v7.7.4 Release Notes for Websense® Web Security Solutions

Topic 50540 | Release Notes | Web Security Solutions | Version 7.7.4 | Updated 10-Aug-2013

Applies To:	Web Filter, Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series Appliance, v7.7.4

Version 7.7.4 is a stability patch for on-premises Websense Web Security solutions. It rolls up many resolved customer issues for the v7.6.x and v7.7.x series. This patch release is recommended for all sites.

Use these Release Notes to find information about what's changed and improved in version 7.7.4.

New in 7.7.4

Topic 50541 | Release Notes | Web Security Solutions | Version 7.7.4 | Updated 10-Aug-2013

Applies To:	Web Filter, Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series Appliance, v7.7.4

Version 7.7.4 is considered a patch release, but the following feature have been added:

- Client functionality is now supported on the Windows 8 graphical Start screen, as well as the desktop.
- The Web Security logon application (LogonApp.exe) now offers full support for Windows 8 clients.
- Content Gateway: In prior releases, regardless of whether SSL decryption was enabled or disabled, if Websense Filtering Service was down or unreachable by Content Gateway, all SSL sites were decrypted, included sites configured for SSL bypass. A new **records.config** parameter lets you turn off SSL decryption when Content Gateway cannot reach Filtering Service.

  To use the new feature

  1. Add the following line to the records.config file:

     ```
     CONFIG wtg.config.ssl_fail_open INT 1
     ```

  2. Use the following command to re-read records.confg:

     ```
     /opt/WCG/bin/content_line -x
     ```

  Setting the wtg.config.ssl_fail_open paramter to ‘1’ causes all SSL sites NOT to be decrypted when the proxy cannot reach Filtering Service.

  The default value is 0.

Installation and upgrade

Topic 50542 | Release Notes | Web Security Solutions | Version 7.7.4 | Updated 10-Aug-2013

Applies To:	Web Filter, Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series Appliance, v7.7.4

All Web Security solutions

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)

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

- Microsoft SQL Server 2008 SP3 or 2008 R2 SP2, Standard or Enterprise, 64-bit or 32-bit
- 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
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 8).

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:

> ✓ **Note**
> This section applies to the V-Series appliance. Please refer to the 7.7.4 X-Series Getting Started Guide for information about the X-Series appliance.

1. Run the **firstboot** script and configure the full policy source appliance.
2. Download the TRITON Unified Installer (see *Downloading the installer*, page 8).
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 7.7.4.
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 Security components on Red Hat Linux 6.x 64-bit

If you plan to install 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 Security, 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.x-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.x-x64 computer.

Upgrade overview

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

Your Current Verion	Step One	Final Step
Web Security Gateway on X-Series 7.7.1	Direct upgrade to 7.7.4	Done
Web Security Gateway on V-Series 7.7.0	Upgrade to 7.7.3	Upgrade to 7.7.4
Web Security Gateway on V-Series 7.6.x	Upgrade to 7.7.0, then 7.7.3	Upgrade to 7.7.4
Web Security Gateway on X-Series 7.6.4	Upgrade to 7.7.1	Upgrade to 7.7.4
Web Security Gateway on V-Series 7.5.x	Upgrade to 7.6.0, then 7.7.0, then 7.7.3	Upgrade to 7.7.4
Web Security Gateway software 7.5.x (no appliance)	Direct upgrade to 7.7.4	Done
Web Security Gateway software 7.6.x, 7.7.0 (no appliance)	Direct upgrade to 7.7.4	Done
Web Filter or Web Security software 7.5.x, 7.6.x, 7.7.0	Direct upgrade to 7.7.4	Done
Content Gateway software 7.6.x, 7.7.0	Direct upgrade to 7.7.4	Done

To upgrade directly to Websense Web Security Version 7.7.4:

- Your current software deployment must be at Version 7.5 or later. V-Series appliances require this path: 7.5 > 7.6.0 >7.7.0 > 7.7.3 > 7.7.4.
- 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 v7.7.4.
  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** (7.7.4).

