Upgrading User Quick Start Tutorial

Websense® Web Security Solutions

v7.7

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published 2012
Printed in the United States and Ireland

Trademarks

Contents

1 Welcome

Use this quick start tutorial to become comfortable with the new features and functions of your Websense Web Security software.

This introductory section tracks basic changes that are important regardless of which versions you have previously used. Instead of separate glossaries for each version, for example, a single table charts terms added or revised in every version since 7.0.

Even if you are upgrading from a very recent version, please skim the introductory material for URL changes and supported platform information:

- *The TRITON™ Unified Security Center*
- *Term and concept reference*
- *Finding information within TRITON - Web Security*
- *Third-party product support*

You may also be interested in one or more of the following topics:

- *What's New in Version 7?*
- *What's New in Version 7.1?*
- *What's New in Version 7.5?*
- *What's New In Version 7.6?*
- *What's new in version 7.7?*
- *Where Do I Find...?*
- *How Do I...?*

The TRITON™ Unified Security Center

The TRITON Unified Security Center is a browser-based console used to perform configuration, administration, and reporting tasks for Websense Web Security, Data Security, and Email Security software and appliances.

To access the TRITON console from anywhere in the network, open a supported browser (Microsoft Internet Explorer 8 or 9, Mozilla Firefox 4.x, 5.x, or 6.x, or Google Chrome 13 or later) and enter the following URL:

```
https://<IP address or hostname>:9443/triton/
```

Replace <IP address or hostname> with the name or location of the TRITON - Web Security machine.

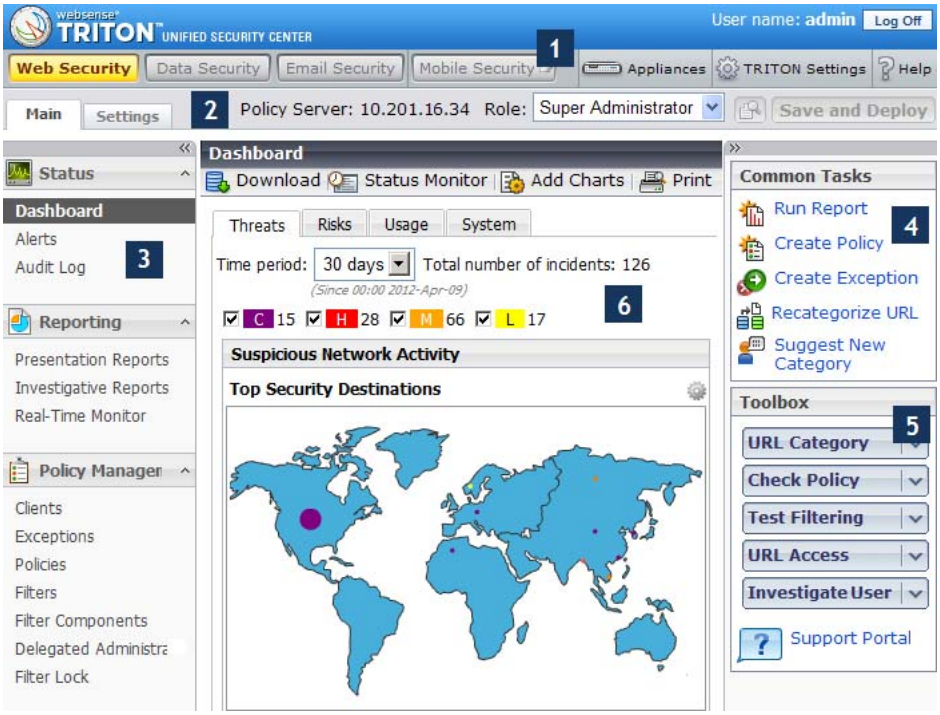
Any administrator with Web Security access to the TRITON console is taken to the Web Security **Status > Dashboard** page after logon. (The administrator may be prompted to enter a subscription key or launch a quick start tutorial before the Dashboard appears.)

The Threats dashboard displays information about suspicious activity in your network that may be related to advanced malware threats.

- Super Administrators determine which delegated administrators, if any, have access to the Threats dashboard.
- Administrators who cannot access the Threats dashboard may still be granted access to the Risks, Usage, and System dashboards.
- Even administrators without permission to view reporting information in any part of the Web Security Dashboard can see limited system status information on the System dashboard.

For more information about the Web Security Dashboard, see *Monitor Web Security status*, page 13.

As in previous versions, TRITON - Web Security provides access to policy management tools and the settings used to configure your deployment. If you have upgraded from version 6.3.x or earlier, note that all reporting tools are also accessed from this console. See *Create reports within TRITON - Web Security*, page 14.



Legend

1. At the top of the screen:
   - The **banner** shows information about your logon session.
   - The **TRITON toolbar** makes it easy to switch between TRITON modules, access V-Series appliances in your network, configure TRITON settings, and access Help.

     Click Help > **Explain This Page** for detailed information about the functions displayed in the content pane. The TRITON - Web Security Help system, the New User and Upgrading User Quick Start tutorials, and the Websense Knowledge Base and forums are also accessible from the Help menu.
2. Just under the TRITON toolbar, the **Web Security toolbar** offers access to functions that can be used regardless of where you are in the interface:
   - The IP address of the Policy Server you are connected to is displayed. If your deployment includes multiple Policy Servers, use the drop-down list to switch between instances.
   - In general, changes are cached when you click OK. The **Save and Deploy** button changes color to indicate whether there are cached changes waiting to be saved. Click the magnifying glass icon (View Pending Changes) to see a list of currently cached changes before saving.
3. Use the left navigation pane to access TRITON - Web Security features and functions:
   - The **Main** tab offers access to all policy management tasks, status information, including alerts and audit logs, and reporting tools (if you have installed reporting on Windows).
   - The **Settings** tab provides access to most Websense software configuration tasks, previously accessed via the Server > Settings menu.
4. The **Common Tasks** lists provides quick links to the pages where the most frequently-performed TRITON - Web Security tasks can be performed. The last link, Suggest New Category, links to the MyWebsense site, where, after logging on, you can suggest that a site be recategorized in the Master Database.
5. The **Toolbox** lets you quickly identify how a site is categorized, which policy applies to a specific client, how a specific request by a given client is filtered, whether a URL has been accessed from within your network in the past 14 days, and what sites a user has requested in the past 14 days. The last two queries launch an investigative report (formerly, Websense Explorer report) with the details. See *Verify your Websense filtering setup*, page 14.
6. Each time you open TRITON - Web Security, the **Dashboard** > **Threats** page displays suspicious network activity that may be associated with advanced malware threats.

Term and concept reference

As part of an ongoing effort to make the TRITON Unified Security Center and its modules more intuitive and consistent, several Web Security concepts, policy

components, and features have been given new names. For example, since category sets, yes lists, and protocol sets have similar roles in determining how policies filter client requests, they have been renamed category filters, limited access filters, and protocol filters, respectively, and are collectively referred to as “filters.”

The following list provides a quick reference to help you find features whose names have changed. This includes changes introduced in versions 7.0 through 7.7.

