v7.7.3 Release Notes for Websense® Web Security

Topic 55406 | Release Notes | Web Security Solutions | Version 7.7.3 | Updated 18-January-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.3

Use the Release Notes to find information about what's new and improved in Websense Web Security Version 7.7.3.

New in Websense Web Security v7.7.3

Topic 50231 | Release Notes | Web Security Solutions | Version 7.7.3 | Updated 18-Jan-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.3

Remote Filtering Client support for Mac OS X

Websense remote filtering software enables enforcement of Web Security policies on machines that reside outside your network. It includes a server component

- **Remote Filtering Client** is installed on each machine that will be filtered when used outside the network.
- **Remote Filtering Server** resides inside your firewall, and acts as a proxy to Websense Filtering Service.

This version adds support for Remote Filtering Client on machines running Mac OS X 10.6 or later.

Use the Websense Endpoint Package Builder to create Mac OS X installation packages for Remote Filtering Client. Note that the Package Builder runs only on Windows, even when it is being used to create installation packages for Mac.

By default, the Package Builder files are installed in the following directory on any Windows server that includes Websense components (including the TRITON management server and the Log Server machine):

```
Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\
```

To create an installation package:

1. Navigate to the folder containing the configuration tool (by default, Websense\Web Security\DTFAgent\RemoteFilteringAgentPack\) and double-click **WECfg.exe**.

   The Websense Endpoint Package Builder opens.

2. Mark the **Web security endpoint clients** check box, then select **Remote Filtering Client**. Also select a language from the drop-down list at the bottom of the page. This is the language used to display messages to the end user (if any such messages are enabled).

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

3. Select one or more operating systems (**Mac 64bit**, **Mac 32bit**,**Windows 32-bit**, **Windows 64-bit**) for which to create an installation package, then enter and confirm the anti-tampering **Password** that administrators may use to modify or uninstall the Remote Filtering Client. Also specify whether or not to **Protect the installation directory from modification or deletion**.

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

4. Specify the installation path for Remote Filtering Client on end user machines.
   - Select **Use the default location** to install Remote Filtering Client in the directory displayed in the tool. This should be the **/Applications** directory. Do not change this path.
5. On the Internal Connections screen, enter the internal **IP address or hostname** and internal **Port** of each Remote Filtering Server to which this client will connect. Use the > button to move the information to the selected list. When you are finished, click **Next**.

   Remote Filtering Client sends its heartbeat to these IP addresses and ports to determine whether or not it is inside the network.

   If you have multiple Remote Filtering Server instances, Remote Filtering Client rotates through the list in order until a functioning server is located.

   Remote Filtering Server has a 2-minute inactivity timeout period. If the client connects, and then does not send an Internet request in the timeout period, the server drops the connection. When the next request is made, Remote Filtering Client goes through its list to connect again. This protects server performance by reducing the number of unused connections that might otherwise accumulate.
6. On the External Connections screen, enter the external **IP address or hostname** and **Port** of each Remote Filtering Server listed on the previous screen. Use the > button to move the information to the selected list.

   Each server must be identified by an externally visible IP address or fully qualified domain name (FQDN).

   

   Important

   Be sure to use the **same format** (IP address or FQDN) that you used when installing Remote Filtering Server.

   When Remote Filtering Client is outside the network, filtering requests are sent to Remote Filtering Server via the specified IP address or FQDN and port.
7. Indicate whether or not to **Log user Internet activity** seen by Remote Filtering Client instances installed using this customized installation package, and then click **Next**.
8. Use the **Trusted Sites** list to enter up to 4 URLs, IP addresses, or regular expressions for sites that Remote Filtering Client users can access directly, without being filtered or logged. Click **Add** to enter a URL, IP address, or regular expression.

   When you are finished, click **Next**.
9. Indicate whether or not to **Notify users when HTTPS or FTP traffic is blocked**, then, if notification is enabled, specify how long (in seconds) the message is displayed.
10. Enter and confirm the **Pass phrase** used for communication with Remote Filtering Server. This must match the pass phrase created when Remote Filtering Server was installed.

