If Filtering Service is not installed anywhere in your network, you must install it before installing Network Agent, a filtering plug-in, or Linking Service.

## Completing the installation

1. On the **Pre-Installation Summary** screen, verify the information shown. The summary shows the installation path and size, and the components to be installed.
2. Click **Next** to start the installation. The **Installing Websense** progress screen is displayed. Wait for installation to complete.
3. On the **Installation Complete** screen, click **Next**.
4. If you have not selected any other TRITON Unified Security Center module, you are returned to the Modify Installation dashboard. Installation is complete. If you have chosen to install other modules of the TRITON Unified Security Center, you are returned to the Installer Dashboard and the next component installer is launched.

## Step 5: Install Data Security management components

Follow these instructions to install Data Security management components on the TRITON management server. This includes:

- ◆ A Data Security policy engine
- ◆ Primary fingerprint repository
- ◆ Forensics repository
- ◆ Endpoint server

1. It is assumed you have reached this point by starting a TRITON Unified Security Center installation. If not, see [Step 3: Install the TRITON Infrastructure](#), page 17.
2. When the Websense Data Security Installer is launched, a **Welcome** screen appears. Click **Next** to begin Data Security installation.



**Note**

If the .NET 2.0 framework is not found on this machine, the Data Security Installer installs it.

---

3. In the **Select Components** screen, click **Next** to accept the default selections.



**Note**

If there is insufficient RAM on this machine for Data Security Management Server components, a message appears. Click **OK** to dismiss the message. You are allowed to proceed with the installation. However, it is a best practice to install only if you have sufficient RAM.

---

4. 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.

5. 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.

6. If your SQL Server database is on a remote machine, you are prompted for the name of a temporary folder. This screen defines where Data Security should store temporary files during archive processing as well as system backup and restore.

Archiving lets you manage the size of your incident database and optimize performance. Backup lets you safeguard your policies, forensics, configuration, data, fingerprints, encryption keys, and more.

If you do not plan to archive incidents or perform system backup and restore, you do not need to fill out this screen.

Before proceeding, create a folder in a location that both the database and TRITON management server can access. (The folder must exist before you click **Next**.) On average, this folder will hold 10 GB of data, so choose a location that can accommodate this.

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.



### Important

The account used to access the SQL Server must have **BACKUP DATABASE** permissions to communicate with the installer. If it does not, an error results when you click **Next**.

---

To grant this permission, issue the following T-SQL commands on the SQL Server instance:

```
USE master
GRANT BACKUP DATABASE TO <user>
GO
```

After installation of Data Security components, you can revoke this permission:

```
USE master
REVOKE BACKUP DATABASE TO <user>
GO
```

7. In the **Installation Confirmation** screen, click **Install** to begin installation of Data Security components.
8. 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.*

Clicking **No** cancels the installation.

A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.

9. The **Installation** progress screen appears. Wait for the installation to complete.
10. When the **Installation Complete** screen appears, click **Finish** to close the Data Security installer.
11. If no other TRITON Unified Security Center module is chosen for installation, you are returned to the Modify Installation dashboard. Installation is complete. Otherwise, you are returned to the Installer Dashboard and the next component installer is launched.

For information on installing a supplemental Data Security server, see [Installing Data Security components](#), page 42. For information on installing other Data Security components, such as the protector, mobile agent, printer agent, SMTP agent, TMG agent, or endpoint client, see the [Data Security Installation Guide](#).

## Step 6: Install Email Security management components

Follow these instructions to install the Email Security module of the TRITON Unified Security Center. In addition to the Email Security module (also referred to as Email Security manager), you will be given the option to install Email Security Log Server on this machine. As Log Server consumes considerable system resources, for TRITON Enterprise deployments it is recommended to install it on another machine. See [Installing Email Security Log Server](#), page 48.

1. It is assumed you have reached this point by starting a TRITON Unified Security Center installation and selecting the Email Security module. If not, see [Step 3: Install the TRITON Infrastructure](#), page 17.
2. Once the Email Security Installer is launched, the **Introduction** screen appears; click **Next** to begin Email Security installation.
3. On the **Select Components** screen, deselect the Email Security Log Server option, then click **Next**.

Email Security manager (i.e, the Email Security module of the TRITON Unified Security Center) will be installed automatically. You cannot deselect it.



### Note

If you do not see the Email Security module on this screen, TRITON Infrastructure was not detected by the Email Security Installer. TRITON Infrastructure must be installed already to be able to install Email Security management components.

---

4. On the **Email Security Database** screen, specify the IP address or IP address and instance name (format: IP address\instance) for the Email Security database. You may specify whether the connection to the database should be encrypted. Please note the following issues associated with using this encryption feature:
  - You must have imported a trusted certificate to the Log Server machine in order to use the encryption option. See your database documentation for information about importing a trusted certificate.
  - The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
  - The connection from the Email Security module on the TRITON console to the V-Series appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.

Designate the login type for the database, either Windows authentication or **sa** account.

5. On the **Email Security Gateway** screen specify the Email Security Gateway appliance to be managed by this installation of the TRITON Unified Security Center and then click **Next**.

Enter the IP address of the **C** interface of the Email Security Gateway appliance. You must specify an IP address only. Do not use a fully-qualified domain name (FQDN).