   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 2.5 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

Websense Content Gateway

The Websense Deployment and Installation Center is the complete resource for deployment, installation, and upgrade information for all v7.7.x TRITON Enterprise solutions.

Content Gateway is the proxy component of the Web Security Gateway and Web Security Gateway Anywhere solutions. Installation and upgrade must be performed in the context of installation or upgrade of Web Security Gateway (Anywhere).

Important

If you are using Content Gateway on a V-Series appliance, Content Gateway is installed when the appliance is factory imaged and upgraded with the appliance patch facility.

TRITON solution **installation information** starts here.

TRITON solution **upgrade information** starts here.

Content Gateway step-by-step upgrade instructions start here.

Below are summaries of Content Gateway:

- *Hardware requirements*
- *Operating system and software requirements*
- *Instructions for downloading the installer*

Note

Data Security Policy Engine with Content Gateway:

Content Gateway includes an on-board Data Security policy engine. The v7.7.3 policy engine, which is the most current version, is compatible with Content Gateway v7.7.0 - v7.7.4; however, to take advantage of v7.7.3 policy engine improvements, Content Gateway must be v7.7.3 or higher.

Hardware requirements

CPU	Quad-core running at 2.8 GHz or faster
Memory	
• If RHEL 6, 64-bit	6 GB
• If RHEL 5, 32-bit	4 GB

Disk space	2 disks: • 100 GB for the operating system, Websense Content Gateway, and temporary data. • 147 GB for caching If caching will not be used, this disk is not required. The caching disk: – Should have minimum size of 2 GB, maximum 147 GB for optimal performance – Must be a raw disk, not a mounted file system – Must be dedicated – Must *not* be part of a software RAID – Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64MB of write-through cache
Network Interfaces	2

To support transparent proxy deployments

Router	Must support WCCP v2, or Policy Based Routing (PBR). A Cisco router must run IOS 12.2 or later. Client machines, the destination Web server, and Websense Content Gateway must reside on different subnets.
—or—	
Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). To support L2 forward or return, Content Gateway must be Layer 2 adjacent to the switch. The switch must be able to rewrite the destination MAC address of frames traversing the switch. The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Operating system and software requirements

Websense Content Gateway version 7.7.4 is certified on:

- Red Hat Enterprise Linux, 6 series, updates 0, 1, 2, and 3, 64-bit, Basic Server
  - Kernel version for 6.0: 2.6.32-71
  - Kernel version for 6.1: 2.6.32-131
  - Kernel version for 6.2: 2.6.32-220
  - Kernel version for 6.3: 2.6.32-279
- Red Hat Enterprise Linux, 5 series, updates 3, 4, 5, 6, and 7, base or Advanced Platform, 32-bit only

- Corresponding CentOS versions (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

Although not certified, Websense, Inc. provides “best effort” support for newer versions of Red Hat Enterprise Linux. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion unless the issue is deemed a Red Hat Enterprise Linux-specific issue, at which point you must contact Red Hat directly for assistance.

Only kernels shipped with the above Linux versions are supported. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

```
/bin/uname -r
```

Important

If you are installing Content Gateway on Red Hat Enterprise Linux 6, you must see Requirements for Red Hat Enterprise Linux for a list of library requirements, critical ethernet interface naming requirements, and other considerations.

Websense Web Security Gateway (Anywhere)

- Version 7.7.4 required

Important

Web Security Gateway (Anywhere) must be installed prior to Content Gateway.

Websense Data Security

- Version 7.7.3
- Any version can be used via the ICAP interface. See Content Gateway Manager Help for configuration instructions.

Web browsers:

- Websense Content Gateway is configured and maintained with a Web-based user interface called Content Gateway Manager. Content Gateway Manager supports the following Web browsers:
  - Microsoft Internet Explorer 8 and 9
  - Mozilla Firefox versions 5 and later

- Google Chrome 13 - 26

Note

Browser restrictions apply only to the use of Content Gateway Manager and not to client browsers proxied by Content Gateway.