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

11. Specify a **Save location** for the new installation package. Enter a valid directory path or click **Browse** to navigate to the path.
12. Click **Finish**.

The new installation package can now be used to deploy Remote Filtering Client to users' machines.

To deploy the software:

1. Copy the Mac installation package (ZIP file) to the client machine and unzip the package.
2. To start the installation, double-click **WebsenseEndpoint.pkg**.
   - The **RFAdmin.hsw** and **RFClient.hsw** settings files must reside in the same directory as the installer package (pkg) file in order to install Remote Filtering Client.
   - Local administrator permissions are required to install the client software.
3. Follow the onscreen instructions to install Remote Filtering Client.

To uninstall Remote Filtering Client on Mac machines:

1. Open **System Preferences** and locate the **Websense** preference pane (in the "Other" section).
2. Click **Uninstall Endpoint**.
   - Local administrator permissions are required to remove the client software.
   - If an anti-tampering password was set in the Package Builder, the administrator must enter the password to uninstall the client software.

Web Endpoint support for Mac OS X

Websense Web Security Gateway Anywhere customers can install Websense Web Endpoint software on client (end-user) machines to:

- Enforces the use of the hybrid service for Web filtering.
- Pass authentication information to the hybrid proxies, enabling secure transparent authentication.

This version adds support for Web Endpoint on client machines running Mac OS X 10.6 or later.

To enable Web Endpoint deployment:

1. Log on to TRITON - Web Security and navigate to the **Settings > Hybrid Configuration > Hybrid User Identification** page.
2. Mark **Enable installation and update of Web Endpoint on client machines**.

   This allows you to configure Web Endpoint deployment and automatic update settings. If you later deselect this option, any installed endpoint clients continue to work until they are uninstalled, though they no longer receive automatic updates.

3. Enter and confirm your anti-tampering password. This password:
   - Protects endpoint files and folders from being deleted or renamed.
   - Is required to uninstall the endpoint or stop the endpoint service.

   You are required to define an anti-tampering password before you can download endpoint software. The password is automatically linked to your endpoint deployment.

   

   Important

   For security reasons, Websense does not retain a copy of your anti-tampering password. If you forget your password, you can reset it on the Settings > Hybrid Configuration > Hybrid User Identification page in TRITON - Web Security. After you enter and confirm a new password, all installed endpoints are updated to use the new password next time they connect to the Internet.

4. Click **Deploy Web Endpoint Manually**. This is the only deployment option applicable for Mac versions of the Web Endpoint. With this option, you can:
   - Download or copy the files onto individual client machines, then launch the installer by double-clicking the package.
   - Download or copy the files onto a Mac machine, then use Apple Remote Desktop software to distribute the installation package.
5. Click **View Web Endpoint Files**, then select a client operating system (**Mac 64bit**, **Mac 32bit**) from the drop-down list.
6. Click a filename to start the download.

   You can also view a PDF of the release notes for each version by clicking a release notes link. Click **Close** when done.
7. Mark **Automatically update endpoint installations when a new version is released** if you want to ensure that all endpoints on your client machines always have the latest version when it is available from the hybrid service.
8. Click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

To deploy Web Endpoint to Mac clients:

1. Download the installation package via TRITON - Web Security (as described above), and copy the files to the machine:
   - On which you want to install Web Endpoint
   - From which you want to deploy Web Endpoint to other Mac clients
2. Use either of the following methods to install the client software:
   - Use Apple Remote Desktop to deploy the file to other Mac clients.
   - Double-click the downloaded endpoint package to launch the installer.

Administrator permissions are required to install the endpoint client software.

Remote Filtering Client support for Windows 8

Remote Filtering Client can be installed on client (end-user) machines running Windows 8.

Internet Explorer Desktop UI mode is supported on the Windows 8 client machines (Metro UI mode is not supported with version 7.7.3).

