v7.6 Release Notes for Websense Web Security

Topic 50180 / Updated: 27-Apr-2011

Applies To:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere Version 7.6

Use the Release Notes to find information about what's new and improved in Websense Web Security and Websense Web Filter Version 7.6.

- *Introducing Web Security v7.6*
- *Operating tips*
- *Resolved and known issues*

Log on to mywebsense.com and click the **Downloads** tab to download the Version 7.6 installation package.

Deployment planning, installation, and upgrade information is available online in the Deployment and Installation Center.

Additional information about the v7.6 release is available in:

- v7.6 Release Notes for TRITON Unified Security Center
- v7.6 Release Notes for Websense Content Gateway
- v7.6 Release Notes for Websense V-Series Appliances

Introducing Web Security v7.6

Topic 50181 / Updated: 27-Apr-2011

Applies To:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere Version 7.6

In this version, Websense Web Security solutions are available in English only.

Installation

Version 7.6 introduces a single installer for Websense Web Security and Data Security, as well as for the off-appliance (management and reporting) components of Websense Email Security Gateway. (Websense Content Gateway, a Linux-only component, continues to be installed separately.)

When installing Websense Web Security, the new, shared TRITON Infrastructure components must be installed before the TRITON - Web Security module. TRITON Infrastructure is listed as the first option in the shared installer.

As in previous versions, when TRITON - Web Security is installed on a separate machine from core filtering components, Policy Broker, Policy Database, and Policy Server must be installed before the management console.

Note that in this release, TRITON - Web Security can no longer be installed on Linux platforms.

Complete planning and installation information for all v7.6 Websense security solutions is available online in the Deployment and Installation Center.

TRITON Unified Security Center changes

This release introduces a fully centralized TRITON Unified Security Center, which allows all Web Security, Data Security, and Email Security management components to be installed on a single Windows Server 2008 R2 64-bit machine, and accessed through the same user interface.

To support this change, 2 familiar Websense Web Security services have new names:

- Apache2Websense is now **Websense Web Reporting Tools**.
- ApacheTomcatWebsense is now **Websense TRITON - Web Security**.

In addition, the new Websense TRITON Unified Security Center, TRITON Central Access, and TRITON Settings Database services provide the infrastructure to seamlessly integrate Web, Email, and Data management.

All modules of the TRITON Unified Security Center can be accessed from the following supported browsers:

- Microsoft Internet Explorer 7, 8 (not Compatibility View), and 9
- Firefox 3.5.x, 3.6.x, or 4

See the TRITON Unified Security Center Release Notes for more information.

Introducing Real-Time Monitor

In Version 7.6, a new reporting tool, Real-Time Monitor, provides insight into current Internet filtering activity in your network. Filter results to focus on a specific subset of traffic, or pause the monitor to review existing data at length, as needed.

The monitor displays:

- The originator of each request (user name or IP address)
- All or part of the URL requested (configurable)
- Whether or not the URL was recategorized by Content Gateway scanning (Websense Web Security Gateway and Gateway Anywhere)

  This is indicated by the presence of an icon. Hover over the icon to see the original category for the site.
- The site category used for filtering
- The action (permit or block) applied to the request
- The time Real-Time Monitor received the record

  Due to differences in the way that Real-Time Monitor and the Log Database receive filtering data, this time may vary slightly from the time that appears in other reporting tools, like investigative reports.

Real-Time Monitor takes its real-time data from Usage Monitor, a component typically installed with Policy Server, rather than from Log Server. As a result, the monitor must be connected to a Policy Server that is associated with a Usage Monitor instance

A Real-Time Monitor instance shows data for a single Policy Server at a time. To monitor traffic associated with multiple Policy Server instances, you can open multiple Real-Time Monitor windows simultaneously. (This requires that each Policy Server instance have its own Usage Monitor instance.)

Real-Time Monitor is typically installed with the TRITON Unified Security Center, and includes 3 services: Websense RTM Client, Websense RTM Server, and Websense RTM Database.

Detailed information about configuring and using Real-Time Monitor is available in the TRITON - Web Security Help.

Reporting changes

Version 7.6 introduces support for Microsoft SQL Server Express 2008 R2.