Original Term	New Term
Always Block (category set)	Block All (category filter)
category set	category filter
continue (filtering option)	confirm (action)
Custom URLs (Not Filtered)	permitted exceptions
Custom URLs (Recategorized)	recategorized URLs
delegated reporting role	investigative reporting role
directory objects	users or directory clients (all directory entries—users, groups, and domains [OUs]—that can be added as filtering clients)
disposition	action
Filter Definitions	• Policies • Filters (category filters, protocol filters, and limited access filters) • Filter Components (categories, protocols, custom URLs, keywords, and file types)
filtering option	action *or* filtering action
*Global policy	Default policy
History page	Web Security Dashboard (also includes the former Today page)
hits (used in reporting)	hits, *also* requests (generic term for hits and visits)
Log Server Configuration Utility	[discontinued], *replaced by* Settings > Reporting > Log Server (page in TRITON - Web Security)
Network Traffic Detector (*also*, Traffic Visibility Tool)	[discontinued]
Never Block (category set)	Permit All (category filter)
pattern	regular expression
protocol set	protocol filter
Real-Time Analyzer	[discontinued], *replaced by* Real-Time Monitor

Original Term	New Term
Remote Administrator	conditional Super Administrator (Some administrator permissions have changed. See *Delegated administration and reporting*, page 33.)
Save All (*also*, Save Changes)	Save and Deploy
Save Changes (*also*, Save All)	Save and Deploy
Super Administrator	unconditional Super Administrator (Web Security access only), *also* Global Security Administrator (access to all TRITON modules)
Today page	Web Security Dashboard (also includes the former History page)
Traffic Visibility Tool (*also*, Network Traffic Detector)	[discontinued]
Unfiltered URLs	exceptions (permitted)
URL pattern	regular expression
visits	visits, *also* requests (generic term for hits and visits)
Web Filter Lock	Filter Lock
WebsenseAdministrator	admin (Global Security Administrator)
Websense Explorer	investigative reports
Websense Manager	TRITON - Web Security (module of the TRITON Unified Security Center)
Websense Reporter	[discontinued], *replaced by* presentation reports
workstation (client)	computer
yes list	limited access filter

Finding information within TRITON - Web Security

To help you get the most from your Websense software, TRITON - Web Security includes 5 types of Help:

1	An icon accompanies many important product features. Position your mouse over this icon for a brief explanation of the feature.
2	For complex or advanced tasks, help text appears directly on the page, providing usage guidelines or other pointers for using a tool or field.

3	Detailed information about each page in TRITON - Web Security, often including step-by-step usage instructions, is also available. Click **Help** in the TRITON toolbar, and then select **Explain This Page**.
4	To browse the TRITON - Web Security Help, click **Help**, and then select **Contents**. The Help system is displayed in a separate browser window. For a printer-friendly version of the Help system in PDF format, click the Adobe PDF icon near the top, right corner of any Help page. (Adobe Reader must be installed to open this file.)
5	If you are unable to find the information you need within TRITON - Web Security, the **Help** menu provides links to the Websense Support Portal, the online source for all product, technical, and customer support resources, including a knowledge base and customer forums.

Third-party product support

Websense Web Security runs on a number of platforms and communicates with various third-party products to provide management capabilities, URL filtering, user-based policies, and reporting functionality.

Complete information about integration and interaction with third-party products can be found in the Deployment and Installation Center (available from support.websense.com). This section provides brief information about recently added product and platform support.

Browser support

In version 7.7, the TRITON Unified Security Center (including all reporting tools) can be accessed using the following supported browsers:

- Microsoft Internet Explorer versions 8 (not compatibility mode) and 9
- Mozilla Firefox versions 4.x and later
- Google Chrome version 13 and later

2 What's New in Version 7?

Websense Web Security and Websense Web Filter versions 7.0 and later include a browser-based interface to make it easier to configure and manage your Websense software from anywhere in the network.

If you're used to an earlier version of Websense Manager, you may want to start with an overview of the new interface:

- *The TRITON™ Unified Security Center*, page 7
- *Term and concept reference*, page 9

Your Websense software also includes a number of new features that you can use to:

- *Monitor Web Security status*, page 13
- *Verify your Websense filtering setup*, page 14
- *Create reports within TRITON - Web Security*, page 14
- *Maintain centralized policy information*, page 15
- *Back up and restore policy information*, page 16
- *Allow concurrent administrator logons*, page 16
- *Identify conditional Super Administrators*, page 17
- *Create exceptions to user identification settings*, page 17
- *Integrate with Websense Web Security Gateway*, page 18

Monitor Web Security status

When you open TRITON - Web Security, the **Status > Dashboard** page displays a **Threats** dashboard that summarizes suspicious activity that may be related to advanced malware threats in your network.

The Web Security Dashboard includes 3 other tabs:

- **Risks** shows information about permitted and blocked requests in the Security Risk class.
- **Usage** gives an overview of Internet activity in your network.

- **System** provides general health and status information for your deployment.

Super Administrators control which delegated administrators have access to dashboard reporting information.

Because the Web Security Dashboard was revised substantially in version 7.7, see *What's new in version 7.7?*, page 41, for more information.

Verify your Websense filtering setup

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The right shortcut pane includes a **Toolbox** that you can use to quickly find out how sites are categorized, how users are being filtered, and other information about your current filtering setup.

Tool	Description
URL Category	Find out how a site is categorized. Enter a URL, and then click **Go**. The site category is displayed. If the URL has been recategorized, the new category is shown.
Check Policy	Determine which policies currently apply to an individual client. (Multiple policies may apply when a user belongs to more than one group.) Enter a fully qualified user name or IP address, and then click **Go**. A list of policies is displayed.
Test Filtering	Find out what happens when a specific client requests a site. First enter a URL, then provide the fully qualified user name or IP address, and then click **Go**. The site category, the action applied to the category, and the reason for the action are displayed.
URL Access	See whether users have attempted to access a site in the past 2 weeks. Enter a URL, and then click **Go**. An investigative report shows whether the site has been accessed, and if so, when, and by whom. You might use this tool after receiving a security alert to find out if your organization has been exposed to phishing or virus-infected sites.
Investigate User	Review a client's Internet usage history for the past 14 days. Enter all or part of a user name (if user-based filtering applies) or IP address (for requests from machines to which user-based filtering is not applied), and then click **Go**. An investigative report showing the client's usage history is displayed.

Create reports within TRITON - Web Security

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

All Websense Web Security reporting tools have been integrated into the TRITON console. Like the charts on the Dashboard, investigative and presentation reports

require Log Server, a Windows-only component. (Real-Time Monitor, introduced in v7.6, does not require Log Server, but instead receives Internet filtering activity information from Usage Monitor. See *Introducing Real-Time Monitor*, page 32.)

The **Reporting > Presentation Reports** page replaces the Websense Reporter application. This page presents a list of predefined charts and tabular reports, each showing specific information from the Log Database.

- Run a report from the list of predefined reports.
- Use the Save As button to copy a predefined report, and then edit the report filter for the new report, specifying which clients, categories, protocols, and actions to include.
- Use the Edit button to update the report filter applied to any custom report.
- Mark a report as a Favorite to help you find it more quickly in the list.
- Schedule reports to run on a delayed or repeating basis, choosing one or more email recipients.

The **Reporting > Investigative Reports** page replaces Websense Explorer. This page presents a summary bar chart (default shows hits by risk class). Except that you access this tool from within the TRITON console, it operates just like Websense Explorer. For example:

- Drill down into specific details by making selections right on the chart.
- Expand the bar chart to show 2 levels of data.
- Use the flexible detail view to generate and modify your own tabular reports.
- Save a report as a Favorite that can be scheduled to run on a delayed or repeating basis.
- Investigate the Internet activity of a particular user by day or month.

Maintain centralized policy information

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

In previous versions of Websense software, each Policy Server stored its own client and policy configuration information. In multiple Policy Server environments, the Central Policy Distribution (CPD) and Central Configuration Distribution (CCD) tools provided a way to keep the disparate Policy Servers synchronized.

Now, a centralized **Policy Database** stores client and policy configuration information for multiple Policy Servers.

- The Policy Database is associated with TRITON - Web Security.
- Use TRITON - Web Security to log on to any Policy Server connected to the Policy Database.
- Administrator, client, and policy information added or edited on one Policy Server is shared by all Policy Servers connected to the Policy Database.

Information specific to a single Policy Server instance, such as Filtering Service or Network Agent connection information, is still stored separately by each Policy Server.

Back up and restore policy information

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The Websense Backup Utility simplifies the process of saving your Websense software settings and policy data and reverting to a specific configuration. Use the utility to:

- Perform an immediate backup or schedule automatic backups of your Websense software.
- Restore your Websense software configuration.
- Import an existing configuration.

The Backup Utility saves and restores:

- Global configuration information, including client and policy data, stored in the Policy Database.
- Local configuration information, such as Filtering Service and Log Server settings, stored by Policy Server.
- Websense component initialization and configuration files.

The Websense Backup Utility is accessed from the command line and should be run on each machine that includes Websense components. See the TRITON - Web Security Help for detailed information about using the tool.

Allow concurrent administrator logons

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

As in previous versions, you can use delegated administration to give specific administrators the ability to maintain policy information or run reports for a defined list of clients.

Now, multiple administrators can log on to the same Policy Server to do policy maintenance or reporting work at the same time.

- Only one administrator at a time can log onto each role with **policy** permissions.
- Multiple administrators can concurrently log on to the same role with **reporting** or **auditor** (*v7.6 and later*) permissions.