Instructions for downloading the installer

Note

If Content Gateway is running on a V-Series appliance, it is installed during factory imaging and upgraded when the v7.7.4 patch is applied. You do not need to download the installer.

Important

Users of Integrated Windows Authentication (IWA):

- If you are upgrading from 7.6.x or 7.7.0, note that the upgrade procedure does not preserve the domain join. Post-upgrade you must re-enable IWA and rejoin the Windows domain.
- When you join the domain, one entry is automatically added to your DNS server for every interface on your appliance or server. The entry for the primary interface is useful, the others must be removed. See IWA domain join in Content Gateway v7.7.4 can create DNS entries that cause problems.

It is highly recommended that you read all of these release notes and follow the upgrade instructions step-by-step.

V-Series appliance upgrade instructions, which includes Content Gateway, start here.

Content Gateway software upgrade instructions start here.

To download the Content Gateway v7.7.4 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** (7.7.4).

   The available installers are listed under the form.

4. Click the plus sign ("+") next to an installer entry for more information about the installer.

Click the **download** link to download the installer.

Websense V-Series appliance

The upgrade to version 7.7.4 is applied to V-Series appliances via a software patch. Patches are installed via the Appliance Manager under the **Administration > Patches/Hotfixes > Patches** page. You must be running version 7.7.3 to use the version 7.7.4 patch. If you are running a previous version, please see the upgrade links below.

The Quick Start poster and Getting Started Guide are your comprehensive resources for installing the physical unit, running **firstboot**, and completing initial configuration.

Comprehensive **upgrade** instructions start here in the Deployment and Installation Center.

> **Important**
>
> Before starting an upgrade on an appliance, make sure any off-box Policy Broker or Policy Server has already been upgraded.

See *Upgrade tips*for additional information.

Security mode provisioning

Version 7.7.4 V-Series appliances support the following security modes.

Security Mode	V5000	V10000 G2 and G3
Standalone mode		
Web Security	X	
Web Security Gateway	X	X
Web Security Gateway Anywhere	X	X
Email Security Gateway	X	X
Email Security Gateway Anywhere	X	X
Dual mode		

Security Mode	V5000	V10000 G2 and G3
Web Security and Email Security Gateway	X	X
Web Security Gateway or Gateway Anywhere and Email Security Gateway or Gateway Anywhere		X

Once configured, the appliance cannot be changed to another security mode without first restoring the factory image. The security mode **cannot** be changed by running **firstboot** again.

Web browsers with the Appliance Manager

V-Series appliances are configured and maintained with a Web-based user interface called the Appliance Manager. The Appliance Manager should be used with one of these supported browsers:

- Microsoft Internet Explorer 8 and 9
- Mozilla Firefox versions 5 and later
- Google Chrome 13 - 26

✓ **Note**
If you are using Internet Explorer, make sure that Enhanced Security Configuration is turned off.

When you access the Appliance Manager for the first time, you will get a certificate warning because the Appliance Manager offers a self-signed certificate. To eliminate the warnings, install the certificate into your browser's CA store. For instructions, see your browser documentation.

Downloading the TRITON Unified Security Center Installer

The TRITON Unified Security Center and several support components are installed off of the appliance, on separate servers.

To download the TRITON version 7.7.4 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** (7.7.4).

   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.

Websense X-Series appliance

Note this important change: In version 7.7.4, **Full policy source** mode is no longer supported on the X10G security blades. **User directory and filtering** and **Filtering only** modes are supported.

X-Series appliances are configured and maintained with a Web-based user interface called the Security Blade Manager.

Within the Security Blade Manager, each security blade is kept up-to-date with a simple, easy-to-use patch management facility.

- Back up the files on the blade, and then use the patch management feature in the security blade console to apply version 7.7.4 to all blades.
- Note: If you are not already running version 7.7.1, complete that installation prior to the 7.7.4 patch upgrade.

Patch download and installation are always initiated manually.

After backing up your blades, go to the **Administration** > **Patches/Hotfixes** page to check for, download, and install patches.