The Log Database can also be hosted by:

- Microsoft SQL Server 2008, 32-bit or 64-bit (not IA64)
- Microsoft SQL Server 2008 R2, 32-bit or 64-bit (not IA64)
- Microsoft SQL Server 2005 SP3, 32-bit or 64-bit

Support for MSDE has been discontinued.

Note that while the TRITON Unified Security Center can be installed on the same machine as SQL Server Express, it should not be installed on the same machine as a full version of SQL Server.

As a result of this change, the Settings > Reporting > Log Database page has been changed to reflect differences in supported rollover methods and partition sizes.

Today and History page changes

Administrators can now click most of the counters on the Status > Today and History pages to open investigative reports or other pages with more details.

On the Today page, the affected counters are:

- Malicious
- Spyware
- Blocked
- Real-Time Security Updates
- Adult
- Requests
- Scanned

On the History page, you can now click the Blocked Security Risk counter for more information.

Delegated administration changes

Full integration of the TRITON Unified Security Center has introduced some changes in the ways that administrator accounts are created and managed. In addition, TRITON - Web Security has added a new role type, and several new administrator permissions.

See the Delegated Administration Quick Start for a more detailed overview of the new process for configuring delegated administration and reporting.

Important

WebsenseAdministrator account is no longer the default administrator account.

The default account (with full permissions in all modules of the TRITON Unified Security Center) is **admin**.

Administrator management

Administrator accounts (both local and network) are now managed on the TRITON Settings > Administrators page. Global Security Administrators with full access to TRITON Settings and all TRITON Unified Security Center modules (Web Security, Data Security, and Email Security) can create administrator accounts and grant the accounts permission to access one or more TRITON modules.

Note

When administrators use network accounts to access the TRITON Unified Security Center, each **user** account must have an email attribute. User accounts that do not include an email attribute are not listed on the Add Network Account page.

Group accounts without an email attribute can be added as administrators.

Administrators are still assigned to delegated administration roles and granted role-specific permissions in TRITON - Web Security.

In environments that allow delegated administrators to use their network accounts to access the TRITON console, directory service communication is now done on the **TRITON Settings > User Directory** page. (End user directory information is still configured on the Settings > General > Directory Services page in TRITON - Web Security.)

Password reset

Version 7.6 introduces a new mechanism for resetting the password for local administrator accounts (formerly called “Websense user accounts”). This requires that all local administrator accounts be associated with an email address.

When an administrator requests a new password, a single-use, temporary password is emailed to the address associated with the account. The password is good for a limited period of time. When the administrator enters the temporary password, he or she is prompted to create a new password.

SNMP setup to enable the email-based password recovery system is performed on the **TRITON Settings** > **Notifications** page.

New role type and new permissions

The delegated administration options available in TRITON - Web Security have been enhanced:

- There are now 2 types of delegated administration roles: policy management and reporting and investigative reporting.
  - Administrators in **policy management and reporting** roles can still be granted permission to create policies for managed clients, report on all clients or managed clients only, or create policies and run reports. Policies for managed clients assigned to this type of role are managed by administrators within the role.
  - Administrators in **investigative reporting** roles can report on managed clients in the role, but policies for those clients are managed in other roles.

    A client can be added to multiple investigative reporting roles, but to only one policy management and reporting role.
- Administrators can now be granted **Auditor** permissions in any policy management and reporting role (including Super Administrator). Auditor permissions provide read-only access to the features and functions available to other administrators in the role. Auditors can explore TRITON - Web Security and see the management capabilities available to other administrators, but cannot save any changes.
- Administrators in the Super Administrator role and in policy and reporting roles have a new reporting permission available: **Real-Time Monitor**. This allows administrators to monitor all filtering activity associated with a Policy Server. Note that Real-Time Monitor permissions cannot be restricted to show information for managed clients only.

Policy distribution options at role creation

When a new delegated administration (policy management and reporting) role is created, Super Administrators now have 2 options for determining which policies initially appear in the new role:

- Give the new role one Default policy, made up of the Super Administrator Default category and protocol filters (previous v7.x behavior).
- Give the new role a snapshot of all policies, filters (except Permit All), custom categories, custom URLs (unfiltered and recategorized), and keywords that exist in the Super Administrator role. When a policy that includes a Permit All filter is copied, the delegated administrator copy instead has a filter called Permit Categories (Modified) or Permit Protocols (Modified).