If you try to log on to a role that is currently in use by another administrator with policy permissions, you are given the option to log on to the selected role with:

- Reporting permissions only

- Read-only (temporary auditor) permissions (*v7.6 and later*)
- Status monitor access (Status > Dashboard and Alerts pages, plus Real-Time Monitor)

Alternatively, you can log on to another role that you are assigned to manage.

Identify conditional Super Administrators

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Administrators in the Super Administrator role can be given either of the following sets of permissions:

- Unconditional Super Administrators have full access to all policy management, reporting, and configuration settings.

  Global Security Administrators (*v7.6 and later*) are automatically granted unconditional Super Administrator access to the Web Security module.
- Conditional Super Administrators are given more limited access to configuration settings.

  Like Remote Administrators in v6.x and earlier, conditional Super Administrators can perform most policy management functions, but cannot alter the Filter Lock or configure many Settings pages.

Create exceptions to user identification settings

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

In addition to the transparent user identification and manual authentication options available in previous versions of Websense software, there is now a **selective authentication** option that lets you set specific authentication options for specific IP addresses.

Selective authentication lets you determine whether users requesting Internet access from a specific machine are identified transparently, prompted to log on to the browser (manual authentication), or never prompted for logon credentials. This can be used to:

- Establish different authentication rules for a machine in a public kiosk than for employees of the organization supplying the kiosk.
- Ensure that users of an exam-room computer in a medical office are always identified before accessing the Internet.

Click **Exceptions** on the **Settings > General > User Identification** page to establish specific user identification settings for some machines in your network.

Integrate with Websense Web Security Gateway

Websense Web Security Gateway takes Websense Web Security protection to the next level, allowing you to enable advanced analysis of online files and Web site content when they are requested. When activated, this analysis occurs only for sites not blocked by Websense Web Security.

- **Content categorization** reviews the content of permitted sites and returns a category for use in filtering.
- **Content security** looks at Web content to find security threats such as phishing, URL redirection, Web exploits, and proxy avoidance.
- **File analysis** inspects file content to determine a whether a threat (like a virus, Trojan horse, or worm) is present.

3 What's New in Version 7.1?

Version 7.1 introduces:

- New health alert messages on the Web Security Dashboard (see *Extended Health Alerts*, page 19)
- Enhanced **Save and Deploy** functionality (see *Safeguards for Save and Deploy*, page 20)
- Simplified process for creating and editing custom presentation reports (see *Edit presentation reports*, page 20)
- New Status > Dashboard charts for Websense Security Gateway (see *New reports for Websense Web Security Gateway*, page 21)
- New presentation reports for Websense Security Gateway (see *New reports for Websense Web Security Gateway*, page 21)

Extended Health Alerts

To help you monitor the status of your Websense software deployment, new health alert messages appear on the System dashboard and Status > Alerts page when:

- There is low (warning) or critically low (error) disk space on a Filtering Service machine.

  This can prevent Master Database downloads and updates.
- There is low (warning) or critically low (error) disk space on a TRITON - Web Security (formerly Websense Manager) machine.

  This can create problems generating presentation reports, or cause other performance problems on the machine.
- There is low (warning) or critically low (error) disk space on a Log Server machine.

  This can cause logging to become intermittent or to stop completely.
- There is low memory on a Filtering Service machine.

  This can prevent Filtering Service from applying Master Database updates.
- There is high CPU usage on the Filtering Service machine.

This can cause slow browsing or incorrect filtering for users, and may indicate a need for additional Filtering Service instances.

- There is low memory on a Network Agent machine.

  This can prevent Network Agent from starting, or cause incorrect filtering.

- There is high CPU usage on the Network Agent machine.

  This can result in incorrect filtering and logging.

- The Websense TRITON - Web Security (formerly ApacheTomcatWebsense) service cannot connect to Log Server.

  When this occurs, presentation report jobs being scheduled are not saved properly, and are lost when the Websense TRITON - Web Security service is restarted. In addition, reports on the Status > Dashboard page, or on the Presentation Reports page, may contain no data, even though data is being stored properly in the Log Database.

- One or more scheduled presentation reports failed.

  Use the Presentation Reports > Scheduler page to find out which jobs failed.

Safeguards for Save and Deploy

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

To ensure that changes are properly cached (or consciously abandoned), a new feature disables the **Save and Deploy** and **View Pending Changes** buttons on some Policy Management pages until you click **OK** or **Cancel**.

The Save and Deploy and View Pending Changes buttons are disabled, even if you have cached (but not saved) changes on other pages.

This change does not affect the Settings pages, or any page in other parts of TRITON - Web Security (formerly Websense Manager) that does not include an **OK** button (for example, Reporting > Investigative Reports or Policy Management > Policies).

Edit presentation reports

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Using presentation reports has been simplified. To help clarify which reports can be edited, and which are fixed, predefined reports are now marked with a "W" icon. You can still generate a predefined report by clicking **Run**, and then selecting the dates to be included.

You can now create a custom report in one step. Simply click **Save As** to create a copy of a predefined report and name the copy. Next, you can edit the report filter immediately, selecting specific clients, categories, protocols, or actions to include. Alternatively, you can return to the Report Catalog and customize the report filter later.

Custom reports are indicated marked with a stylized "user" icon. Select any custom report and click **Edit** to modify the report filter.

New reports for Websense Web Security Gateway

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

New reports provide insight into Websense Web Security Gateway content analysis.

By default, the Dashboard includes charts shows Content Gateway analytic activity.

In addition, 4 new presentation reports have been added. These reports are displayed in the Report Catalog in the Scanning Activity group only after scanning has detected sites whose content has changed from its Master Database classification.

Title	Description
Detail of Full URLs for Scanned Requests	Find out exactly which analyzed pages in each domain contained content that differed from the standard category, if full URLs are being logged. Use this information to improve your understanding of the changing nature of Internet content.
Summary of Scanned Requests by User	See which analyzed URLs were recategorized each day, summarized by user, date, and category. Learn which users are accessing the most sites with dynamically changing content, and evaluate whether policy changes are needed.
Top Categories by Scanned Requests	Find out which categories are identified most for requests subjected to analysis. Assess the security or productivity risk to your organization via Internet access.
User Activity Detail for Scanned Requests	See detailed information about which users requested sites whose analyzed content differed from the standard categorization. Find out what action was taken by Websense software as a result of the new category, and how much bandwidth was consumed.

4 What's New in Version 7.5?

Version 7.5 offers many new features as well as closer integration with other Websense security solutions. This section describes the following key additions and changes:

For a description of all new features, please refer to the v7.5 release notes.

Websense Web Security Gateway Anywhere

Websense Web Security Gateway Anywhere is a comprehensive and flexible security solution that combines Web filtering and data loss prevention (DLP) capabilities.

With a Web Security Gateway Anywhere subscription, your organization can combine Web filtering solutions to balance management and infrastructure needs:

- Use one console—the TRITON Unified Security Center—to perform policy management and reporting tasks for all users, regardless of how they are filtered.
- Maintain the powerful Web security solution that you have already installed and configured in your network.
- Take advantage of Websense hybrid filtering to reduce the need for additional hardware or infrastructure investment, for example, in satellite offices that may not have dedicated IT staff.
- Use remote filtering software, hybrid filter, or both to manage Internet access for users when they are off site.

This solution also includes full Content Gateway capabilities, including the ability to analyze sites and files to find malicious content, and to perform legacy antivirus scanning in real time, as users request sites.

In addition, Web Security Gateway Anywhere includes data leak prevention capabilities to help you regulate what types of content can be posted to the Web from within your organization.

Hybrid Web security

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Web Security Gateway Anywhere offers an alternative to pure service, software, or appliance-based Web security solutions. Rather than choosing between an in-the-cloud or on-premises solution for your enterprise, you can deploy a hybrid solution that encompasses the best of both worlds, and you can manage it from a single user interface: TRITON - Web Security.

An organization might use robust on-premises Web security for a corporate office or central campus, and branch offices or regional campuses through the hybrid service (no additional license required). This reduces the need for additional hardware or infrastructure investment, for example, in satellite offices that may not have dedicated IT staff.

Although you can still install remote filtering software to protect off-site users, you now have the option to use the hybrid service, as well.