- Security blades automatically check for new patches once a day. The time of the check is randomized, cannot be configured, and is different for every blade.
- To manually check for patches at any time, use the **Check for Patches** button.
- When a new patch is available, the patch version number, description, and status are displayed in the **Available patches** table and an alert is displayed on the **Status** > **General** page.
- After a patch is downloaded, it can be copied to another location on your network where it can be easily and efficiently uploaded to multiple blades.
- If the security blade management interface (C) does not directly connect to the Internet, you can configure a proxy server through which the blade checks for patches.
- The Patch History table provides an immediate history of patches that have been applied to the blade.
- Multiple X10G security blades may be installed in your network. However, they must all be running the same version of Websense software modules. Websense, Inc., does not support running different versions of the software on different blades on one network. Filtering results are not expected to be consistent in that scenario.
- Be sure that all Websense modules running off the blade, such as Log Server, are upgraded to the appropriate level each time you patch the security blade.

After patch installation is complete:

- Log onto the Security Blade Manager, go to the **Configuration** > **System** page and confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.
- The upgrade procedure does not preserve the Integrated Windows Authentication join to the Windows Domain. After the upgrade, re-enable IWA and rejoin IWA to the Windows Domain. See **Configuring Integrated Windows Authentication** in Content Gateway Manager Help.

With previous patches, if a security blade was accidentally restarted or powered off in the middle of a patch upgrade, and if the network administrator immediately started the upgrade a second time, the appliance could be left in an unknown state. The recovery from that state could be very challenging.

A safety feature has been added to the upgrade process in this version. This safety feature prevents immediate, additional upgrade attempts, if the upgrade process stops or fails in the middle. This preserves the state of the security blade at the point where the upgrade stopped. With the guidance of your Support professional, you can recover from the power outage or other disruption more quickly.

The Quick Start poster and Getting Started Guide are your comprehensive resources for installing the physical unit, running **firstboot**, and completing initial configuration of an X10G chassis and its security blades.

Security mode provisioning

Each Websense X-Series blade server runs Web Security Gateway / Anywhere and can be configured in either of these modes:

Mode	Module name
Web Security Gateway without Network Agent	Web Security Gateway / Anywhere
Web Security Gateway, optimized for Network Agent	Web Security Gateway / Anywhere (This mode is optional. If used, it applies only to the blade in slot 16.)

You choose the mode of a blade server during initial *firstboot* configuration.

Web browsers with the Security Blade Manager

The Web-based user interface called the Security Blade Manager should be used with one of these supported browsers:

- Microsoft Internet Explorer 8 and 9
- Mozilla Firefox versions 5 and later

- Google Chrome 13 - 26

✓ **Note**

If you are using Internet Explorer, make sure that Enhanced Security Configuration is turned off.

When you access the Security Blade Manager for the first time, you will get a certificate warning because the Security Blade Manager offers a self-signed certificate. To eliminate the warnings, install the certificate into your browser's CA store. For instructions, see your browser documentation.

Downloading the TRITON Unified Security Center Installer

The TRITON Unified Security Center and several support components are installed off of the appliance, on separate servers. These components need to be upgraded also.

To download the TRITON version 7.7.4 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).

   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. The installer detects Websense components on each server where it is run, and will upgrade them with your approval.

Operating tips

Topic 50543 | Release Notes | Web Security Solutions | Version 7.7.4 | Updated 10-Aug-2013

Applies To:	Web Filter, Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series Appliance, v7.7.4

All Web Security solutions

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**.

Websense Content Gateway

Installation

Software installation location and file ownerships

Content Gateway is installed in **/opt/WCG**. If Content Gateway is being upgraded and the existing installation location is **not** /opt/WCG, the location is automatically moved to /opt/WCG by the upgrade script.

Content Gateway files are installed with root ownership. Content Gateway processes are run as root.

Internet connectivity

It is recommended that the Content Gateway host computer have Internet connectivity before starting the software installation procedure. The software will install without Internet connectivity, but analytic databases cannot be downloaded from the Websense Database Download Server until Internet connectivity is available.

