

# v7.8.4 Release Notes for Websense® Web Security

Topic 50700 | Release Notes | Web Security Solutions | Updated 26-Aug-2014

<b>Applies to:</b>	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.4
--------------------	--

Use the Release Notes to find information about what's new and improved for Websense Web Security solutions in version 7.8.4.

- ◆ *[New in Websense Web Security v7.8.4, page 2](#)*
- ◆ *[Installation, page 6](#)*
- ◆ *[Operating tips, page 11](#)*
- ◆ *[Resolved and known issues, page 12](#)*

For information about Web Endpoint, please refer to the [Release Notes for Websense Web Endpoint](#).

For information about Data Endpoint, please refer to the [Release Notes for Websense Data Security](#).

# New in Websense Web Security v7.8.4

Topic 50701 | Release Notes | Web Security Solutions | Updated 26-Aug-2014

<b>Applies to:</b>	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.4
--------------------	--

The Web Security Help is available in both English and Japanese. Select your Help system language on the TRITON Settings > My Account page in the TRITON console.

## Security

---

Some previous versions of Websense Web Security included an OpenSSL version that includes the man-in-the-middle (MITM) vulnerabilities (CVE-2014-0224). Exploiting this vulnerability, an attacker that is capable of intercepting communications between a vulnerable client and server can exploit an MITM attack, allowing the attacker to transparently decrypt and modify traffic to and from both client and server. In version 7.8.4 of Websense Web Security, the vulnerable version of the OpenSSL libraries has been replaced with a fixed version.

## IPv6 Support

---

Support for IPv6 has been enhanced to include Web Security reporting tools.

IPv6 information is now included in standard logging data. Log Server will receive log records from Filtering Service or Websense Multiplexer and then store destination IPv6 addresses and source IPv6 addresses in the Log Database for use in reporting. A user's IPv6 address is shown in the user name field when user name information is not available for a client.

IPv6 addresses:

- ◆ Will display on presentation reports and charts and investigative reports that include source IP addresses, destination IP addresses, or user information.
  - When these reports are scheduled, they will process and send data that include IPv6 addresses.
  - Reports containing IPv6 addresses can also be exported to PDF, Excel, or HTML.
- ◆ Can also be used on the **Clients** tab of the **Presentation Reports > Edit Report Filter** page. They can also be used in the **Search** features of investigative reports.
- ◆ Display on application reports and charts.

- ◆ Display on the **Status > Dashboard** charts, including **Threats > Event Details** page, that include source IP addresses, destination IP addresses, or user information.
- ◆ Are used in the calculation of Internet browse time for websites with IPv6 addresses.
- ◆ Will be included in the uncategorized and security URLs collected by WebCatcher.
- ◆ Will display in Real-Time Monitor information.
  - IPv6 addresses can be used as a filter.
  - Columns that include IPv6 addresses will be sorted effectively.
- ◆ Are included in the records forwarded to any Security Information and Event Management (SIEM) integration you have enabled.

To support the IPv6 feature, a new Log Database logging partition will be added to your database when you upgrade to v7.8.4. The Log Database is upgraded when Log Server is upgraded. Reports can still be run against existing logging partitions.

Please refer to the list of supported versions of SQL Server in [Requirements overview](#).

## Incremental Upgrades

---

Beginning with v7.8.4, the upgrade process for Websense Web Security solutions no longer requires all machines and components to be upgraded simultaneously. Your deployment will continue to function normally as it is upgraded over a period of time. Policy enforcement, logging, and reporting will continue as the incremental upgrade progresses.

The incremental upgrade process is based on the ability to upgrade one “logical deployment unit” at a time. Each logical deployment unit is made up of a Policy Server instance and all components that rely on it.

See the new [Incremental Upgrade](#) guide for details, including requirements that must be met prior to upgrading, steps to complete an incremental upgrade, and the limitations and restrictions associated with it.

## Single sign-on using PingFederate (hybrid)

---

A single sign-on feature has been added to provide authentication using a third-party identity provider that communicates with your directory service. Designed to work for hybrid configurations, this version of single sign-on supports only PingFederate as the identity provider.

Single sign-on provides clientless transparent authentication via a gateway hosted on your network. Clients connecting to the hybrid proxy from a filtered location are redirected to PingFederate. Once users are authenticated against your directory service, they are directed back to the proxy and the appropriate policy is applied.