Hybrid security introduces 2 new services, deployed with your Websense software:

- **Websense Sync Service** transports policy and user data to, and retrieves reporting data from, the hybrid service.
- **Websense Directory Agent** collates user and group information from your organization's directory service for use by the hybrid service.

Use the **Settings** > **Hybrid Configuration** pages to set up hybrid filtering, then use existing policy management and reporting features to apply policies to and review Internet activity for all clients, regardless of how they are filtered.

Two new charts on the Web Security Dashboard provide an overview of Internet activity by the members of your organization filtered by the hybrid service.

Chart Name	Description
Hybrid Requests Processed	Shows how many requests by users from your organization were permitted and blocked by the hybrid service.
Hybrid Bandwidth Usage	Shows the bandwidth consumed by Internet requests from users in your organization filtered by the hybrid service.

You can generated investigative reports by Source Server or Source IP to get more detailed information about clients filtered by the hybrid service. (Presentation reports show combined data for all clients, without distinguishing between those filtered by the hybrid and on-premises portions of your Websense software.)

Data loss prevention over the Web

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Websense Web Security Gateway Anywhere protects you from data loss over the Web, and when combined with Web filtering, this provides security for both inbound and outbound content.

After installing Websense Content Gateway, use the TRITON Unified Installer to install Websense Web Security and Websense Data Security, then use TRITON - Data Security to establish data security policies and view incidents and reports.

Data security policies contain rules, exceptions, conditions, and resources. Rules and exceptions define the logic of the policy. Conditions define the circumstances to watch for (such as a 16-digit number with a 4-digit date). And resources define the sources and destinations of data in your network as well as the action to take when a breach is discovered.

You can use predefined regulatory policies or you can create custom policies for your organization. In your policy, you define whether you want to monitor or block attempts to move sensitive data over Web channels (HTTP, HTTPS, or FTP over HTTP).

To identify your sensitive data, you can "fingerprint" it using the Websense patented PreciseID™ technology. (You can also identify key phrases, regular expression patterns, dictionaries, or file properties.)

You can link your Web and data security software to give Websense Data Security access to category information from the Master Database and user information from User Service.

Introducing TRITON - Web Security

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

As the Websense Web, data, and email security solutions continue to interoperate more closely, the TRITON Unified Security Center provides a centralized approach to managing Websense software.

When you log on to any TRITON module, a button tray shows the active module (highlighted in yellow), as well as the other existing TRITON modules.

- The names of modules that have been configured in your environment, and that are currently available, are shown in blue.
- The names of modules that have not been configured, or that are not currently available, are shown in gray.

The Help menu, which now contains links to the Websense Knowledge Base and customer forums, is in the TRITON toolbar (just under the Websense banner; moved in v7.6). The Select Policy Server and Save and Deploy functions have been moved to

the Web Security toolbar (below the TRITON toolbar). (See *The TRITON™ Unified Security Center*, page 7, for a visual overview of the new organization.)

TRITON - Web Security features collapsible left and right navigation panes to allow administrators to expand the content pane as needed. When the left navigation pane is minimized, one of the following narrow icon bars is displayed.

Each icon represents a functional grouping: Status, Reporting, and Policy Management on the Main tab; General, Alerts, Network Agent, and Reporting on the Settings tab. (Additional Settings groups appear in a Websense Web Security Gateway Anywhere deployment.) Hover the mouse pointer over any icon to access features within the group without expanding the navigation pane.

Security overrides

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

In previous versions, custom URL definitions and unlimited access filters (formerly yes lists) took priority over any Master Database categorization. This meant that if a site was defined as an unfiltered URL or a recategorized URL in a permitted category, or if it appeared in an unlimited access filter, the site was permitted, even if the site was also assigned to a Security Risk category (like Malicious Web Sites, Spyware, or Phishing and Other Frauds).

Version 7.5 introduced the option to configure Websense software to prioritize Security categorization over custom categorization. After the configuration change, if the Master Database or Websense Web Security Gateway scanning placed a site in a Security Risk category, and that category was blocked, the site was blocked.

In Version 7.6, the behavior was updated so that Filtering Server and the hybrid service prioritize Security Risk class categorization by default. See *Filtering based on Security Risk status*, page 36.

Improved presentation report generation

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

A new presentation reports feature offers improved performance of reports generated on the fly while making it easier to schedule and access very large reports.

When you run a report on the fly, choose between 2 options:

- Run the report in the background to schedule the report to run once, and run now.
- Run the report in the foreground to generate the report in a new window without scheduling it.

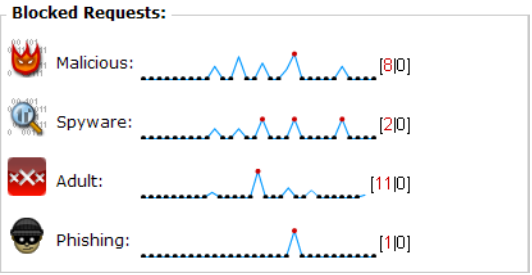
In either case, the report is run immediately. If you choose the option that schedules the report, you can elect to receive an email notification as soon as the report is ready. You can also monitor the job queue to check the status of the report. The report runs in the background, and is added to the Review Reports list when it is complete. This allows you to access and manage the report from within TRITON - Web Security.

If you prefer not to schedule the report, the report is generated in a separate window, allowing you to continue to work in TRITON - Web Security while the report is running. When the report is ready, you can view and save the report. The report is not, however, saved automatically, and does not appear in the Review Reports list.

Enhanced history page summary

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The **30-Day Risk Trends** section of the Risks dashboard has been enhanced to provide a more detailed overview of blocked requests in targeted categories over the past 30 days. A spark chart for each category highlights the peak number of blocked requests, while also providing general trend data about requests for those categories.



Click the peak number next to any line to open the Threats dashboard or investigative report (depending on category) with more detailed information about requests for the selected category.

Note that the 4 charts may each use a different scale. If one category has a peak of 500 requests, while another has a peak of only 10 requests, the charts may look similar, though the scale is very different. Use the numbers to the right of each chart to better assess its scale.

New settings for Websense Web Security Gateway

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Web Security Gateway and Web Security Gateway Anywhere administrators now have access to the following enhanced functionality, configured on the Settings > Scanning > Scanning Options page in TRITON - Web Security.

- **Embedded URL link analysis** can optionally be performed during content categorization for more accurate categorization of certain types of pages. For example, a page that otherwise has little or no undesirable content, but that links to sites known to be undesirable, can be more accurately categorized. URL link analysis can find malicious links embedded in hidden parts of a page, and can detect pages returned by image servers that link thumbnails to undesirable sites.
- A **content categorization sensitivity control** allows you to tune the sensitivity of the methods (classifiers) used to classify content and ultimately determine a category. It is important to understand that categorization results from content analysis that applies several methods (classifiers). The effect of changing the sensitivity level, with respect to resultant category, cannot be predicted. The sensitivity level is optimized (tuned) by Websense Security Labs using a very large URL test set, to provide accurate results across that test set.
- **Tunneled protocol detection** analyzes traffic as it transits Content Gateway to discover protocols that are tunneled over HTTP and HTTPS. Such traffic is reported to Filtering Service for protocol filtering enforcement. Scanning is performed on both inbound and outbound traffic. This feature can be used to block protocols used for instant messaging, peer-to-peer applications, and proxy avoidance.
- Security threat options now include the ability to scan, detect, and block **rich Internet applications**, such as Flash, that contain malicious code.
- A new security threat content scanning option supports the **scanning of outbound Web content for bot and spyware phone home traffic**. When phone home traffic is detected, it is forwarded to the scanning log database and categorized, so that you can run a report to obtain a list of the computers in your system that are infected with bot and spyware.

SSL decryption bypass (Content Gateway)

To support organizations using SSL Manager in Content Gateway to manage encrypted traffic, and who do not want to decrypt HTTPS sessions that users establish with sensitive sites (such as personal banking or health provider sites), administrators can now specify categories of sites that will bypass SSL decryption on the Settings > Scanning > SSL Decryption Bypass page in TRITON - Web Security.

For convenience, a predefined Privacy Category group includes categories that may be subject to regulatory requirements, such as education, financial data services, health care, and others. Administrators can also specify a list of hostnames or IP addresses for which SSL decryption is not performed.