Ports

A full deployment of Content Gateway requires that several ports be open. See Installing Content Gateway in the Deployment and Installation Center for information about open ports and the reassignment of ports, if necessary.

‘admin’ password restrictions

The password you enter for the Content Gateway administrator during installation (default name: admin) must be 15 characters or fewer.

To create a strong password (recommended), use 8 or more characters, with at least 1 each of the following: capital letter, lower-case letter, number, special character.

The password **cannot** contain the following special characters:

- space
- $ (dollar symbol)
- : (colon)
- ‘ (backtick; typically shares a key with tilde, ~)
- \ (backslash)
- “ (double-quote)

Cache size

Cache size should be restricted to 147 GB. This size provides optimal resource utilization while also providing an excellent end-user experience. Because today’s

Internet sites are often composed of dynamic, uncacheable content, caching is a less significant factor in the end user's web browsing experience.

Configuration

In explicit proxy deployments, send HTTPS traffic to port 8080

In explicit proxy deployments, when HTTPS (SSL Manager) is enabled, browsers should be configured to send HTTPS traffic to the proxy on port 8080. The **ipnat.config** rule that was used to redirect traffic from 8070 to 8080 was removed in version 7.6.

Accessing Intranet sites in an explicit proxy deployment

If your clients cannot access your Intranet sites, verify that your operating system has been correctly configured to resolve all internal and external hostnames. Use the **nslookup** command to verify that a domain is listed in your DNS server:

For internal-facing servers:

```
nslookup intranet.example.com
```

For external websites:

```
nslookup www.example.com
```

If your organization has multiple DNS domains, verify that a hostname in each domain resolves correctly. If you are unable to resolve hostnames, verify the contents of the **/etc/resolv.conf** file, which provides search rules for how domain names are resolved in DNS.

When Content Gateway is on a V-Series appliance, the domain of the hostname is automatically added to **/etc/resolv.conf**. For example, if the hostname of the appliance is vseries.example.com, then Content Gateway treats "intranet" requests as "intranet.example.com".

Virtual IP address must not match any real IP address

When configuring the Virtual IP address feature, make sure that the Virtual IP addresses do not conflict with any existing IP addresses in the network.

Restart the proxy after protocol settings change

Any time you change your protocol settings in Content Gateway Manager (for example, with **Configure** > **SSL** > **Decryption/Encryption** > **Inbound** > **Protocol Settings**), restart the proxy to cause the new settings to take effect.

Using extended event logging

To investigate unexpected system behavior, it is sometimes helpful to enable the **Log Transaction and Errors** option (extended event logging) in Content Gateway

Manager (**Configure > Subsystems > Logging**). However, extended event logging adds significant load to Content Gateway processes. If possible, do not enable extended event logging when Content Gateway is at the high end of its processing capacity.

Reverse proxy

Content Gateway does **not** function as a reverse proxy.

Proxy user authentication

Client browser limitations

Not all web browsers fully support transparent user authentication.

The following table indicates how a browser responds to an authentication request when Integrated Windows Authentication (IWA) is configured.

Browser/ Operating System	Internet Explorer (v8, 9 & 10 tested)	Firefox (v11 tested)	Chrome (v17 & 18 tested)	Opera (v10 tested on Windows, v11 tested on Red Hat)	Safari (v5 tested)
Windows	Performs transparent authentication	Performs transparent authentication	Performs transparent authentication	Falls back to NTLM and prompts for credentials	Falls back to NTLM and prompts for credentials
Mac OS X	Not applicable	Performs transparent authentication	Browser issue prevents IWA from working	Not tested.	Performs transparent authentication
Red Hat Enterprise Linux, update 6	Not applicable	Performs transparent authentication	Browser issue prevents IWA from working	Does not support any form of proxy authentication	Not applicable

LDAP support for passwords with special characters

LDAP user authentication can support passwords containing special characters.

Configuration is made directly in the **records.config** file.