Clients who have authenticated once do not have to authenticate again for subsequent browsing sessions.

PingFederate supports only the Proxy Auto-Configuration (PAC) file assigned to port 8082. It will not use the PAC file assigned to port 80.

When Ping Federate is used as the identity provider, single sign-on cannot fall back to secured form authentication.

Single sign-on using PingFederate has been certified on:

- ◆ Red Hat Enterprise Linux 6.5
- ◆ Microsoft Windows Server 2012 R2
- ◆ V-Series appliances
- ◆ Client browsers on Microsoft Windows 7 (64-bit), 8.1 (64-bit), and 8.0 (64-bit)
  - Internet Explorer 11
  - Firefox 30
  - Chrome 35

In addition, single sign-on using PingFederate is supported on:

- ◆ Red Hat Enterprise Linux 5 and 6
- ◆ Microsoft Windows Server 2008, 2008 R2, and 2012
- ◆ Client browsers
  - Internet Explorer 8, 9, and 10
  - Firefox 4.4 or higher
  - Chrome 13 or higher

See [Integrating a single sign-on identity provider](#) in Web Security Help for details on how to set up single sign-on. See also [Configuring single sign-on](#) in TRITON Cloud Security Help for additional information.

## **Logon application support**

---

Logon Agent communicates with the logon application (LogonApp) on client machines to identify users as they log onto or off of Windows domains.

The logon application supports the following operating systems:

- ◆ Mac OS X 10.9.2 (64-bit)
- ◆ Microsoft Windows 8.1 Update 1 (32-bit and 64-bit; Windows 8.1 RT is not supported)

For more information about Logon Agent and the logon application, see the [Using Logon Agent for Transparent User Identification](#) white paper.

## Third-party platform and product support

---

This version introduces support for:

- ◆ Internet Explorer 10, standards mode
- ◆ Internet Explorer 11, standards mode
- ◆ Firefox 30
- ◆ Chrome 35

Note that installing Web Security components on Windows Server 2012 or 2012 R2 requires Microsoft .NET Framework v3.5. Install .NET Framework v3.5 before running the TRITON Unified installer.

# Installation

Topic 50702 | Release Notes | Web Security Solutions | Updated 26-Aug-2014

<b>Applies to:</b>	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.4
--------------------	--

## Requirements overview

---

Most Websense Web Security components can be run on the following operating systems:

- ◆ Microsoft Windows Server 2008 R2, 2008 R2 SP1, 2012, or 2012 R2



### Important

Before installing any components, make sure that .NET Framework 3.5 is installed on the machine.

- ◆ Red Hat Enterprise Linux 6.x (64-bit)

The following components run on Windows platforms only:

- ◆ TRITON Unified Security Center
- ◆ Linking Service
- ◆ Web Security Log Server
- ◆ DC Agent
- ◆ Real-Time Monitor

Websense Content Gateway is a Linux-only component that requires Red Hat Enterprise Linux 6.2, 6.3, 6.4 or 6.5.

In appliance-based deployments, in addition to the Windows-only components, the following components, when used, must be installed off-appliance:

- ◆ Sync Service
- ◆ Remote Filtering Server and Client

Note that while the Remote Filtering Client Pack option no longer appears in the installer, the utility used to configure Remote Filtering Client is included automatically on any Windows server that includes Web Security components. See the [Remote Filtering Software](#) technical paper for details.

- ◆ Transparent identification agents (eDirectory Agent, Logon Agent, RADIUS Agent)

To enable Web Security reporting tools, use one of the following certified database engines:

- ◆ Microsoft SQL Server 2012 SP2 (or the latest service pack from Microsoft) Standard, Business Intelligence, or Enterprise



#### Important

SQL Server 2012 uses a different security model than previous versions. To successfully create the Log Database in SQL Server 2012, you must either:

- ◆ Install the database in the default SQL Server folder.
  - ◆ Grant the database engine full control over the folder that will host the database before you install Log Server.
- 

- ◆ Microsoft SQL Server 2008 SP3 (or the latest service pack from Microsoft) Standard or Enterprise
- ◆ Microsoft SQL Server 2008 R2 SP2 (or the latest service pack from Microsoft) Standard or Enterprise
- ◆ For very small networks and evaluation environments, SQL Server 2008 R2 Express SP 2 (packaged in the TRITON Unified Installer).