New reports for Websense Web Security Gateway

New Status > Dashboard charts and presentation reports provide information about Web 2.0 sites requested by users in your organization and analyzed by Websense Web Security Gateway.

The Usage dashboard includes 2 new charts:

Chart Name	Description
Web 2.0 Categories	Shows the most frequently requested Web 2.0 categories. Use this information to learn more about Internet usage patterns and to discover potential productivity issues.
Web 2.0 Bandwidth	Shows the Web 2.0 sites that consume the most bandwidth. Use this information to evaluate whether policy changes are needed to manage bandwidth.

On the Presentation Reports page, 6 new report templates have been added to the Report Catalog that highlight scanning activity in your network.

Report Name	Description
Top Web 2.0 Categories Visited by Requests	Shows which categories are most frequently assigned to scanned Web 2.0 sites.
Top Web 2.0 Sites by Bandwidth	Shows which Web 2.0 sites consume the most bandwidth.
Top Web 2.0 Users by Browse Time	Shows which users spend the most time browsing Web 2.0 sites.
Web 2.0 User Activity Summary	Gives an overview who went to which Web 2.0 sites, and when.
Top Sites Blocked by Link Analysis	Shows which sites are being blocked by scanning link analysis.
Link Analysis: Detail of Full URLs	Provides the full URL of pages blocked by scanning link analysis, if full URLs are being logged.

5 What's New In Version 7.6?

Version 7.6 introduces the following new features and expanded functionality:

Enhanced TRITON Unified Security Center

Previously, the management consoles for Websense Web Security and Data Security were loosely integrated to form an initial shared user interface: the TRITON Unified Security Center.

This version introduces the next generation TRITON Unified Security Center, which provides centralized Web Security, Data Security, and Email Security administration and reporting, as well as:

- An access point for all V-Series appliances in your network. Click Appliances in the TRITON toolbar (just under the banner) to see information about all registered appliances.

- Centralized administrator account creation for all modules. Create administrators once on the TRITON Settings > Administrators page, and grant them access to one or more TRITON modules.
- Password recovery management for administrators in all modules. Configure SNMP settings on the TRITON Settings > Notifications page to enable this feature.

Now, all management components can be installed on a single Windows Server 2008 R2 machine, and accessed through the same user interface. Integration between modules is performed during installation, eliminating the need for manual linking of management consoles.

When Websense Web Security is installed by itself, without other Websense TRITON Enterprise modules, TRITON - Web Security can run on a Websense Appliance. This configuration is only recommended for evaluation purposes.

To support the changes to TRITON, the following Web Security services have new names:

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

Introducing Real-Time Monitor

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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 instance that has a Usage Monitor
- Can be used in environments that don't include other reporting tools

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.

New Log Database platforms

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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

Support for MSDE has been discontinued.

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.

Delegated administration and reporting

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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.

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.

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

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 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 and filters (except Permit All) that exist in the Super Administrator role.

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

New DC Agent health alerts

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Two health alerts have been introduced to warn administrators of common DC Agent configuration problems:

- A DC Agent instance has insufficient permissions

  This alert appears when DC Agent is run without the **domain admin** or **enterprise admin** permissions required for it to communicate with domain controllers and directory servers.
- A DC Agent instance is unable to access a required file

  This alert appears when DC Agent is unable to open, write to, or create the **dc_config.txt** file, which stores domain controller information.

Block pages

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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, and a site requested by that client is blocked, the block page includes a **Switch Credentials** button. The 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.

Filtering based on Security Risk status

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

When Filtering Service or the hybrid service determines that a site belongs to a Security Risk category, the site is now filtered based on Security Risk status, even when it is:

- A recategorized URL
- An unfiltered URL
- Included in a limited access filter

The ability to determine whether a Security Risk site is filtered based on Security Risk status or custom categorization was introduced in version 7.5. At the time, the default behavior was to prioritize custom categorization.

If you want to always filter based on custom categorization, regardless of whether a site appears in a Security Risk category (like Malicious Web Sites or Spyware), you can edit the **SecurityCategoryOverride** parameter in **eimserver.ini** and **syncservice.ini** to disable the default behavior. See "Prioritizing Security Risk categorization" in the TRITON - Web Security Help for details.

Monitoring Web Security status

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

As in previous releases, you have the option to monitor the Dashboard 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 Dashboard page, click the **Status Monitor** button in the toolbar at the top of the Dashboard, 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

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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

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

In addition, an updated Remote Filtering Client configuration utility (part of the TRITON Unified Endpoint Package Builder) makes it easy to create and edit Remote Filtering Client deployment profiles. Specify which Remote Filtering Server instances each set of clients uses, then set the installation mode and level of tamper protection for those clients.

Policy Server key management

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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.

User Service caching

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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 (now Save and Deploy) 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 action. Instead, the cache is cleared at save time only a when 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

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Version 7.6 introduced the ability to have Network Agent permit or block all IPv6 traffic.

This functionality has been expanded in version 7.7 to allow full filtering of IPv6 clients and URLs. See *IPv6 client and URL filtering*, page 53.

Usage alert editing

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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.

Internationalized domain name (IDN) support

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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

- Investigative and presentation reports
- Dashboard charts
- Usage Monitor category alerts
- Custom URLs
- 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

Because the Master (URL) Database uses Punycode, regular expressions and keywords that include Unicode characters will never find a match.

Content Gateway access and alerting

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

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 Dashboard, 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.

6 What's new in version 7.7?

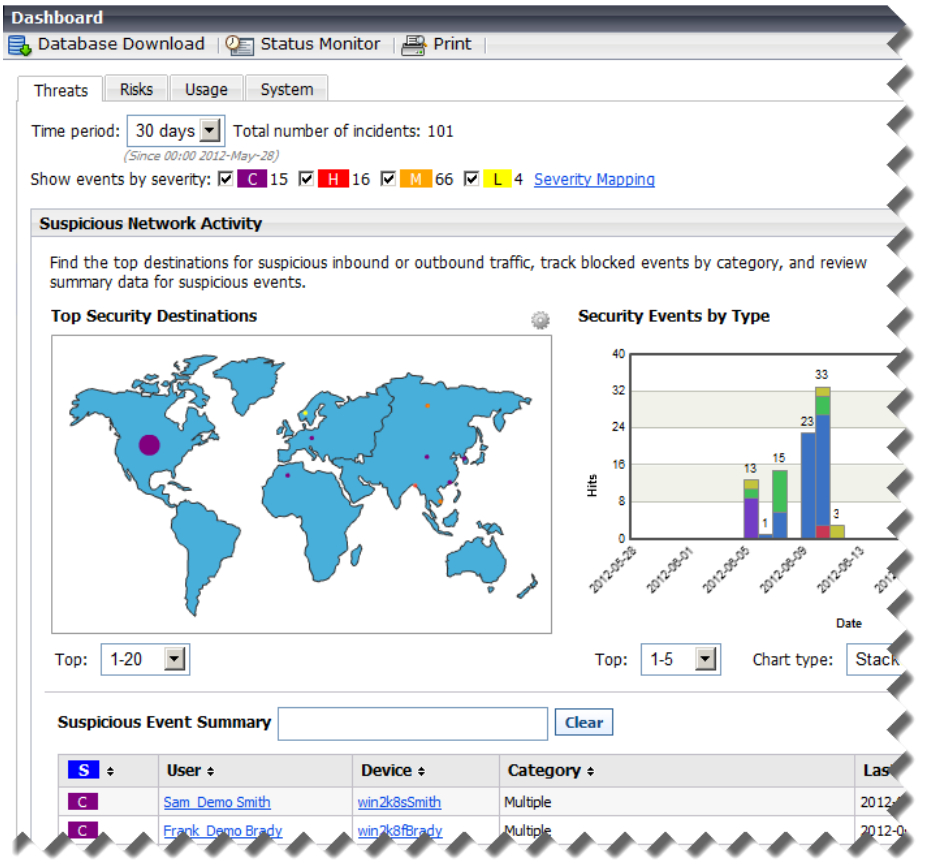
Version 7.7 introduces the following new features and expanded functionality:

Enhanced Web Security Dashboard

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The Status > Today and History pages have been merged and enhanced into a multi-tab Status > Dashboard page.