The following parameter must be enabled, and the correct encoding name to which the special characters belong must be configured.

Add these entries to **records.config**. Note that the default setting is 0 (feature disabled).

```
// To enable the feature specify 1.
CONFIG proxy.config.ldap.proc.encode_convert  INT <1 or 0>
// Specify an encoding name here. For example,
// for German specify "ISO-8859-1".
CONFIG proxy.config.ldap.proc.encode_name  STRING <encoding
name>
```

SSL Manager

SSL Manager and the Root CA

In v7.7.0 (and beginning with v7.6.5), the SSL Manager default Root CA (presented to clients) is signed with SHA-1. In prior versions, the Root CA was signed with MD5.

It is strongly recommended that all instances of Content Gateway use the same Root CA, and that for best security the signature algorithm is SHA-1.

The best practice is to replace the Websense default Root CA with your organization's Root CA signed by SHA-1 or stronger. See Internal Root CA in Content Gateway Help.

The Root CA should be imported into all affected clients.

✓ **Note**

Client connections may fail (depending on specific browser behavior) if the client sees a certificate generated by an unknown Root CA.

Post upgrade

Integrated Windows Authentication (IWA)

The upgrade procedure does not preserve the IWA join to the Windows Domain.

Post upgrade, re-enable IWA and rejoin IWA to the Windows Domain. See **Configuring Integrated Windows Authentication** in Content Gateway Manager Help.

! **Important**

When you join the domain, one entry is automatically added to your DNS server for every interface on your appliance or server. The entry for the primary interface is useful, the others must be removed. See IWA domain join in Content Gateway v7.7.4 can create DNS entries that cause problems.

Web Security Gateway and Data Security

If Web Security Gateway Anywhere and Data Security are deployed together and upgraded from v7.6.x to version 7.7.4, you must remove stale entries of Content Gateway instances registered in Data Security system modules:

1. Log onto the TRITON console.
2. Select the **Data Security** tab.
3. Select **Settings > Deployment > System Modules**.
4. Listed are 2 instances of each Content Gateway module registered with the system. Delete the older instances. You can identify these by looking at the version number.
5. Click **Deploy**.

If Web Security Gateway Anywhere and Data Security are deployed together and configured to use the on-box policy engine, and then reconfigured during upgrade or later to use the ICAP interface, the Content Gateway instance must be deleted from the list of Data Security system modules or the deployment will fail.

1. Log on to the TRITON console.
2. Select the **Data Security** tab.
3. Select **Settings > Deployment > System Modules**.
4. Locate the entry for the Content Gateway instance, click on it to open its **Details** page and then click **Delete**.
5. Click **Deploy**.

All Websense appliances

Interface setup tip

If the P2 interface is used and it is in the same subnet as P1, the default gateway is automatically assigned to P2, which is bound to eth1. You should perform a test to ensure that outbound packets can reach the Internet.

Avoiding port conflicts

See the ports list for a table of the Websense software module versions that are compatible with each appliance version.

Check the ports article to avoid port conflicts if you plan to make a change from a default port.

For example, if you want to use an HTTP proxy server port that is different from the default port (8080), be sure to check the ports list first, to avoid conflict with ports already in use by the V-Series.

Upgrade tips

After patch installation is complete:

- Log onto the Appliance Manager, go to the **Configuration** > **System** page and confirm and adjust, if necessary, the **Time and Date** settings, paying particular attention to the time zone setting.
- If the upgraded appliance is a Policy Server, log onto TRITON console, go to the TRITON - Web Security **Settings** > **General** > **Policy Servers** page and add the appliance. Next go to the TRITON console **Appliances** tab and register the appliance.
- The upgrade procedure does not preserve the Integrated Windows Authentication join to the Windows Domain. Post upgrade, re-enable IWA and rejoin IWA to the Windows Domain. See **Configuring Integrated Windows Authentication** in Content Gateway Manager Help.

With previous patches, if the appliance was accidentally restarted or powered off in the middle of a patch upgrade, and if the network administrator immediately started the upgrade a second time, the appliance could be left in an unknown state. The recovery from that state could be very challenging.