Filters copied to a delegated administration role are subject to the Filter Lock.

Block page changes

Two new features have been added to enhance the usefulness of block pages:

- Hover text has been added to the block icon and block message to provide more information to end users who see a partial block page in a section of an otherwise permitted page.
- An account override feature, when enabled, allows users to enter new credentials on the block page to change the filtering policy applied to a request.

Block page in small screen areas

When some content on an otherwise permitted page is blocked, users may see only a tiny piece of the block page. This can cause confusion about what is happening, or why the section of content is blocked.

Now, if the user hovers the mouse over the visible portion of the block page, a message explains that the content is blocked, and that the user can click the message to see the full block page with detailed information about why the content is blocked.

If the user clicks the message, the full block page appears in a new window.

Account override

When account override permissions are assigned to a client, when a site requested by that client is blocked, the block page includes a **Switch Credentials** button. The end user can then enter network credentials (user name and password) to have the request filtered by a different policy.

- If the new policy permits the request, the user sees the site.
- If the new policy blocks the request, the user is not given access to the site. The user may or may not have another opportunity to enter different credentials, depending on the permissions assigned to the filtered account.

The new credentials continue to be applied to requests for a period configured on the Settings > General > Filtering page (5 minutes, by default).

Account override permissions might be granted, for example, to a computer client (IP address) corresponding to a kiosk machine used by internal and guest users who are not asked to authenticate. The IP address-based policy would apply to all requests by default, but users with valid network credentials could provide those credentials when a request is blocked, to see if their usual filtering policy permits the request.

Monitoring Web Security status

As in previous releases, you have the option to monitor the Today, History, and Alerts pages in TRITON - Web Security without timing out. Now, invoking this option also provides access to Real-Time Monitor.

The mechanism for activating this option has changed. Instead of marking a check box on the Today page, click the **Status Monitor** button on the Today, History, or Alerts page, or select **Status Monitor Mode** from the Role drop-down box in the Web Security toolbar.

When you enter Status Monitor mode in TRITON - Web Security, you are logged out of any other TRITON modules that you may have accessed.

Remote Filtering Client 64-bit support

Remote Filtering Client is now supported on the following 64-bit operating systems:

- Windows 7
- Windows Vista
- Windows XP
- Windows Server 2008 SP 1 and above, and R2
- Windows Server 2003 SP2 and above, and R2 SP2 and above

In addition, an updated Remote Filtering Client configuration utility makes it easy to create and edit Remote Filtering Client deployment profiles.

Citrix Integration Service 64-bit support

Citrix Integration Service now supports the following Citrix products:

Product	Operating System
XenApp 6.0	Windows Server 2008 R2
XenApp 5.0	Windows Server 2008 (32- and 64-bit) Windows Server 2003 (32- and 64-bit)

Product	Operating System
Presentation Server 4.5/4.0	Windows Server 2003 (32-bit) Windows Server 2000 (32-bit)
MetaFrame Presentation Server 3.0	Windows Server 2003 (32-bit) Windows Server 2000 SP4 (32-bit)

In addition, an updated endpoint package utility makes it easy to create and edit Citrix Integration Service installation packages.

Policy Server key management

The Settings > General > Policy Servers page has been updated to show key information for all Policy Servers associated with a TRITON - Web Security instance.

As before, you can add or delete Policy Server connections on this page. Now, you can also establish relationships between Policy Server instances that share a key. When you designate an instance as a primary Policy Server, and then associate additional instances as secondary Policy Servers, the hierarchy is reflected on the page. If the key for the primary instance changes, all of the secondary instances are updated automatically.

You can also have multiple primary Policy Server instances, each with its own key.

When a new primary Policy Server instance is added, use the **Verify Connection** button to make sure TRITON - Web Security can communicate with the new instance. If the connection is established, the success message indicates whether or not the selected Policy Server already has an associated key. If there is already a key, that key is displayed.

The base Policy Server (the Policy Server that TRITON - Web Security connects to during installation) must always be a primary. Its key can still be viewed and changed on the Settings > General > Account page.

Switching Policy Servers

In deployments that include multiple Policy Se7rver instances, when administrators change their Policy Server connection during a TRITON - Web Security session, they are no longer logged out of the TRITON console. Instead, the switch to the new Policy Server occurs seamlessly.