When you log on to TRITON - Web Security, the Threats dashboard is displayed, showing information about suspicious activity in your network. The type of information and level of detail depends on your subscription level. Web Security Gateway or Web Security Gateway Anywhere is required to display information about outbound threats and to provide detailed forensic data about the threats. See *Tools to fight advanced malware threats*, page 43.



The dashboard includes 3 additional tabs:

- **Risks** shows information about blocked and permitted requests for URLs that fall into the Security Risk class. The amount of information depends on your subscription level. Web Security, Web Security Gateway, or Web Security Gateway Anywhere is required to see information about requests in some security-specific categories.
- **Usage** shows information about traffic patterns in your network.

- **System** shows alert messages, status information, and graphical charts that show the current state of your Web security software, focusing on Internet activity in your network.

Elements on the Risks, Usage, and System dashboards can be configured to show data for various time periods (from one day to 30 days, by default). Most charts can be edited to display in bar, line, or pie chart format.

In addition, you now have the option to show multiple versions of the same dashboard element, either on the same tab, or on different tabs. You might display one Top Uncategorized chart with today's values, next to a Top Uncategorized chart for the last 2 weeks.

Up to 12 dashboard elements can be displayed on each tab.

Changes to dashboard charts and overall dashboard layout are saved separately for each administrator account.

Tools to fight advanced malware threats

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Use the **Threats** dashboard to monitor and investigate suspicious activity in your network that could indicate advanced malware attacks.

- Web Security Gateway or Web Security Gateway Anywhere is required to display information about outbound threats and to provide detailed forensic data about the threats.
- You cannot add elements to, nor remove elements from, the Threats dashboard.

The initial Threats dashboard has 3 main elements:

- **Top Security Destinations** shows the top 10 countries that are targets (destinations) for suspicious network traffic.
- **Security Events by Type** shows the number of blocked requests for sites (destinations) in security categories associated with malware threats.
- **Suspicious Event Summary** lists information about the severity, source IP address, user, host name (if available; requires Websense Content Gateway), category, time, direction, and destination of blocked and permitted requests associated with malware threats.

Controls at the top of the tab let you restrict the information displayed to specific severity types (Critical, High, Medium, or Low), directions (inbound or outbound), and time periods (since midnight, past 24 hours, past 48 hours, past week, and so on).

You can also click a geographical area or a category in the charts at the top of the page to further refine the information that appears in the summary table.

Click a user name, IP address, or device name in the summary table to see a detail page with information about all incidents associated with the selected client, including the forensics data (if any) collected.

Note that unconditional Super Administrators can grant access to the Threats dashboard while blocking access to forensics data associated with threat incidents. Because advanced malware attacks try to steal sensitive data from individuals and organizations, forensics data may include files containing sensitive information.

Severity-based alerting on suspicious Internet activity

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Websense software can notify you via email or SNMP when suspicious activity of a specified severity level (critical, high, medium, or low) reaches a defined threshold. Suspicious activity may be a sign of an advanced malware attack in your network.

- Define alerts for permitted requests and blocked requests at each severity level.
- Each alert message includes a link to the Threats > Event Details page that you can use to investigate the associated incidents.

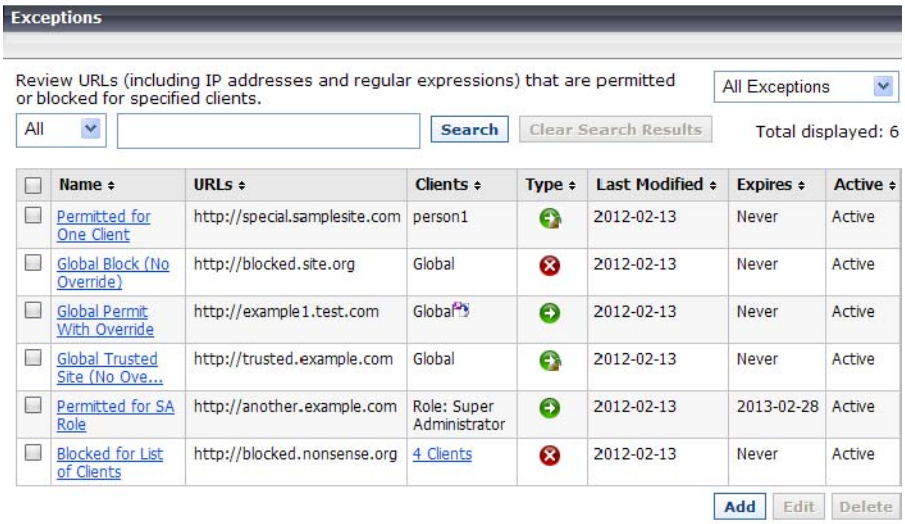
Use the **Settings > Alerts > Suspicious Activity** page to enable, disable, or change alerting configuration for alerts associated with suspicious events in your network.

Flood control settings configured for category and protocol usage alerts are also applied to suspicious activity alerts.

Exceptions: URL black and white lists

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Exceptions give administrators a way to quickly permit URLs and IP addresses in blocked categories, or block URLs and IP addresses in permitted categories.



Creating an exception does not require changing the category of a URL, nor does it change the policy assigned to affected clients. It simply allows a flexible and rapid response to user requests, changes in company policies, spikes in Internet activity, or other changes in circumstance.

Permitted exceptions replace unfiltered URLs as a method for permitting one or more clients to access URLs or IP addresses in blocked categories.

Manage exceptions on the **Policy Management > Exceptions** page in TRITON - Web Security.

Super Administrators see all exceptions, regardless of the role in which they were created. Delegated administrators see all exceptions that affect their current role.

Exceptions can be created for:

- A single client (user, group, OU, IP address, or network range)
- A list of specific clients (identified by user, group, or OU name, IP address, or IP address range)
- All clients in all roles (a global exception)

  Only Super Administrators can create global exceptions. When a global exception is created, the Super Administrator can specify whether the global exception takes precedence over all delegated administrator exceptions (the default), or whether delegated administrator exceptions can be used to override the global exception.
- All clients in a delegated administration role

Enhanced presentation reporting

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Presentation reporting has been enhanced to offer:

- The option to create your own reports from scratch. In addition to working from existing (custom or predefined) reports, you can select one of 2 **base templates** to create a **trend** or **top N** report.

Template Name	Description
Base Templates > New Trend Report	Used to define a new trend report. Provide a name and title for the report, assign it to a report category, then define the basic elements of the report, including: • Time unit (day, week, month, or year) • Sort option (category, protocol, risk class, action, user, or group) • Primary unit of measure (requests, browse time, bandwidth) • Additional units of measure (if requests are the primary unit of measure, browse time and bandwidth might be added as secondary measurements) Click **Save and Edit** to further refine the report using the same report filters used for any predefined or custom report.
Base Template > New Top N Report	Used to define a new top N report. Provide a name and title for the report, assign it to a report category, then define the basic elements of the report, including: • Sort option (category, protocol, risk class, action, user, or group) • Primary unit of measure (requests, browse time, bandwidth) • Additional units of measure (if requests are the primary unit of measure, browse time and bandwidth might be added as secondary measurements) Click **Save and Edit** to further refine the report using the same report filters used for any predefined or custom report.

- New predefined trend reports to track Social Networking and Security Risk trends.

Report Name	Description
Trends > Social Networking Trends by Requests	Shows requests for URLs in Social Networking categories over a selected period of time. Summary information showing request totals for each data point in the period are provided below the chart.
Trends > Security Risk Trends by Requests	Shows requests for URLs in Security Risk categories over a selected period of time. Summary information showing requests totals for each data point in the period are provided below the chart.

- A new **User-Defined** category in the Report Catalog for storing custom reports.
- Combined request, browse time, and bandwidth information (when available) in existing reports. Previously, all 3 measures could not be shown together.

Browse time available in investigative detail reports

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

In previous versions, investigative reports could include Internet browse time information only in summary reports. In version 7.7, you have the option to enable browse time calculation for investigative detail reports on the **Settings** > **Reporting** > **Log Database** page in TRITON - Web Security.

When this option is enabled, **Browse Time** appears as an available column when you are creating or modifying investigative detail reports.

- Saving browse time detail information increases the size of the Log Database. Monitor Log Database **Growth Rates and Sizing** data on the Log Database page after enabling this feature in case the size difference warrants changes to your rollover settings.
- Browse time information for detail reports is only available for dates subsequent to when the feature was enabled.