A safety feature has been added to the upgrade process in this version. This safety feature prevents immediate, additional upgrade attempts, if the upgrade process stops or fails in the middle. This preserves the state of the appliance at the point where the upgrade stopped. With the guidance of your Support professional, you can recover from the power outage or other disruption more quickly.

Logging tip

If you want to examine log files for Network Agent in Appliance Manager, be sure to turn on Network Agent logging in the TRITON - Web Security console first. To do this, log on to **TRITON - Web Security** and navigate to the **Settings** > **Network Agent** > **Global**. Hover over **Global** and select the Network Agent IP address that you're interested in. At the bottom of the page, open **Advanced Network Agent Settings**, go to the **Debug Settings** area, and set **Mode**, **Output**, and **Port**.

Deployment tips

- When Policy Broker is run on a V-Series appliance (configured as the **Full policy source**), all Policy Servers that point to that Policy Broker (configured as **User directory and filtering**) must be installed on V-Series appliances as well. You cannot install and run Policy Servers on off-box machines and point them to a Policy Broker that runs on an appliance. This configuration is not supported.

  However, you can run Policy Server on multiple appliances (**User directory and filtering** mode) and point these appliances to a Policy Broker running either on or off an appliance.

- **Teamed NICs** share the load under one common identity, with multiple adapters load-balancing under a single IP address. This is also known as link aggregation or trunking.

  If you have implemented NIC teaming, but don't see load balancing working as expected, the problem may be resolved by configuring your switch to disable **flowcontrol send**. To do this, use the command **set port flowcontrol send off** for both the port-channel and channel member ports.

- When Web Security Gateway (Anywhere) is deployed and Content Gateway **Integrated Windows Authentication** (IWA) is configured, if the appliance hostname is changed, IWA will immediately stop working. To repair the IWA configuration, log onto Content Gateway Manager, unjoin the stale domain and join the domain with the new hostname.
- Websense Web Security Log Server now supports **SQL Server SSL encryption**. However, if you are running TRITON - Web Security (manager) on the appliance (recommended only for evaluations and very small deployments), the connection from the console to the database **cannot be encrypted**. This means that if the Microsoft SQL Server "Force Protocol Encryption" option is set to Yes, no data will appear in the Web Security Dashboard or other reporting tools.

Backup and restore tips

- When configuring schedule backups to a remote storage location (FTP server or Samba share), make sure that the account used for backup file creation has **read** and **write** permissions. If you plan to use the option to automatically delete backup files older than some period of time, you must use an account that has **delete** permissions for the backup file directory and its subdirectories.
- In a multiple appliance deployment, after restoring the configuration of a **Policy source** appliance, restart any **Filtering only** or **User directory and filtering** appliances in your network to ensure that user requests are filtered correctly.

Websense Endpoint

Topic 50548 | Updated 10-Aug-2013

Applies To:	- Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere - Websense Data Security

Version 7.7.4.1633 is a Websense Endpoint Package release that introduces expanded support for Windows 8 clients for all Websense endpoint clients: Web Endpoint, Remote Filtering Client, and Data Endpoint.

Websense endpoint clients built with the Websense Endpoint Package Builder can now monitor browsing and most Windows Store applications from the new tiled user interface, as well as from the desktop.

Version 7.7.4.1633 also includes important corrections for the Mac endpoint.

General features

- You can install endpoint software on Windows 8 client machines.
- Data Endpoint can monitor operations on Windows 8 desktop and Windows Store applications (with the exception of Windows Store Mail for the endpoint email destination channel).
- Websense endpoints supports Internet Explorer 10 touch mode. For Data Endpoint, this applies to the endpoint HTTP/S destination channel.
- Websense endpoints support Firefox 18. For Data Endpoint, this applies to the endpoint HTTP/S destination channel.