User Service caching

As in previous versions, User Service caches user and group mappings for a default period of 3 hours. Previously, however, the User Service cache was cleared each time an administrator clicked Save All to implement changes in TRITON - Web Security, regardless of whether changes affecting User Service had been made.

To improve performance, clearing the User Service cache is no longer performed as part of every Save All action. Instead, the cache is cleared at save time only when a change has been made to the Settings > General > Directory Services page.

In addition, the Directory Services page now includes a **Clear Cache** button that administrators can use to prompt User Service to clear its local caches and fetch updated information from the directory service when needed.

IPv6 filtering

In deployments that use Network Agent, you can now specify whether each Network Agent instance permits or blocks all IPv6 traffic. If you choose to block IPv6 traffic in general, you can specify exceptions. An exception can be either a specific IPv6 address or a port. Traffic from the specified addresses or ports is ignored.

Usage alert editing

The Settings > Alerts > Category Usage and Protocol Usage pages have been updated to make it easier to configure multiple usage alerts simultaneously.

This simplifies the process of creating or updating usage alert settings for categories or protocols with the same alerting thresholds and alert notification methods to save administrators time.

DC Agent health alerts

Two health alerts have been added to notify administrators of conditions that could prevent DC Agent from identifying users:

- Unable to access required file for a DC Agent instance
- A DC Agent instance has insufficient permissions

A more detailed version of each alert message is displayed on the Status > Alerts page in TRITON - Web Security. Click a **Solutions** link for information about resolving each issue.

Internationalized domain name (IDN) support

TRITON - Web Security now supports internationalized (Unicode) domain names in the following contexts:

- Investigative and presentation reports
- Today and History page charts
- Usage Monitor category alerts
- Custom URLs (unfiltered and recategorized)
- Limited access filters

In parts of the console that do not support Unicode characters, error messages have been added to explain that Punycode must be used.

Important

Keywords and regular expressions that contain Unicode characters are not matched against the domain portion of a URL. For example, consider this URL:

```
http(s)://www.example.com:port/
path?query#fragment_id
```

Unicode keyword or regular expression matching is applied only to the *path*, *query*, and *fragment_id* strings.

Hybrid configuration changes

Websense Web Security Gateway Anywhere deployments include a number of changes in TRITON - Web Security.

Filtered locations changes

The **Settings > Hybrid Configuration > Filtered Locations** page now contains details of all locations that contain users that can be filtered by the hybrid service.

For users filtered by hybrid filtering both in and outside the network, enter their in-network location details and specify that the location is filtered using the hybrid service.

For users that should be filtered by on-premises components (Filtering Service) when they are inside the network, and by the hybrid service when off site, enter the in-network location details for these users and specify the proxy type (transparent or explicit) for their on-premise filtering. The PAC file generated by the hybrid service configures the appropriate filtering automatically based on the settings that you provide.

If one or more locations uses an explicit proxy for filtering on-premises, specify the explicit proxy details in TRITON - Web Security to ensure requests are routed properly. Click **Manage Explicit Proxies** to define the proxies before adding them to a filtered location. Each filtered location can use more than one explicit proxy, arranged in preference order.

The changes to filtered locations replace the **Combine Filtering Methods** feature that is on the Off Site Users tab in the **Hybrid Configuration >User Access** page in previous releases.

Unfiltered destinations changes

The **Settings > Hybrid Configuration > Unfiltered Destinations** page now includes the option to specify whether an unfiltered destination applies to clients filtered by the hybrid service, clients filtered via explicit proxy in a filtered location, or both.

Off-site users changes

The **Off-Site Users** tab of the **Hybrid Configuration > User Access** page has been removed in this version.

- The **Automatically generate and email passwords** check box is now located on the **Shared User Data** page.
- The Registered Domains options are on the **User Access** page.
- Explicit proxy details are available on the **Filtered Locations > Manage Explicit Proxies** page.

Hybrid support for off site users is now activated with the **Enable hybrid filtering of off-site users** check box on the **User Access** page.

For upgrades from previous versions of Web Security Gateway Anywhere, this box must be explicitly checked to ensure off-site users are being filtered by hybrid filtering.