When you click **Next**, communication with the specified appliance will be verified. Communication may be unsuccessful if:

- Subscription key has already been applied to the appliance (typically meaning another installation of TRITON Unified Security Center has been used to manage the appliance). The subscription key must be reset on the appliance.
  - Version of software to be installed does not match the version of the appliance. Verify whether the versions match.
  - Specified appliance is a secondary appliance in a cluster. Specify the primary appliance in the cluster or a non-clustered appliance.
  - The appliance cannot connect to the specified database server (specified during product installation).
  - Firewall is blocking communication to the appliance on port 6671. Make sure any local firewall allows outbound communication on port 6671.
  - Appliance E interface has not been correctly configured in the Appliance Manager.
6. On the **Installation Folder** screen, specify the location to which you want to install Email Security components and then click **Next**.

To select a location different than the default, use the **Browse** button.

Each component (Email Security manager and/or Email Security Log Server) will be installed in its own folder under the parent folder you specify here.
  7. On the **Pre-Installation Summary** screen, review the components to be installed. If they are correct, click **Install**.

Click **Back** to return to any screen on which you want to modify settings.
  8. The **Installing Websense Email Security** screen appears, as components are being installed.
  9. Wait until the **Installation Complete** screen appears, and then click **Done**.
  10. TRITON Unified Security Setup closes. Installation is complete.



# 3

## Installing Additional Components

### In this topic:

---

- ◆ [Installing Web Security components](#), page 31
  - ◆ [Installing Data Security components](#), page 42
  - ◆ [Installing Email Security Log Server](#), page 48
- 

## Installing Web Security components

---

The steps in this section describe the installation of Web Security components if you have not already installed them on the TRITON management server. If you are distributing components across multiple machines, run the installer and complete the installation steps on each machine.

These instructions assume that you have already launched the installer and selected **Custom**.

### Install Web Security Log Server

Web Security Log Server is a Windows-only component that logs Internet request data, including:

- ◆ Source of request
- ◆ Category or protocol associated with the request
- ◆ Whether the request was permitted or blocked
- ◆ Whether keyword blocking, file type blocking, quota allocations, bandwidth levels, or password protection were applied

Each Log Server instance can log to only one Log Database at a time, and only one Log Server can be installed for each Policy Server.

Log Server processing can consume considerable system resources.

In a software-based deployment, do not install Log Server on the same machine as Filtering Service or Network Agent—policy enforcement or logging performance may be affected if they are on the same machine.

In a Websense appliance-based deployment, Log Server must be installed on a separate Windows machine.



**Note**

Web Security Log Server must be installed before you can see charts on the Status > Dashboard page, or run presentation or investigative reports in the Web Security manager.

## Installation steps

To be able to install Web Security Log Server, a supported database engine (see [Reporting database, page 7](#)) must be running.

1. On the **Select Components** screen in the Websense installer, select Web Security Log Server.
2. On the [Policy Server Connection screen](#), enter the IP address of the Policy Broker machine and the Policy Broker communication port (default is 55880).

In an appliance-based deployment, Policy Broker is installed on the **full policy source** appliance. Enter the IP address of the appliance's C interface and use the default port.

3. On the **Database Information** screen, enter the hostname or IP address of the machine on which a supported database engine is running. If a supported database engine is detected on this machine, its IP address is already entered by default. To use a database engine on a different machine, enter its IP address instead.

If you are using SQL Server clustering, enter the virtual IP address of the cluster.

After entering the IP address of the database engine machine, choose how to connect to the database:

- 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**

The database engine must be running to install Websense reporting components. The installer will test for a connection to the specified database engine when you click **Next** on the **Database Information** screen. The installer cannot proceed unless a successful connection can be made.

4. 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 database location information is taken from TRITON Infrastructure's configuration. Typically, you should accept the default in this case.

If the database engine is on this machine, the default location is the Websense directory (**C:\Program Files (x86)\Websense**). If the database engine is on another machine, the default location is **C:\Program Files\Microsoft SQL Server** on that machine.

It is a best practice to use the default location. If you want to create the Log Database files in a different location (or if you already have Log Database files in a different location), enter the path. The path entered here is understood to refer to the machine on which the database engine is located.

**Important**

The directory you specify for the Log Database files must already exist. The installer cannot create a new directory.

You can also specify a particular database instance in this path. The instance must already exist. See Microsoft SQL Server documentation for information about instances and paths to instances.

5. On the **Optimize Log Database Size** screen, select either or both of the following options and then click **Next**.
  - **Log Web page visits:** Enable this option to log one record (or a few records) with combined hits and bandwidth data for each Web page requested rather than a record for each separate file included in the Web page request. This results in fewer records and therefore smaller databases, allowing for potentially faster report generation and longer storage capacities. Deselect this option to log a record of each separate file that is part of a Web page request, including images and advertisements. This results in more precise reports, but creates a much larger database and causes reports to generate more slowly.
  - **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
6. On the **Installation Directory** screen, accept the default installation path, or click **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 or Program Files (x86)\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.

---

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 **OK**.
  - Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.
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. An **Installing** progress screen is displayed. Wait for the installation to complete.
9. On the **Installation Complete** screen, click **Done**.
10. After installing Log Server, restart the TRITON management server machine.



### Important

When Web Security Log Server is not installed on the TRITON management server, be sure to restart the management server before creating scheduled jobs in presentation reports. Any scheduled jobs you create before restarting the server cannot be saved properly and will be lost, even if they appear to work for a period of time.

---



## 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 Websense 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.)

Best practice is to install Filtering Service on a different machine from the TRITON management server. This is because Filtering Service can consume considerable system resources and may have a performance impact on the server.