Web Endpoint considerations

If you are using Websense Web Endpoint, note that the updated endpoint package is not available from the Settings > Hybrid Configuration > Hybrid User Identification page at this time. To use the features in this update, manually create a new endpoint package with the Websense Endpoint Package Builder.

Endpoint backward compatibility

All Websense endpoints at v7.7.4.1633 can communicate with TRITON management components are compatible with TRITON consoles from v7.7.0 - 7.7.4. Data Endpoint does not work with v7.6.x or earlier management components.

> **Important**
>
> If you deploy Web and Data Endpoint packages, all TRITON management components must be v7.7.0 - 7.7.4 to comply with Data Endpoint requirements.

Remote Filtering Client v7.7.4.1633 is compatible with Remote Filtering Server versions 7.7.x, 7.6.x, and 7.5.x.

Websense Web Endpoint v7.7.4.1633 is compatible with v7.7.x hybrid service components.

Installation and upgrade

ic 43018 | Updated 10-Aug-2013

Applies To:	◆ Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere ◆ Websense Data Security

1. For Data Endpoint, make sure you have a v7.7.3 TRITON management server installed and functioning.
2. Download the new v7.7.3.1631 package builder from MyWebsense. The package includes the following files:
   - WebsenseEndpointPackageBuilder.exe
   - EPA.msi (Data Security only)
   - EPA64.msi (Data Security only)
3. The v7.7.3.1631 Endpoint Package Builder is an independent executable file that can be run on any Windows machine. As a best practice, however, to ensure that you are using the latest files, remove your old Endpoint Package Builder files and replace them with the new files, as follows:
   - For Data Endpoint, backup and remove any existing files from the ...\client folder where you installed Data Security: C:\Program Files *or* Program Files (x86)\Websense\Data Security\client, by default.

When you're done, copy all 3 files to this folder.

- For Web Endpoint and Remote Filtering Client, backup and remove any existing files from the ...\DTFAgent\RemoteFilteringAgentPack folder where you installed Web Security: C:\Program Files *or* Program Files (x86)\Websense\Web Security\DTFAgent\RemoteFilteringAgentPack, by default.

  Then, copy **WebsenseEndpointPackageBuilder.exe** to this folder.
- For combined Web and Data Endpoint, backup and remove existing files in both directories shown above. Then, copy all 3 files to the ...\Websense\Data Security\client folder.

4. Run **WebsenseEndpointPackageBuilder.exe** to generate a new endpoint client installation package.
5. Deploy the v7.7.3.1631 installation package to each endpoint client using one of the following methods:
   - Manually on each endpoint device
   - Using System Center Configuration Manager (SCCM) or Systems Management Server (SMS)
   - Using a Microsoft Group Policy Object (GPO) or other third-party deployment tool for Windows

   > **Important**
   >
   > On Windows 8 clients, Web Endpoint must be installed from the Windows desktop view.

   You do not need to uninstall earlier endpoint versions before installing v7.7.3.1631.

   > **Note**
   >
   > For an upgrade install, the administrator does not need a client password, even if the older endpoint version had a password set.

6. Restart the endpoint software after installation is complete.
7. For Web endpoint or Remote Filtering Client, restart the operating system.

For more detailed information on completing the Websense Endpoint Package Builder wizard and deploying endpoint software, see Installing and Deploying Websense Endpoint Clients.

To manually deploy Web Endpoint to Mac OS X clients by:

1. Download the installation package via the Web Security manager 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.

System requirements

See the Deployment and Installation Center in the Websense Technical Library for Web and Data Security system requirements.

Resolved and known issues

Topic 50544 | Release Notes | Web Security Solutions | Version 7.7.4 | Updated 10-Aug-2013

Applies To:	Web Filter, Web Security, Web Security Gateway, Web Security Gateway Anywhere, and V-Series Appliance, v7.7.4

A separate list of Resolved and Known issues for this release is available to customers with a current MyWebsense account.

If you are not currently logged in to MyWebsense, each link below takes you to a login prompt. Log in to view the lists.

- Web Filter / Web Security
- Websense Content Gateway
- All Websense Appliances
- Websense Endpoint