Websense Web Security and Web Filter can be integrated with the following third-party firewall, proxy, and caching applications:

Product	Versions
Microsoft Forefront TMG	2008 or later
Cisco ASA	v8.0 or later
Cisco Router	IOS v15 or later
Citrix XenApp	5.0, 6.0, or 6.5

In addition, this release supports integration with Bluecoat ProxySG using the ICAP protocol, via the Websense ICAP Service.

This version does **not** support integration with Check Point products, Cisco PIX Firewall, or Cisco Content Engine.

See [System requirements for this version](#) in the Deployment and Installation Center for detailed hardware and software requirements.

# Installation overview

---

The number of steps required to install Websense Web Security Solutions depends on the hardware platforms used in your environment, the size of your network, and how widely you plan to deploy components.

As a best practice, for software component installation, log in as a domain and local administrator to run the installer.

At its simplest, a software installation requires you to:

1. Download the TRITON Unified Installer (**WebsenseTRITON784Setup.exe**).
2. Run the installer on a robust Windows Server 2008 R2, 2008 R2 SP1, 2012, or 2012 R2 machine.
3. Select the **Websense Web Security All installation** option.

All components required for a basic Websense Web Security deployment are installed on the selected machine, including the TRITON Unified Security Center and, if no other Microsoft SQL Server instance is identified in your network, SQL Server 2008 R2 SP2 Express.

A simple appliance deployment requires you to:

1. Run the **firstboot** script and configure the full policy source appliance.
2. Download the TRITON Unified Installer (**WebsenseTRITON784Setup.exe**).
3. Run the installer on a Windows Server 2008 R2, 2008 R2 SP1, 2012, or 2012 R2 machine.
4. Select the **TRITON Unified Security Center** radio button, and the **Web Security** check box beneath it.

Installing the TRITON Unified Security Center requires Microsoft SQL Server. If an existing SQL Server instance is not available, SQL Server 2008 R2 SP2 Express is installed.

5. Run the TRITON Unified Installer again (on the TRITON Management Server or another machine) and select **Custom**, then **Web Security** to install off-appliance components that are not part of the TRITON console, like transparent identification agents.

For a typical software deployment, expect to run the TRITON Unified Installer (or the TRITON Unified Installer plus the Web Security Linux Installer) on at least 3 machines:

1. Use the TRITON Unified Installer or Web Security Linux Installer to perform a **Custom** installation for core filtering components (Policy Broker, Policy Server, Filtering Service, Network Agent, User Service, Usage Monitor) on a supported Windows or Linux machine.
2. Use the TRITON Unified Installer to perform a **TRITON Unified Security Center > Web Security** installation to install core management components and reporting tools on a supported Windows machine.

Installing the TRITON Unified Security Center requires Microsoft SQL Server. If an existing SQL Server instance is not available, SQL Server 2008 R2 SP2 Express is installed.

3. Use the TRITON Unified Installer to perform a **Custom > Web Security** installation of Web Security Log Server on a supported Windows machine.

Start-to-finish installation instructions covering most typical deployments are available in PDF format:

- ◆ [Installation Instructions: Web Security Gateway Anywhere](#)
- ◆ [Installation Instructions: Web Security Gateway](#)
- ◆ [Installation Instructions: Web Security or Web Filter](#)

## Upgrade overview

---

To upgrade to Websense Web Security Version 7.8.4:

- ◆ Your current deployment must be at Version 7.6 or later. (Software deployments can upgrade directly to v7.8.4.)
- ◆ All components that you want to upgrade (rather than install separately after core components are upgraded) must be on a supported operating system. This may require:
  1. Reinstalling your existing version of Policy Broker and Policy Server on a platform supported in v7.8.4.
  2. Migrating policy and configuration settings to the new installation on the new platform. (See [Migrating Web Security management components.](#))
  3. Running the upgrade process.
- ◆ If your Web Security solution is integrated with a third-party firewall, proxy, or cache, make sure that it is supported in this version. If you are using an integration product that is no longer supported, update the integration product before starting the upgrade process.
- ◆ If you are using a version of Microsoft SQL Server prior to 2008, it is recommended that you upgrade the database to a certified version.