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

### Using a filtering only appliance

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

#### Gather the data

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

Security mode	Web
Which Web Security subscription? (if prompted)	Web Security Gateway Anywhere

<p>Hostname (example: appliance.domain.com)</p> <p>1 - 60 characters long.          The first character must be a letter.          Allowed: letters, numbers, dashes, or periods.          The name cannot end with a period.</p> <p>If Content Gateway will be configured to perform Integrated Windows Authentication, the hostname cannot exceed 11 characters (excluding the domain name).</p> <p>For more information, see the section titled Integrated Windows Authentication in Content Gateway Manager Help.</p>	
<p>IP address for network interface C</p>	
<p>Subnet mask for network interface C</p>	
<p>Default gateway for network interface C (IP address) <i>Optional</i></p> <p>NOTE: If you do not provide access to the Internet for interface C, use the Web Security manager to configure P1 to download Master Database updates from Websense servers.</p> <p>See the Appliance Manager Help for information about configuring the interfaces. See the Web Security Help for information about configuring database downloads.</p>	
<p>Primary DNS server for network interface C (IP address)</p>	
<p>Secondary DNS server for network interface C (IP address) <i>Optional</i></p>	
<p>Tertiary DNS server for network interface C (IP address) <i>Optional</i></p>	
<p>Unified password (8 to 15 characters, at least 1 letter and 1 number)</p> <p>This password is for the following:</p> <ul style="list-style-type: none"> <li>• Appliance manager</li> <li>• Web Security manager</li> <li>• Content Gateway manager</li> </ul>	
<p>Send usage statistics?</p>	<p>Usage statistics from appliance modules can optionally be sent to Websense to help improve the accuracy of categorization.</p>

### Run the firstboot 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

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 the a security mode **Web**, then select **Web Security Gateway Anywhere**.
5. Follow the on-screen instructions to provide the information collected above.

After the activation script has been completed successfully, you can access Appliance manager by opening a supported browser and entering this URL in the address bar:

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

Use the Appliance manager to configure your appliance network interfaces and policy source mode (**filtering only**). See your appliance [Getting Started](#) guide for details.

## Installing Filtering Service on Windows

Ensure you have prepared the machine as described in [Preparing servers for TRITON Enterprise deployments](#), page 10.

To install Filtering Service on a supported Windows platform:

1. Log on to the machine with domain admin privileges.
2. Download the TRITON Unified Installer (**WebsenseTRITON782Setup.exe**) from [mywebsense.com](http://mywebsense.com).
3. Right-click **WebsenseTRITON782Setup.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. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that Web Security components should use for communication, then click **Next**. (Prior to 7.8.2, this screen appears after the Policy Server Connection screen in step 9 below.)
7. On the Installation Type screen, select **Custom** and then click **Next**.
8. On the Select Components screen, select the following components, then click **Next**:
  - Filtering Service
  - User Service
  - Usage MonitorOptionally, you may also select:
  - Network Agent
  - State Server
  - Multiplexer
  - DC Agent, Logon Agent, eDirectory Agent, or RADIUS Agent
  - Directory Agent
9. On the Policy Server Connection screen, enter the IP address of the central Policy Server machine and the Policy Server communication port (55806, by default), then click **Next**.
10. If you are installing Directory Agent, on the Policy Broker Connection screen, enter the IP address of the primary or standalone Policy Broker and its communication port (55880, by default), then click **Next**.
11. On the Active Directory screen, indicate whether you are using Windows Active Directory to authenticate users in your network, then click **Next**.
12. On the Computer Browser screen, indicate that the installer should attempt to start the service, then click **Next**.
13. On the Integration Option screen, select **Integrated with another application or device**, then click **Next**.
14. On the Select Integration screen, select **Websense Content Gateway**, then click **Next**.
15. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other Web Security components, then click **Next**.
16. On the Filtering Feedback screen, indicate whether you want Websense software to send feedback to Websense, Inc., then click **Next**.
17. 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.
18. On the Installation Directory screen, accept the default installation path, or click or select **Choose** to specify another path, and then click **Next**.

The installation path must be absolute (not relative). The default installation path is C:\Program Files (x86)\Websense\Web Security\bin\.

The installer creates this directory if it does not exist.



### Important

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

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

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

20. A progress screen is displayed. Wait for the installation to complete.
21. On the Installation Complete screen, click **Finish**.

## Installing Filtering Service on Linux

Ensure you have prepared the machine as described in *Preparing servers for TRITON Enterprise deployments*, page 10.

1. Log on to the installation machine with full administrative privileges (typically, **root**).
2. Create a setup directory for the installer files. For example:  
/root/Websense\_setup
3. Download the Web Security Linux installer package from [mywebsense.com](http://mywebsense.com). The installer package is called **WebsenseWeb78Setup\_Lnx.tar.gz**.

Place the installer archive in the setup directory you created.

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

```
gunzip WebsenseWeb78Setup_Lnx.tar.gz
tar xvf WebsenseWeb78Setup_Lnx.tar
```