Before enabling this option, ensure any filtered locations are correctly configured. Otherwise, users in those locations will be incorrectly routed to the hybrid service. Domain registration, unfiltered destinations, and shared user data configuration are optional, but encouraged.

Block page changes

The **Hybrid Configuration > User Access** page now includes the option to modify the default block page supplied by the hybrid service. The block page title and message can be edited.

The logo that appears on a hybrid filtering block page can also be modified. Create a directory named **logo** in the Websense **ssdata** directory (by default, \Program Files\Websense\Web Security\bin\ssdata\ on Windows, or /opt/websense/bin/ssdata/ on Linux), then place the JPEG, GIF, or PNG logo file in that directory.

Hybrid filtering also supports the new functionality described in *Block page in small screen areas*.

Customized PAC files

The default PAC file is supplied by Websense, and comprises default settings from the hybrid service and any changes you make on the Hybrid Configuration pages. You can now either use your own PAC file, or supply a JavaScript fragment that can be appended to the default PAC file. Sync Service sends the customized PAC information to the hybrid service, and also detects when there is a newer version of the PAC file or fragment and updates the version on the hybrid service.

HTTPS notification pages

Note

This feature is displayed in TRITON - Web Security but will not be active until Websense Authentication Service is available, shortly after release.

A Websense SSL certificate is now available for hybrid filtering. If you deploy this certificate to hybrid filtering users, the hybrid proxy can establish SSL channels with newer browsers (Internet Explorer 8 or later, and Firefox 3.5 or later) in order to serve notification pages to the user – for example, a block page if the SSL site is in a category that requires a notification, or the appropriate page if authentication is required.

User identification changes

A new **Settings > Hybrid Configuration > Hybrid User Identification** page in TRITON - Web Security allows administrators to indicate how the hybrid service should identify users requesting Internet access.

Web Endpoint

Important

Web Endpoint will be available on the Hybrid User Identification page once deployed in the hybrid service, shortly after the TRITON - Web Security v7.6 release.

Websense Web Endpoint is a piece of software that gets installed on an client machine. It enforces the use of Hosted Web Security for Web filtering, and passes authentication information to the hosted proxies, enabling secure transparent authentication.

To enable the use of Web Endpoint for some of all of your end users that browse via the hybrid service, you must deploy it to those users. You can deploy Web Endpoint in the following ways:

- Push the endpoint manually to selected client machines using your preferred distribution method. For example, you might download the endpoint installation file and deploy it using Microsoft Group Policy Object (GPO).
- Deploy the endpoint to the end users in a Web policy directly from the hybrid service. Each user will be asked to install the endpoint software on their machine when they start a browsing session. If they choose not to install the software, they will be asked again the next time they start a browsing session.

Web Endpoint can only be deployed on Windows operating systems. The endpoint has been tested for compatibility with the following VPN clients: Cisco (corporate), Juniper, and Microsoft PPTP (corporate).

Websense Authentication Service

Important

Authentication Service will be available on the Hybrid User Identification page once deployed in the hybrid service, shortly after the TRITON - Web Security v7.6 release.

Websense Authentication Service is an on-network virtual machine that provides an interface between the hybrid proxy server and the Microsoft Active Directory or LDAP services used on-premises at your location. All communications between components are secured.

End users in your network authenticate with the Active Directory/LDAP server within the network, leveraging existing network security. Roaming users logged on to a computer using domain credentials have their Active Directory/LDAP credentials collected by the hybrid proxy and passed to Authentication Service to be validated against your Active Directory/LDAP server. Once these credentials are verified with Authentication Service, the appropriate policy is applied for that user.

Authentication Service requires installation and configuration on a machine in your network, and setup in TRITON - Web Security. For more information, see the *Authentication Service Installation and Configuration Guide*.

NTLM identification and manual authentication

The following options are also available on the **Settings > Hybrid Configuration > Hybrid User Identification** page as alternatives to, or fallback options for Web Endpoint and Authentication Service:

- NTLM can identify users transparently using directory information gathered by Directory Agent. This is the recommended option if Directory Agent is sending data to the hybrid service.

- If user authentication for hybrid filtering users is enabled, users who cannot be identified via another means will see a logon prompt when accessing the Internet.