Web Endpoint support for Windows 8

Websense Web Security Gateway Anywhere customers can install Websense Web Endpoint software on client (end-user) machines running Windows 8.

Internet Explorer Desktop UI mode is supported on the Windows 8 client machines (Metro UI mode is not supported with version 7.7.3).

Use GPO or local deployment to install the Web Endpoint. Do not install from the hybrid cluster.

Web Endpoint not supported yet with Firefox 18

Websense Web Security Gateway Anywhere customers using Websense Web Endpoint software should note that Firefox 18 is not yet supported for Web endpoint or Data endpoint clients with TRITON version 7.7.3. This support is planned for the future; customers will be informed when it becomes available.

Installation and upgrade

Topic 50232 | Release Notes | Web Security Solutions | Version 7.7.3 | Updated 18-January-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.3

Requirements overview

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

- Microsoft Windows Server 2008 (32-bit) or 2008 R2
- Red Hat Enterprise Linux 5.x (32-bit) or 6.x (32-bit and 64-bit)

The following components run on Windows platforms only:

- TRITON Unified Security Center

  There is one exception to this limitation. TRITON - Web Security 7.7.x can also run on a Websense appliance. In most cases, this deployment option should be used only for evaluation purposes, and not in production environments.
- Linking Service
- Log Server
- DC Agent
- Real-Time Monitor

Websense Content Gateway is a Linux-only component.

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 Deployment and Installation Center or Remote Filtering Software technical paper for details.
- Transparent identification agents (eDirectory Agent, Logon Agent, RADIUS Agent, *plus DC Agent, which runs only on Windows)*

To enable Web Security reporting tools, one of the following supported database engines must be used:

- Microsoft SQL Server 2008 or 2008 R2 Standard or Enterprise
- Microsoft SQL Server 2005 SP4 Standard or Enterprise
- Microsoft SQL Server 2008 R2 Express (installed using 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 PIX Firewall	v5.3 or later
Cisco ASA	v7.0 or later
Cisco Content Engine	ACNS v5.5 or 5.6
Cisco Router	IOS v12.3 or later

Product	Versions
Check Point	Firewall-1 NGX or NGX 65; UTM-1 (VPN-1) Edge
Citrix XenApp	5.0 or 6.0

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

This version does **not** support:

- Squid Web proxies
- Microsoft ISA Server
- Citrix Presentation Server

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 a new software component installation, log in as a domain and local administrator to run the installer.

At simplest, a new software installation requires you to:

1. Download the TRITON Unified Installer (see *Downloading the installer*, page 12).
2. Run the installer on a robust Windows Server 2008 (32-bit) or 2008 R2 machine.
3. Select the **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 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 (see *Downloading the installer*, page 12).
3. Run the installer on a Windows 2008 R2 server. Note that Windows Server 2008 32-bit is still supported for Web Security console (only) at 7.7.3.
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 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 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.

See the Deployment and Installation Center for more detailed information.

Installing Web Filter components on Red Hat Linux 6.x 64-bit

If you plan to install Web Filter or Web Security components on a Red Hat Linux v6.x machine, you must first install compatibility modules. In v6.x, Red Hat packages 32-bit versions of its system libraries in an add-on module (rather than installing them by default as in previous releases).

1. On the machine where you are installing Web Filter, set up a Yum repository for the 32-bit compatibility libraries.
   a. Mount the Red Hat Enterprise Linux installation DVD to the folder **/mnt/cdrom**.
   b. Create a file named **RH62-Media.repo** in the **/etc/yum.repos.d** folder.
   c. Add following content to **RH62-Media.repo** and save the file.

      ```
      [RH62-Media]
      name=RedHat-$releasever - Media
      baseurl=file:///mnt/cdrom
      gpgcheck=0
      enabled=1
      ```
   d. Run the following command:

      ```
      # yum clean all
      ```

2. Install the required library packages:

```
yum install libuuid.i686
yum install compat-libcap1-1.10-1.i686
yum install gdbm.i686
yum install libidn.i686
yum install libXtst-1.0.99.2-3.el6.i686
yum install libpam.i686
```

Network Agent on Red Hat Linux 6.x 64-bit

If you plan to install Network Agent on a server running RHEL6.3-x64, you will need two additional system library files for 32-bit compatibility before installation. Without the missing files, the installer skips the step that handles Network Card Selection for Network Agent.