Enhanced file type blocking

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

In previous versions, when file type blocking was applied to a category, the blocking was performed based purely on file extension.

Now, when Websense Web Security Gateway and Gateway Anywhere customers enable file type blocking, when a user requests a site, Websense software:

1. Determines the URL category.
2. Checks the file extension.
3. If the file is not blocked by extension, Content Gateway or the hybrid service analyzes the file to determine its true file type.

In addition, the predefined file types used for extension matching have been extended as follows:

File Type	Associated Extensions
Compressed files	.ace, .arc, .arj, .b64, .bhx, .cab, .gz, .gzip, .hqx, .iso, .jar, .lzh, .mim, .rar, tar, taz, .tgz, .tz, .uu, .uue, .xxe, .z, .zip
Documents	.ade, .adp, .asd, .cwk, .doc, .docx, .dot, .dotm, .dotx, .grv, .iaf, .lit, .lwp, .maf, .mam, .maq, .mar, .mat, .mda, .mdb, .mde, .mdt, .mdw, .mpd, .mpp, .mpt, .msg, .oab, .obi, .oft, .olm, .one, .ops, .ost, .pa, .pdf, .pip, .pot, .potm, .potx, .ppa, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .prf, .pst, .pub, .puz, .sldm, .sldx, .snp, .svd, .thmx, .vdx, .vsd, .vss, .vst, .vsx, .vtx, .wbk, .wks, .wll, .wri, .xar, .xl, .xla, .xlb, .xlc, .xll, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .xsf, .xsn
Executables	.bat, .exe
Images	.bmp, .cmu, .djvu, .emf, .fbm, .fits, .gif, .icb, .ico, .jpeg, .jpg, .mgr, .miff, .pbf, .pbm, .pcx, .pdd, .pds, .pix, .png, .psb, .psd, .psp, .rle, .sgi, .sir, .targa, .tga, .tif, .tiff, .tpic, .vda, .vst, .zif
Multimedia	.aif, .aifc, .aiff, .asf, .asx, .avi, .ivf, .m1v, .m3u, .mid, .midi, .mov, .mp2, .mp2v, .mp3, .mpa, .mpe, .mpg, .mpv2, .ogg, .qt, .ra, .ram, .rmi, .snd, .wav, .wax, .wm, .wma, .wmp, .wmv, .wmx, .wxv
Rich Internet Applications	.swf
Text	.htm, .html, .txt, .xht, .xhtml, .xml
Threats	.vbs, .wmf

Extended information on block pages

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

When a user clicks **More Information** on a block page, a secondary block page displays:

- The **Real-time category**, if any, assigned to the URL. This is the category returned by Content Gateway analysis of the site.
- The **Static category** assigned to the URL in the Websense Master Database.
- Which Web Security component provided the category that led the site to be blocked (**Category set by**).

As in previous versions, administrators can right-click the top frame of More Information page for details about how the request was filtered.

In Websense Web Security Gateway and Gateway Anywhere deployments, there is now an option to enhance the security block page with a link to ACEInsight. This free service from Websense Security Labs can be used to review detailed information about a URL.

To enable the ACEInsight link on the security block page, navigate to the **Settings** > **General** > **Filtering** page in TRITON - Web Security.

When an HTTPS site is sent to ACEInsight for analysis, the block page passes only the domain portion of the URL. This prevents potentially sensitive information in the query string from being sent over the Internet. As a result, ACEInsight is not able to provide the same deep analysis of the page as Content Gateway performed, and may therefore return a different categorization than was used to block the request.

Centralized Log Server configuration

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The features and functions of the Web Security Log Server Configuration Utility have been integrated into the TRITON console. Instead of launching a separate tool to manage Log Server connection details, navigate to the **Settings** > **Reporting** > **Log Server** page in TRITON - Web Security.

Use this page to:

- Update Log Server port information.
- Manage the Log Database ODBC connection.
- Enable or disable SSL-encrypted communication with the Log Database (see *Support for SQL Server SSL encryption*, page 51).
- Manage the account Log Server uses to connect to the Log Database.
- Test communication between Log Server and the Log Database.
- Configure the method used to add log records to the database (ODBC or BCP), as well as where cache or BCP files are stored.
- Configure log record consolidation and specify whether to store hits or visits.
- Specify how often Log Server retrieves user and group information from User Service.

WebCatcher configuration is now performed on the **Settings** > **General** > **Accounts** page.

As a benefit of these changes, Log Server configuration updates no longer require restarting the Websense Log Server service. Changes to the database connection, however, do require a restart of the Websense TRITON - Web Security service so that dashboard charts and presentation reports can continue to retrieve reporting data.

Enhanced Log Database configuration

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The **Settings > Reporting > Log Database** page in TRITON - Web Security has been enhanced to improve the ease of Log Database configuration, as well as to support new features.

- A new **Growth Rates and Sizing** chart plots the average daily size of each Log Database logging partition.

  Use this information to plan for future growth and help optimize rollover scheduling.

- **Internet Browse Time** options now include the option to calculate detailed browse time information for use in investigative detail reports. See *Browse time available in investigative detail reports*, page 47.

  Enabling detailed browse time calculations increases Log Database size.

- To support trend reporting in the Web Security Dashboard and presentation reports, **Trend Data Retention** options let you choose whether to calculate and store trend data. You can also specify how long to store weekly, monthly, and yearly trend data. Daily trend data is stored for 90 days.

  Enabling trend data storage increases Log Database size.

Extended support for non-standard SQL Server ports

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

During TRITON Unified Security Center installation, you can now select a non-standard Microsoft SQL Server port. If you enter a non-standard port in the TRITON Infrastructure installer, that port information is passed to the Web Security installer.

Previous versions required that you use default port 1433 during installation, with the option to change the port once installation was complete.

You can still change the SQL Server connection port after installation, if needed, on the Settings > Reporting > Log Server page in TRITON - Web Security. (The separate Log Server Configuration Utility is no longer needed.)

Support for SQL Server SSL encryption

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

If your Microsoft SQL Server installation is configured to use SSL encryption, a new **Use SSL** option is available in the TRITON Unified Installer and on the Settings > Reporting > Log Server page in TRITON - Web Security.

> **Important**
> Depending on your Microsoft SQL Server configuration (if "Trust Server Certificate" is set to "No" in SQL Server), you may need to deploy CA-signed certificates to the SQL Server, TRITON management server, and Log Server machines before you enable this feature in either the installer or the TRITON console.

This allows organizations with special security requirements to encrypt the data that Log Server sends to the Log Database.

See your Microsoft SQL Server documentation for information about configuring SSL encryption.

Enhanced DC Agent configuration

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

DC Agent uses a file called **dc_config.txt** to record the domains and domain controllers it finds. When one or more DC Agent instances are installed in your network, you can now review the complete list of domains and domain controllers polled by all DC Agent instances in your network from within TRITON - Web Security. Just navigate to the **Settings > General > User Identification** page and click **View Domain List**.

In addition, you can now configure DC Agent domain discovery settings on the **User Identification > DC Agent** page.

- Enable or disable automatic domain discovery (the process by which DC Agent automatically identifies the domains and domain controllers it can query).
- Specify how often DC Agent performs its discovery process.
- Configure whether domain discovery is performed by DC Agent or User Service.

As in previous versions, these settings can also be configured manually in the **transid.ini** file for each DC Agent instance. (The transid.ini file is no longer created at installation time, but it is preserved on upgrade, and can also be created manually.)

New transparent identification and logging health alerts

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

A series of new health alerts notify administrators when Filtering Service cannot communicate with a Websense transparent identification agent:

- Filtering Service is unable to communicate with DC Agent.
- Filtering Service is unable to communicate with Logon Agent.
- Filtering Service is unable to communicate with eDirectory Agent.
- Filtering Service is unable to communicate with RADIUS Agent.

When a network issue or other communication problem prevents Filtering Service from communicating with a transparent identification agent, the Filtering Service user map may not be updated in a timely manner, and user-based policies may not be applied correctly.

Other new health alerts give administrators early notification of potential Log Database and Log Server issues:

- The cache directory for a Log Server contains more than 100 cache files.