5. 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
```

### Perform the Filtering Service installation

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 **Next**.

3. If the machine has multiple NICs, on the Multiple Network Interfaces screen, select the IP address of the NIC that Web Security components should use for communication, then click **Next**. (Prior to 7.8.2, this screen appears after the Policy Server Connection screen in step 6 below.)
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 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 MonitorOptionally, you may also select:
  - Network Agent
  - State Server
  - Multiplexer
  - Logon Agent, eDirectory Agent, or RADIUS Agent
  - Directory Agent
6. On the Policy Server Connection screen, enter the central Policy Server IP address and communication port (55806, by default).
7. If you are installing Directory Agent, on the Policy Broker Connection screen, enter the IP address of the primary or standalone Policy Broker machine, and the Policy Broker communication port (55880, by default).
8. On the Integration Option screen, select **Integrated with another application or device**, then click or select **Next**.
9. On the Select Integration screen, select **Websense Content Gateway**, then click or select **Next**.

When you install Content Gateway, you will be prompted for the Filtering Service IP address.
10. If you are installing Network Agent, on the Network Card Selection screen, select the NIC that Network Agent should use to communicate with other Web Security components, then click or select **Next**.
11. On the Filtering Feedback screen, indicate whether you want Websense software to send feedback to Websense, Inc., then click or select **Next**.
12. 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 and Logon Agent use this information to query the domain controller for user and group information.
13. 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.

14. 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.

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

**Note**

If you are using the command-line Linux installer, do **not** cancel (Ctrl-C) the installer after the **Pre-Installation Summary** screen, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

---

16. On the Installation Complete screen, click or select **Done**.

## Install Websense Content Gateway

Websense Content Gateway is a Linux-based, high-performance Web proxy and cache that provides real-time content analysis and website classification to protect clients from malicious content while enabling access to safe content.

Content Gateway offers:

- ◆ Categorization of dynamic websites
- ◆ Categorization of new and unclassified websites
- ◆ Optionally, HTTPS and FTP content analysis, in addition to HTTP
- ◆ Enterprise Web proxy caching capabilities
- ◆ Prevention of data loss over web channels

Content Gateway is a required component of Websense Web Security Gateway and Web Security Gateway Anywhere. In a software-based deployment, Content Gateway must be installed on a Linux machine. The machine should be dedicated to running Content Gateway.



**Important**

In a Websense-appliance-based deployment, when Web Security Gateway Anywhere is configured, Content Gateway is already installed.

---

For full instructions on preparing a Linux machine and installing Content Gateway, see [Installing Websense Content Gateway](#) in the [Websense Technical Library](#).

## Installing other Web Security components

For information about installing other Web Security components, see the section “Install additional Web Security components” in the installation instructions for [Web Security Gateway Anywhere](#).

## Installing Data Security components

---

Once you’ve installed Data Security on the TRITON management server, you can install other Data Security components as needed. In larger deployments, you might install supplemental Data Security servers, crawlers, or policy engines. In some scenarios, you might install the Data Security protector and/or any number of Data Security agents such as the printer agent for monitoring printer output or ISA agent for monitoring data on Microsoft ISA servers.

Data Security agents are installed on the relevant servers (ISA agent on the ISA server, printer agent on the print server, etc.) to enable Data Security to access the data necessary to analyze the traffic from these servers. The Data Endpoint agent enables administrators to analyze content within a user’s working environment (PC, laptop, etc.) and block or monitor policy breaches.



**Important**

Before you install a Data Security component—for example, a supplemental server or agent—make sure that the TRITON infrastructure is already installed in your network along with the Data Security management components.

Do not install any Data Security component on a domain controller.

---



This section covers the installation of supplemental Data Security servers. For information on installing other Data Security agents, see the [Data Security Installation Guide](#).

## Installing supplemental Data Security servers

Medium to large enterprises may require more than one Data Security server to perform content analysis efficiently. Having multiple Data Security servers allows your organization to grow, improves performance, and allows for custom load balancing.

Supplemental Data Security server installations include:

- ◆ A policy engine
- ◆ SMTP agent (Windows Server 2003 installations only)
- ◆ Secondary fingerprint repository (the primary is on the management server)
- ◆ Endpoint server
- ◆ Optical Character Recognition (OCR) server
- ◆ Crawler



### Notes:

In production environments, do not install a Data Security server on a Microsoft Exchange, ISA, or print server. These systems require abundant resources.

## Operating system requirements

Supplemental Data Security servers must be running on one of the following operating system environments:

- ◆ Windows Server 2003 (32-bit) Standard or Enterprise R2 SP2
- ◆ Windows Server 2008 (64-bit) Standard or Enterprise R2
- ◆ Windows Server 2012 (64-bit) Standard Edition

## Hardware requirements

Supplemental Data Security servers must meet the following hardware requirements.

Server hardware	Minimum requirements	Recommended
CPU	2 Dual-core Intel Xeon processors (2.0 GHz) or AMD equivalent	2 Quad-core Intel Xeon processors (2.0 GHz) or AMD equivalent
Memory	4 GB	8 GB
Hard drives	Four 72 GB	Four 146 GB
Disk space	72 GB	292 GB
Free space	70 GB	70 GB

Server hardware	Minimum requirements	Recommended
Hardware RAID	1	1 + 0
NICs	1	2

## Software requirements

The following requirements apply to all Data Security servers:

- ◆ For optimized performance, verify that the operating system's file cluster is set to 4096B. For more information, see the Websense knowledge article: "File System Performance Optimization."
- ◆ Windows installation requirements:
  - Set the partition to 1 NTFS Partition. For more information, see the Websense knowledge-base article: "File System Performance Optimization."
  - Regional Settings: should be set according to the primary location. If necessary, add supplemental language support and adjust the default language for non-Unicode programs.
  - Configure the network connection to have a static IP address.
  - The Data Security Management Server host name must not include an underscore sign. Internet Explorer does not support such URLs.
  - Short Directory Names and Short File Names must be enabled. (See <http://support.microsoft.com/kb/121007>.)
  - Create a local administrator to be used as a service account. If your deployment includes more than one Data Security Server, use a domain account (preferred), or the use same local user name and password on each machine.
  - Be sure to set the system time accurately on the TRITON management server.

## Antivirus

Exclude the following directories from antivirus scanning:

- ◆ The folder where Data Security was installed. By default, this is one of the following:
  - Program Files\Websense\
    - Program Files (x86)\Websense\\*.\*
- ◆ \*:\Inetpub\mailroot\\*. \* - (typically at the OS folder)
- ◆ \*:\Inetpub\wwwroot\\*. \* - (typically at the OS folder)
- ◆ C:\Documents and Settings\- ◆ %WINDIR%\Temp\\*. \*

- ◆ The forensics repository (configurable; defaults to Websense folder)



### Note

This document lists the default installation folders. You can configure the software to install to other locations.