Once all components are on a supported platform, the third-party integration (if any) is up-to-date, and a supported database engine is in place, upgrade your Web Security components in the following order:

1. Upgrade the Policy Broker machine (or full policy source appliance). If upgrading from 7.8.1 or later, this would be the primary (or standalone) Policy Broker machine.
2. If upgrading from 7.8.1 or later, upgrade any replica Policy Broker machines you may have.
3. Upgrade any Policy Server machines that do not have a Policy Broker installed.
4. Upgrade the Web Security Log Server machine (if different from the Policy Broker or Policy Server machine).

To support the IPv6 feature, an upgrade to 7.8.4 will create a new Log Database logging partition in your database.

5. Upgrade the TRITON Management Server (if on a separate machine from Policy Broker, Policy Server, or Log Server).
6. Upgrade any user directory and filtering appliances. If you have multiple user directory and filtering appliances, the upgrade processes can run in parallel.
7. Upgrade any filtering only appliances. If you have multiple filtering only appliances, the upgrade processes can run in parallel. (Be sure that all Policy Server instances, on and off appliance, have been upgraded before you upgrade filtering only appliances.)
8. Upgrade all other machines hosting Web Security software. If there are multiple other Web Security machines, the upgrade processes can run in parallel.
9. Upgrade Remote Filtering Client and Web Endpoint on client machines (if used).

## Downloading the installer

---

To download the TRITON Unified Installer or Web Security Linux Installer:

1. Go to [mywebsense.com](https://mywebsense.com) and log in to your account.  
You are taken to the My Products and Subscriptions page.
2. Click the **Downloads** tab.
3. Under Download Product Installers, select your **Product** and **Version** (7.8.4).  
The available installers are listed under the form.
4. Click the plus sign (“+”) next to an installer entry for more information about the installer.
5. Click the **download** link to download the installer.

Note that the TRITON Unified Installer is very large (approximately 1.6 GB), so if you have a slower network connection, it may take some time to download.

## Installation and upgrade tools and references

---

- ◆ Deployment and Installation Center: [Web Security Installation](#)
- ◆ Deployment and Installation Center: [Web Security Upgrade](#)
- ◆ Web Security [Default Ports](#)

# Operating tips

Topic 50703 | Release Notes | Web Security Solutions | Updated 26-Aug-2014

<b>Applies to:</b>	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.4
--------------------	--

To improve your experience with the Web Security manager:

- ◆ Disable all browser pop-up blocking features.
- ◆ If you have problems accessing the console from Internet Explorer:
  1. Make sure that Internet Explorer Enhanced Security Configuration (IE ESC) is disabled.
  2. If problems continue, reset Internet Explorer to its default configuration. To do this, in Internet Explorer, go to **Tools > Internet Options** and select the **Advanced** tab, then click **Reset**. When prompted, click **Reset** again.
- ◆ Make use of the quick start tutorials offered from the Getting Started section of the TRITON console Help menu.
  - If this is your first experience with Websense Web Security, use the New Admin Quick Start tutorial to learn about policy creation and reporting.
  - If you have used previous Web Security versions, use the Upgrading Admin Quick Start tutorial to orient yourself to what has changed in this version.
- ◆ Avoid using the browser Back and Refresh buttons. Instead, use the breadcrumbs at the top of the page or the left and right navigation panes.
- ◆ **Click OK at the bottom of each page in the Web Security manager to cache changes made on the page.**

In some instances, when you are performing secondary tasks, you must click OK on the secondary page, and then click OK again on the main page to cache your changes. Make sure you see the “Changes have been cached” success message.
- ◆ Click **Save and Deploy** to implement cached changes.

It can take up to 30 seconds for all Websense components to be updated with the changes.

**To improve your experience with Websense reporting tools:**

- ◆ If you install the TRITON management server first, and then install Log Server, you must manually restart the **Websense TRITON - Web Security** service on the TRITON management server machine. This ensures that reporting data appears in the Web Security manager, and that scheduled jobs are properly stored in the Log Database.
- ◆ If you are using Internet Explorer 8, make sure that Compatibility View (the button between the URL and the Refresh button in the browser address bar) is turned **off**.

# Resolved and known issues

Topic 50704 | Release Notes | Web Security Solutions | Updated 26-Aug-2014

---

<b>Applies to:</b>	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.4
--------------------	--

---

A list of [resolved and known issues](#) in this release is available to Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere customers.

If you are not currently logged in to MyWebsense, clicking the link brings up a login prompt. Log in to view the list.