  Optionally a Welcome page can be displayed when users who have not been identified via NTLM open a browser to connect to the Internet.

Directory Agent changes

- Websense Web Security Gateway Anywhere now supports the use of Sun Java System Directory and Oracle Directory Server for sending user and group information to the hybrid service.
- For every context added for a user directory on the **Hybrid Configuration** > **Shared User Data** page, you can add one or more contexts within the directory search that should be excluded from the data sent to the hybrid service.
- The **Test Context** button now checks for both the existence of the specified context, and any dependencies between the new context and existing contexts.
- If groups are found in the directory search, Directory Agent can now pick up all users from those groups even if some of the users are in a different context. To enable this, select **Include all users in selected groups, regardless of context** on the **Shared User Data** page. This option is enabled by default for Active Directory.
- Directory Agent can pick up users and groups based on search filters you define. Select **Customize Search Filters** to fine-tune user and group search filters for each context.

Sync Service changes

The following new features have been added to Sync Service:

- Policy data can be sent to the hybrid service immediately rather than waiting for the next scheduled update.
- Reporting data retrieval from the hybrid service can be scheduled for specific days and time periods.
- Sync Service traffic can be routed through a proxy server or firewall if required.

Configure these settings on the **Hybrid Configuration** > **Scheduling** page.

In addition, the **SecurityCategoryOverride** parameter is now set to ON by default. If you are filtering by custom categorization, a custom permitted site may still be blocked if it appears in a Security Risk category, unless you edit the parameter.

Hybrid Service Status changes

The Hybrid Service Status page is now available under **Main** > **Status**.

Click **View Report** on this page to download reporting data from the hybrid service and see a breakdown of how hybrid users are identified or authenticated with the service. The report output shows the number of clients using each available

authentication method (Web Endpoint, Authentication Service, NTLM identification, and manual authentication), if configured, over the last 7 days. Click an authentication method in the table to see a list of users who have most recently authenticated with that method. The report data can be exported to PDF or XLS.

Important

Authentication reporting data will be available on the Hybrid Service page once deployed in the hybrid service, shortly after the TRITON - Web Security v7.6 release.

The Hybrid Service page now also includes:

- statistics for the number of users and groups being sent to the hybrid service
- information about the PAC file currently in use
- details of the custom block page logo uploaded to the hybrid service, if used.

Content Gateway access and alerting

In Websense Web Security Gateway and Gateway Anywhere deployments, Content Gateway now automatically receives its key information from Policy Server. This means that key information no longer has to be entered in Content Gateway Manager.

In addition:

- A new **Settings > General > Content Gateway Access** page in TRITON - Web Security allows administrators to launch Content Gateway Manager from within TRITON.

  The page displays the status (running or stopped), IP address and host name, cluster name, and description for each Content Gateway instance that has registered with the selected Policy Server.
- Important Content Gateway health alerts are displayed in TRITON - Web Security.

  As with other health alerts, a short alert is shown on the Status > Today page, with a longer message appearing on the Alerts page.
- Use the Settings > Alerts > System page to configure both Web Security and Content Gateway system alerts.

  As with existing Web Security alerts, you can configure which Content Gateway conditions cause alert messages to be sent, and which methods (email, pop-up, or SNMP) are used to send the alert. Note that pop-up alerts are not supported on Windows 2008 and 2008 R2 machines.

Operating tips

Topic 50182 / Updated: 27-Apr-2011

Applies To:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere Version 7.6

To improve your experience with TRITON - Web Security:

- Make use of the quick start tutorials offered when you launch TRITON - Web Security.
  - If this is your first experience with Websense filtering software, use the New User Quick Start tutorial to learn about basic configuration, filtering policy creation, and reporting.
  - If you have used previous versions of Websense filtering software, use the Upgrading User Quick Start tutorial to orient yourself to the new features in this version.
- Disable all browser pop-up blocking features.
- On Windows Server 2008 machines, make sure that Internet Explorer Enhanced Security Configuration (IE ESC) is disabled.
- If you are accessing the TRITON console from a Linux machine, use Firefox 3.5 or later for best results.
- 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 All** (at the top of the right shortcut pane) 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 - Web Security 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, 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 50183 / Updated: 27-Apr-2011

Applies To:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere Version 7.6

A list of resolved and known issues in this release of 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.