The FP-Repository folder is usually located inside the installation folder.

## Port requirements

The following ports must be kept open for supplemental Data Security servers:

### Outbound

To	Port	Purpose
Data Security Management Server	17443	Incidents
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

\* This range is necessary for load balancing.

### Inbound

From	Port	Purpose
Data Security Management Server	8892	Syslog
Data Security Management Server	139	File sharing
Data Security Management Server	445	File sharing
Data Security Management Server	17500-17515*	Consecutive ports that allow communication with Websense agents and machines.

\* This range is necessary for load balancing.

## Installation steps

1. Download the Websense installer (**WebsenseTRITON782Setup.exe**) from [mywebsense.com](http://mywebsense.com).
2. Launch the installer on the machine where you want to install the supplemental server.
3. Accept the license agreement.
4. Select **Custom**.
5. Click the **Install** link for **Data Security**.
6. On the **Welcome** screen, click **Next** to begin the installation.

7. In the **Destination Folder** screen, specify the folder into which to install the server software.

The default destination is C:\Program Files *or* Program Files (x86)\Websense\Data Security. If you have a larger drive, it is used instead. Large removable drives may be detected by the system as a local drive and used as the default. Do not install on removable media.



#### **Important**

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

---



#### **Note**

Regardless of what drive you specify, you must have a minimum of 0.5 GB of free disk space on the C: drive. This is because Data Security installs components into the Windows “inetpub” folder on C:.

---

8. On the **Select Components** screen, select **Data Security Server**.
9. The **Fingerprinting Database** screen appears. To choose a location other than the default shown, use the **Browse** button.
10. The **Virtual SMTP Server** screen appears. This is because an SMTP agent is included with supplemental Data Security server installations.  
In the **Select Virtual Server** list, select the IIS virtual SMTP server that should be bound to the SMTP agent. The SMTP agent will monitor traffic that goes through this virtual server. If there multiple SMTP servers listed, the SMTP agent should typically be bound to Inbound.
11. In the **Server Access** screen, select the IP address to identify this machine to other Websense components.
12. In the **Register with the Data Security Server** screen specify the location and log on credentials for the TRITON management server.  
FQDN is the fully-qualified domain name of a machine. The credentials should be for a TRITON - Data Security administrator with System Modules permissions.
13. In the **Local Administrator** screen, supply a user name and password as instructed on-screen. The server/host name portion of the user name cannot exceed 15 characters.
14. If you installed a Lotus Notes client on this machine so you can perform fingerprinting and discovery on a Lotus Domino server, the **Lotus Domino Connections** screen appears.

If you plan to perform fingerprinting or discovery on your Domino server, complete the information on this page.



### Important

Before you complete the information on this screen, make sure that you:

- ◆ Create at least one user account with administrator privileges for the Domino environment. (Read permissions are not sufficient.)
  - ◆ Be sure that the Lotus Notes installation is done for “Anyone who uses this computer.”
  - ◆ Connect to the Lotus Domino server from the Lotus Notes client.
- 

- a. On the **Lotus Domino Connections** page, select the check box labeled **Use this machine to scan Lotus Domino servers**.
- b. In the **User ID file** field, browse to one of the authorized administrator users, then navigate to the user’s **user.id** file.



### Note

Select a user that has permission to access all folders and Notes Storage Format (NSF) files of interest, otherwise certain items may not be scanned.

---

- c. In the **Password** field, enter the password for the authorized administrator user.
15. In the **Installation Confirmation** screen, if all the information entered is correct, click the **Install** button to begin installation.

Installation may seem to take a long time. Unless a specific error or failure message appears, allow the installer to proceed.

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.*

Clicking **No** cancels the installation.

A similar message for port 443 may appear. Click **Yes** to continue or **No** to cancel the installation.

16. Once installation is complete, the **Installation Complete** screen appears to inform you that your installation is complete. Click **Finish**.
17. Log onto TRITON - Data Security and click **Deploy** to fully connect the supplemental server with the management server.

## Installing Email Security Log Server

---

Websense Email Security Gateway is an appliance-based solution. All components run on the appliance except the Email Security manager (the Email Security module of the TRITON Unified Security Center) and Email Security Log Server. These are the only two Email Security components that may be installed using the Websense installer.

It is recommended that you install Email Security Log Server on a different machine from the TRITON management server:

1. Download and launch the Websense installer on the Log Server machine.
2. Choose the **Custom** installation type.
3. On the **Custom Installation** dashboard, click the **Install** link for Email Security. The Email Security component installer is launched.
4. On the **Introduction** screen, click **Next**.  
The Email Security Installer does not detect TRITON Infrastructure on the machine, and operates in custom mode.
5. In the **Select Components** screen, Email Security Log Server is selected for installation by default. To install Email Security Log Server, SQL Server must already be installed and running in your network. (See [Reporting database](#), page 7, for supported database systems.)

If you choose to install Email Security Log Server, the Email Security Log Server Configuration utility is also installed. This utility can be accessed by selecting **Start > All Programs > Websense > Email Security > Email Security Log Server Configuration**.

6. On the **Email Security Database** screen, specify the location of a database engine and how you want to connect to it.
  - **Log Database IP:** Enter the IP address of the database engine machine. If you want to use a named database instance, enter it the form `<IP address>\<instance name>`. Note that the instance must already exist. See your SQL Server documentation for instructions on creating instances.
  - You may specify whether the connection to the database should be encrypted. Please note the following issues associated with using this encryption feature:
    - You must have imported a trusted certificate to the Log Server machine in order to use the encryption option. See your database documentation for information about importing a trusted certificate.
    - The Bulk Copy Program (BCP) option for inserting records into the Log Database in batches cannot be used. Not using the batch method may affect Log Database performance.
    - The connection from the Email Security module on the TRITON Console to the V-Series appliance cannot be encrypted. If you enable encryption for Log Database, you must disable the SQL Server force encryption feature.
  - **Database login type:** Select how Email Security Log Server should connect to the database engine.

- **Trusted connection:** connect using a Windows trusted connection.
- **Database account:** connect using a SQL Server account.

Then enter a user name and password.

- If using a trusted connection, enter the domain\username of the account to be used. This account must be a trusted local administrator on the database engine machine.
- If using a database account, enter the name of a SQL Server account. This account must have certain roles assigned; see [Installing with SQL Server](#).

When you click **Next**, connection to the database engine is verified. If the connection test is successful, the next installer screen appears.

7. On the **Email Security Database File Location** screen, specify where Email Security database files should be located and then click **Next**.