1. Locate the two files listed below from your RHEL ISO image or CD-ROM:

   libstdc++-4.4.6-4.el6.i686.rpm

   libgcc-4.4.6-4.el6.i686.rpm
2. Install the rpm packages:
   a. run: rpm -ivh libstdc++-4.4.6-4.el6.i686.rpm
   b. run: rpm -ivh libgcc-4.4.6-4.el6.i686.rpm
3. Run the TRITON Unified Installer and select the Web Security components you wish to install on the RHEL6.3-x64 computer.

Upgrade overview

The following table indicates the upgrade paths for Web Filter, Web Security, and Web Security Gateway on Websense appliances as well as your local server (software upgrades).

Your Current Version	Step One	Final Step
Web Security Gateway on V-Series 7.7.0	Direct upgrade to 7.7.3	Done
Web Security Gateway on V-Series 7.6.x	Upgrade to 7.7.0	Upgrade to 7.7.3
Web Security Gateway on V-Series 7.5.x	Upgrade to 7.6.0, then 7.7.0	Upgrade to 7.7.3
Web Security Gateway software 7.5.x (no appliance)	Direct upgrade to 7.7.3	Done
Web Security Gateway software 7.6.x, 7.7.0 (no appliance)	Direct upgrade to 7.7.3	Done
Web Filter or Web Security software 7.5.x, 7.6.x, 7.7.0	Direct upgrade to 7.7.3	Done
Content Gateway software 7.6.x, 7.7.0	Direct upgrade to 7.7.3	Done
All upgrade paths require upgrade to TRITON management console 7.7.3.		

To upgrade directly to Websense Web Security Version 7.7.3:

- Your current software deployment must be at Version 7.5 or later. V-Series appliances require this path: 7.5.x > 7.6.0 >7.7.0 > 7.7.3.
- All components that you want to upgrade (rather than those you plan to 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 v7.7.3.
  2. Migrating policy and configuration settings to the new installation on the new platform.
  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 MSDE, or a version of Microsoft SQL Server prior to 2005 SP4, upgrade the database to a supported 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).

2. Upgrade the Web Security Log Server machine (if different from the Policy Broker machine).
3. Upgrade the TRITON Management Server (if on a separate machine from Policy Broker or Log Server).
4. Upgrade any secondary (user directory and filtering or filtering only) appliances. If you have multiple secondary appliances, the upgrade processes can run in parallel.
5. Upgrade all other machines hosting Web Security software. If there are multiple other Web Security machines, the upgrade processes can run in parallel.
6. Upgrade Remote Filtering Client and Web Endpoint on client machines (if used).

Downloading the installer

To download the TRITON Unified Installer, Web Security Linux Installer, or TMG plug-in installer:

1. Go to 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** (7.7.3).

   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 50233 | Release Notes | Web Security Solutions | Version 7.7.3 | Updated 18-January-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.3

To improve your experience with TRITON - Web Security:

- Disable all browser pop-up blocking features.
- Make sure that Internet Explorer Enhanced Security Configuration (IE ESC) is disabled.
- Make use of the quick start tutorials offered when you launch TRITON - Web Security.
  - If this is your first experience with Websense Web Security, use the New User Quick Start tutorial to learn about policy creation and reporting.
  - If you have used previous Web Security versions, use the Upgrading User 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 TRITON - Web Security 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 TRITON - Web Security 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 TRITON - Web Security, and that scheduled jobs are properly stored in the Log Database.
- If you are using Internet Explorer 8 or 9, 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 50234 | Release Notes | Web Security Solutions | Version 7.7.3 | Updated 18-January-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7.3

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.