It is a best practice to use the default location. However, if you want to create the Log Database in a different location (or if you already have a Log Database in a different location), enter the path to the database files.

The path entered here is understood to refer to the machine on which the database engine is located. The path entered must specify a directory that already exists.

If any Email Security components (e.g., TRITON - Email Security or another instance of Email Security Log Server) have already been installed in your deployment, the following message appears:

*The Email Security database exists, do you want to remove it?*

This occurs because the database was created upon installation of the other Email Security components. Click **No** to continue using the existing database. In general, you should keep the database if you are sure the database was created only during the course of installing other components in your current deployment. Clicking **Yes** removes the database.



#### Warning

If any Email Security log data has been written to the database it will be lost if you remove the database. If you want to keep this data, back up the esglogdb76 and esglogdb76\_n databases. See your SQL Server documentation for backup instructions.

---



#### Warning

If you remove the database, any currently quarantined email will no longer be accessible.

---

8. On the **Installation Folder** screen, specify the location to which you want to install Email Security Log Server and then click **Next**.



#### Important

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

---

To select a location different than the default, use the **Browse** button.

Email Security Log Server will be installed in its own folder under the parent folder you specify here.

9. On the **Pre-Installation Summary** screen, review the components to be installed. If they are correct, click **Install**.
10. The **Installing Websense Email Security** screen appears, as components are being installed.
11. Wait until the **Installation Complete** screen appears, and then click **Done**.



# 4

## Initial Configuration

### In this topic:

---

- ◆ [General configuration](#), page 51
  - ◆ [Log on to the TRITON console](#), page 52
  - ◆ [Web Security initial configuration](#), page 53
  - ◆ [Additional configuration for Web Security Gateway Anywhere](#), page 55
  - ◆ [Data Security initial configuration](#), page 57
  - ◆ [Email Security Gateway initial configuration](#), page 58
  - ◆ [Content Gateway initial configuration](#), page 59
  - ◆ [Network Agent and stealth mode NICs](#), page 60
- 

## General configuration

---

- ◆ Some of the ports required by Websense components during installation are no longer needed when installation is complete. For information about the ports required for component communication, as well as details about which components need Internet access, see [Websense TRITON Enterprise default ports](#).
- ◆ To avoid interference with the performance of Websense components, exclude certain Websense folders and files from antivirus scans. See [Excluding Websense files from antivirus scans](#).
- ◆ If administrators use Internet Explorer to access the TRITON Unified Security Center (management console), make sure that Enhanced Security Configuration is disabled on their machines.

For example, in Windows Server 2008:

- a. Open the Server Manager.
- b. Under **Server Summary**, in the Security Information section, click **Configure IE ESC**.
- c. In the **Internet Explorer Enhanced Security Configuration** dialog box, under **Administrators**, select the **Off** radio button, and then click **OK**.

Administrators may also need to restore default settings in their browser in order for the TRITON console to display properly in Internet Explorer. To do this, in Internet Explorer go to **Tools > Internet Options** and select the **Advanced** tab, then click **Reset**. When prompted, click **Reset** again.

## Log on to the TRITON console

---

1. Use a supported browser (see [Requirements, page 7](#)) to launch the TRITON console and log on using the default account:

- a. Navigate to the following URL:

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

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

- b. Log on as the default **admin** account, using the password set during installation.



### Note

Ensure you have installed all the TRITON components that you need in your deployment before you enter subscription keys. If components are missing, the keys will not validate.

---

2. Enter your subscription key or keys. At first startup:
  - The Web Security manager prompts for a subscription key in the Initial Setup Checklist.  
If you have a Web Security Gateway solution, the key you enter is automatically applied to Content Gateway, as well.
  - The Data Security manager displays the subscription key page. See the *Initial Setup* section of the Data Security Help for more information.
  - The Email Security manager prompts for a subscription key. If you do not enter the subscription key in the prompt, you can enter it in the **Settings > General > Subscription** page. See the Email Security Help for more information.

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

3. 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. See the TRITON Console Help for more information.

Continue with the initial configuration steps for the Websense security solutions you have installed:

- ◆ [Web Security initial configuration, page 53](#)
- ◆ [Data Security initial configuration, page 57](#)
- ◆ [Email Security Gateway initial configuration, page 58](#)

- ◆ [Content Gateway initial configuration, page 59](#)

## Web Security initial configuration

### Getting started with Web Security solutions

After entering your Web Security subscription key, use the Initial Setup Checklist to complete basic setup tasks.

- ◆ If you have Web Security Gateway or Gateway Anywhere, also see [Content Gateway initial configuration, page 59](#).
- ◆ If you have Web Security Gateway Anywhere, also see [Additional configuration for Web Security Gateway Anywhere, page 55](#).

Next, you can:

- ◆ Configure transparent user identification on the **Settings > General > User Identification** page (see the “User Identification” topic in the Web Security Help).
  - If you installed Logon Agent, you must create and deploy a client logon script in addition to configuring Logon Agent in the Web Security manager. See the [Using Logon Agent for Transparent User Identification](#) technical paper for instructions.
  - If you were unable to grant User Service, DC Agent, or Logon Agent administrator privileges during installation, see the “Troubleshooting” > “User Identification” topic on changing User Service, DC Agent, and Logon Agent service permissions in Web Security Help.
- ◆ Enable email or SNMP alerting on the **Settings > Alerts > Enable Alerts** page (see the “Alerting” topic in the Web Security Help).
- ◆ Customize reporting behavior (see the “Reporting Administration” topic in the Web Security Help).
- ◆ Configure optional Remote Filtering components to enable filtering of off-site users. For instructions, see the [Remote Filtering Software](#) technical paper.

### Additional tips for working with Web Security solutions

- ◆ All Websense tools and utilities installed on Windows Server platforms (such as wsbackup.exe and websenseping.exe), as well as text editors used to modify Websense 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.
  1. Navigate to the Websense **bin** directory (C:\Program Files (x86)\Websense\Web Security\bin\).
  2. Right-click the relevant executable file, and then click **Properties**. Following is a list of files for which this should be done.

3. In the **Compatibility** tab, under **Privilege Level**, select **Run this program as an administrator**. Then, click **OK**.
- ◆ If you installed Network Agent on a machine with multiple NICs, you can configure the agent to use more than one NIC to monitor and block requests. See the “Network Configuration” topic in Web Security Help for more information. To configure a stealth mode NIC for monitoring, see [Network Agent and stealth mode NICs](#), page 60.

## Identifying Filtering Service by IP address

When Websense software blocks an Internet request, the browser is redirected to a block page hosted by Filtering Service. The block page URL takes the form:

```
http://<FilteringServiceNameorIPAddress>:<MessagePort>/cgi-bin/blockpage.cgi?ws-session=#####
```

If Filtering Service is installed on a machine with multiple NICs, and Filtering Service is identified by machine hostname rather than IP address, users could receive a blank page rather than a block page.

- ◆ If you have an internal domain name server (DNS), enter the Filtering Service machine’s IP address as a resource record in your DNS. See your DNS documentation for instructions.
- ◆ If you do not have an internal DNS:
  1. On the Filtering Service machine, go to the Websense bin directory (by default, **C:\Program Files\Websense\bin** or **opt/Websense/bin**).
  2. Make a backup copy of **eimserver.ini** in another directory.
  3. Open the original **eimserver.ini** file in a text editor.
  4. In the **[WebsenseServer]** section, enter the following command:

```
BlockMsgServerName=<IP address>
```

Here, *<IP address>* is the IP address of the Filtering Service machine.



### Important

**Do not** use the loopback address (127.0.0.1).

---

5. Save the file.
6. Restart Websense Filtering Service.
  - *Windows*: Use the Windows Services dialog box (Start > Administrative Tools > Services) to restart **Websense Filtering Service**.
  - *Linux*: Use the `/opt/Websense/WebsenseDaemonControl` command to restart **Filtering Service**.

## Additional configuration for Web Security Gateway Anywhere

In addition to the items under *Web Security initial configuration*, page 53, perform these procedures if your subscription includes Web Security Gateway Anywhere.

### Confirm Content Gateway registration with Data Security

Content Gateway registers with Data Security automatically. To ensure that registration is successful:

- ◆ Synchronize the date and time on the Content Gateway and Data Security Management Server machines to within a few minutes.
- ◆ If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the communication interface (“C” on a V-Series appliance) 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 V-Series appliance). This is the NIC used by the Data Security 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 Data Security Management Server.
2. In Content Gateway Manager, on the **Configure > My Proxy > Basic > General** page, in the **Networking** section confirm that **Data Security > Integrated on-box** is enabled.
3. Restart Content Gateway to initiate another registration attempt.

Alternatively:

- a. Go to **Configure > Security > Data Security** and enter the IP address of the **Data Security Management Server**.
- b. Enter a user name and password for a Data Security administrator with Deploy Settings privileges.
- c. Click **Register**.

After Content Gateway has registered with Data Security, in Content Gateway Manager go to **Configure > Security > Data Security** and set the following options:

1. **Analyze FTP Uploads:** Enable this option to send FTP uploads to Data Security for analysis and policy enforcement.
2. **Analyze Secure Content:** Enable this option to send decrypted HTTPS posts to Data Security for analysis and policy enforcement. SSL Manager must be enabled on Content Gateway.

These options can be accessed whenever Data Security is registered by going to the **Configure > Security > Data Security > General** page.

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

Data Security and the proxy communicate over ports 17000-17014.

## Configuring the Content Gateway policy engine

When Content Gateway is registered with the Data Security Management Server, a Content Gateway module appears on the Data Security manager System Modules page.

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. From the Data Security manager, select **Settings > Deployment > System Modules**.
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.

---

## Verifying Web and data security linking

When Linking Service is installed, it automatically configures linking between Web and Data Security to allow Data Security access to user identification and URL categorization data.

1. Log onto the Data Security manager.
2. Select **Settings** (under General) > **System > URL Categories & User Names**.

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.

## Data Security initial configuration

---



### Note

TRITON - Data Security may not be available immediately after installation. It takes a few minutes to initialize the system after it is first installed.

To complete your Data Security installation, log onto TRITON - Data Security and click **Deploy**.

See the [Initial Setup](#) section of the TRITON - Data Security Help for information on the following topics:

- ◆ Defining general system settings
  - Connection to directory services
  - System alerts
- ◆ Setting up notifications
  - Notifications when policy breaches occur
- ◆ Configuring Web attributes
  - Web DLP policies
  - Policies for particular Web sites
  - Policy owners
- ◆ Configuring email policies
- ◆ Creating a regulatory and compliance policy
- ◆ Configuring system modules
  - Viewing Data Security modules
  - Configuring the protector
- ◆ Deploying your settings

## Email Security Gateway initial configuration

---

### Email Security Gateway initial configuration

The first time you access TRITON - Email Security, you are prompted for your subscription key. Then, you are asked if you want to use the First-Time Configuration Wizard. This wizard guides you through the process of entering some essential configuration settings. It is strongly recommended you use this wizard. See the TRITON - Email Security Help for more information about the wizard.



---

**Important**

The configuration wizard is offered only once, at initial start up of TRITON - Email Security. If you choose to not use the wizard it will no longer be available. All settings configured in the wizard can be configured in TRITON - Email Security individually. The wizard simply offers a more convenient way to enter some initial settings.

---

See the [Getting Started](#) section in TRITON - Email Security Help for information on initial configuration in the following areas:

- ◆ First-time Configuration Wizard, for establishing
  - An initial mail route for a protected domain
  - Trusted IP addresses for which some inbound email analysis is not performed
  - Email Security Log Server IP address and port
  - System notification email address
- ◆ Websense Data Security registration, to allow the use of email data loss prevention (DLP) policy options
- ◆ Master database download scheduling, to manage spam and virus filter updates

For help with the following Email Security settings, see the [Configuring System Settings](#) section in the Email Security Help:

- ◆ Administrator management, to modify administrator roles established in the TRITON Unified Security Center
- ◆ System settings, to establish system preferences like the SMTP greeting and console language settings
- ◆ Appliance management, for administering all the appliances in your network
- ◆ User directory creation and management
- ◆ Protected domain and trusted IP address lists, to designate all the domains that you want Email Security Gateway to protect and the IP addresses whose mail can bypass some email analysis
- ◆ User authentication and recipient validation options



- ◆ Transport Layer Security (TLS) certificate handling, to provide an extra layer of security for email communications
- ◆ Email Security manager backup and restore functions, to preserve important configuration files, including your appliances list, administrator settings, and report templates
- ◆ System alerts, to configure delivery methods for distributing various Email Security system health alerts

## Email Security Gateway Anywhere initial configuration

If your subscription includes Email Security Gateway Anywhere, you need to register with the email hybrid service. See the [Registering for the hybrid service](#) topic in the Email Security Help for descriptions of email hybrid service registration.

After you have registered with the hybrid service, you can configure Hybrid Service Log properties and view the Hybrid Service Log. See Email Security Help for details.

## Content Gateway initial configuration

After Content Gateway is installed, perform these basic configuration activities:



### Note

The subscription key is **automatically applied** to Content Gateway when you enter it in the Web Security manager.

- ◆ 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, configure [Web Security user identification](#).
- ◆ Configure the real-time [Scanning Options](#) in TRITON – Web Security.
- ◆ If you enabled content caching during installation, [configure content caching](#).

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

- ◆ When HTTPS (SSL Manager) is used, in TRITON – Web Security 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)

## Network Agent and stealth mode NICs

---

Websense software can inspect all packets with a monitoring NIC (network interface card) that has been configured for *stealth mode*. A NIC in stealth mode has no IP address and cannot be used for communication. Security and network performance are improved with this configuration. Removing the IP address prevents connections to the NIC from outside resources and stops unwanted broadcasts.

If Network Agent is configured to use a stealth-mode NIC, the installation machine must have multiple NICs. If Network Agent is installed on a separate machine, a second, TCP/IP-capable interface (i.e., it is not in stealth mode) must be configured to communicate with Websense software for filtering and logging.

During installation, stealth-mode interfaces do not display as a choice for Websense communications. Make sure you know the configuration of all the interfaces in the machine before attempting an installation.



### Important

On Linux, stealth mode NICs appear together with TCP/IP-capable interfaces and must not be selected for communication.

---

Stealth mode for the Network Agent interface is supported on Windows and Linux.

## Windows

Configure a NIC for stealth mode as follows.

1. Go to **Start > Settings > Network and Dial-up Connection** to display a list of all the interfaces active in the machine.
2. Select the interface you want to configure.
3. Select **File > Properties**.  
A dialog box displays the NIC connection properties.
4. Clear the **Internet Protocol (TCP/IP)** checkbox.
5. Click **OK**.

## Linux

To configure a NIC for stealth mode in Linux, disable the Address Resolution Protocol (ARP), which breaks the link between the IP address and the MAC address of the interface. Run the following commands, replacing *<interface>* with the NIC's name, for example, `eth0`.

- ◆ To configure a NIC for stealth mode, run this command:

```
ifconfig <interface> -arp up
```

- ◆ To return the NIC to normal mode, run this command:

```
ifconfig <interface> arp up
```



### Important

Network Agent can work with a stealth mode NIC only if the interface retains its old IP address in the Linux system configuration file, `/etc/sysconfig/network-scripts/ifcfg-<adapter name>`.

---