  Normally, Log Server cache files are moved to the Log Database at a steady rate. If cache files are accumulating, there may be a network issue, a change to the account that Log Server uses to connect to the Log Database, disk space problems on the Log Database machine, or other issues.
- Log Server has not received log files from Filtering Service for over an hour.

  Filtering Service is responsible for providing log data to Log Server. If Filtering Service cannot communicate with Log Server, that log data is lost.
- The Log Database ETL job has not completed successfully after 4 hours

  The ETL (Extract, Transform, and Load) job is responsible for processing data into the partition database. It requires sufficient disk space, disk speed, and other system resources to run efficiently.

Time-based actions in multiple Filtering Service deployments

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

If your deployment includes multiple instances of Filtering Service that might handle a request from the same user, an optional component, **Websense State Server**, can be installed to enable proper application of time-based filtering actions (Quota, Confirm, Password Override, and Account Override).

When State Server is installed, it allows its associated Filtering Service instances to share timing information, so users receive the correct allotment of quota, confirm, or override session time.

State Server is typically installed on a Policy Server machine, and only one State Server instance is required per **logical deployment**. A logical deployment is any group of Policy Server and Filtering Service instances that might handle requests from the same set of users.

- All Filtering Service instances that communicate with the same State Server instance must share the same time zone, and the time on all machines must be in synch.
- Each Filtering Service instance can communicate with only one State Server.
- All Filtering Service instances associated with the same Policy Server must communicate with the same State Server.
- Multiple Policy Server instances can share a single State Server.

Integration with third-party SIEM solutions

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

If your organization uses a supported Security Information and Event Management (SIEM) solution, you can configure Websense software to forward log data from Filtering Service to the SIEM product.

Before you enable SIEM integration, you must install a new component, **Websense Multiplexer**, for each Policy Server in your deployment.

Enable SIEM integration on the **Settings > General > SIEM Integration** page in TRITON - Web Security, then select the syntax to use in formatting the data (syslog/CEF [Arcsight], syslog/LEEF [QRadar], syslog/key-value pairs [Splunk and others], or custom). If you select custom, you are prompted to provide a format string.

Once SIEM integration is enabled, Multiplexer begins passing data from Filtering Service to both Log Server and the SIEM product.

IPv6 client and URL filtering

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The ability to block and permit IPv6 traffic using Network Agent, introduced in v7.6, has been extended to allow full filtering of IPv6 addresses.

- Create custom URLs or exceptions to recategorize, block, or permit Web sites identified by IPv6 address.
- Add and assign policies to clients identified by IPv6 address or range.

No special configuration is required to enable this functionality.

When a field in TRITON - Web Security requires a specific IP address format, the format is noted (for example, "IPv4 address"). Otherwise, either format can be used.

The machines hosting Websense Web Security components must have an IPv4 address.

Super Administrator direct access to Content Gateway Manager

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Websense Web Security Gateway and Gateway Anywhere Global Security Administrators and unconditional Super Administrators can now enable single sign-on access for Super Administrators connecting to Content Gateway Manager from within TRITON - Web Security.

When single-sign-on access is enabled, Super Administrators with **Content Gateway single sign-on** permissions can navigate to the **Settings > General > Content Gateway Access** page in TRITON - Web Security and click **Log On** next to the IP address or hostname of a Content Gateway instance.

Content Gateway single sign-on permissions are granted when the administrator is added to the Super Administrators role, and can be removed by any unconditional Super Administrator.

The administrator is taken directly to Content Gateway Manager without seeing a logon page or having to enter credentials.

Enhanced Directory Agent configuration

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The **Settings > Hybrid Configuration > Shared User Data** page in TRITON - Web Security has been enhanced to make it easier for Websense Web Security Gateway Anywhere administrators to configure Directory Agent to include and exclude specific directory service contexts.

Instead of typing in directory context information, the directory tree is displayed. Navigate to the context that you want to include or exclude from Directory Agent searches, or use search to display matching contexts in the tree.

This helps administrators to more easily:

- Identify contexts containing users filtered by the hybrid service.
- Limit which directory contexts are synchronized with the hybrid service to save time and enhance performance.
- Exclude contexts that might lead to synchronization problems (for example, contexts containing groups with duplicate email entries).

Hybrid user agent reporting and custom authentication

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The **Status > Hybrid Service** page now includes a link to the **User Agent Volume** report. The report output consists of a table, showing:

- User agents that have requested authentication.

  A user agent is the string sent from the browser or application to identify itself, its version number, and system details like operating system.
- The number of authentication requests and total requests made by each user agent.
- When the number of requests was last updated.
- Whether or not a custom authentication rule has been created for the user agent.

If a user agent in the report has a high number of authentication requests, it may be experiencing authentication problems. You can create a new custom authentication rule to allow the agent to either bypass authentication or use a different type of authentication. Select on or more user agents in the report, then click **Create Rule**.

Custom authentication rules are configured on the new **Settings > Hybrid Configuration > Custom Authentication** page. Here, you can identify applications that do not properly handle authentication challenges by specifying user agents, domains, or URLs, or a combination of these options.

After defining the application, specify which type of authentication, if any, to use.

On-premises failover to the hybrid service

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Websense Web Security Gateway Anywhere administrators now have the option to configure failover to the hybrid service for filtered locations that use explicit proxies. This ensures that users are able to access the Internet and are always filtered in the event that your other proxies are unavailable.

Failover to the hybrid service for a filtered location must be approved, to ensure that Websense services can provision the correct number of users at the data center nearest to your location. Once failover for a filtered location has been approved, it does not need to be re-approved if you change the failover details or later disable and then re-enable failover.

Other hybrid service enhancements

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

- The **Settings > Hybrid Configuration > Filtered Locations** page has been enhanced to more clearly distinguish between locations filtered by on-premises components and locations filtered by the hybrid service.
- The **Settings > Hybrid Configuration > Hybrid User Identification** page now includes the option to create or change the Web Endpoint anti-tampering password.
- The **Settings > Hybrid Configuration > Hybrid User Identification** page now includes an additional method for user identification and authentication. In addition to NTLM and basic authentication, secure form authentication can be used.
- For sites that want to use the default PAC file, but have port 8082 or 8081 locked down, the Proxy Auto-Configuration File section of the **Settings > Hybrid Configuration > User Access** page now offers 2 options:
  - The default PAC file URL, retrieved over port 8082 (also requires port 8081)
  - An alternate PAC file URL, retrieved over port 80

7 Where Do I Find...?

The upgrade process preserves your existing client, policy, and configuration information. Changes to TRITON - Web Security (formerly Websense Manager), however, mean that some common features and functions have moved or been renamed.

Use this section to locate your accustomed tools, features, and functions as you become more familiar with TRITON - Web Security.

To get started, select the tool or function that you want to locate:

My Global policy

Your ***Global** policy has been renamed **Default**.

- It still enforces the same filtering settings on the same schedule.
- It still filters all clients whenever no other policy applies.

To verify that your filtering settings have not changed, go to **Policy Management > Policies**, and then click **Default**. Click a time period in the schedule to see which filters (formerly category sets, protocol sets, and yes lists) are enforced by the policy.

Important

The **Default** policy should cover all time periods, 24 hours a day, 7 days a week. If your Global policy contained gaps, after upgrade, you are not automatically prompted to provide complete coverage. When you edit the Default policy, however, you cannot save changes until all gaps are filled.

My Default Settings category and protocol sets

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Your **Default Settings** category and protocol sets have been renamed. They are now the **Default** category and protocol filters.

This is a rename only. It does not affect your filtering settings.

To verify the settings enforced by the Default category and protocol filters, go to **Policy Management > Filters**, and then click the filter name in the appropriate list.

My Today and History pages

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The Today and History pages have been merged into the **Web Security Dashboard**. The dashboard includes 4 tabs: Threats, Risks, Usage, and System.

Changes to dashboard tabs and charts are saved separately for each administrator account.

The charts and counters available in versions 7.0 and later are distributed across the Risks, Usage, and System dashboards.

Where a “today” and “history” version of the same chart existed in previous versions, there is now a single chart that can be configured to show data for “today” or a longer (configurable) time period. You can also display 2 copies of the chart, one showing today’s data, and one showing a longer period.

You can change which charts and counters are displayed on which tabs.

The Threats dashboard introduces new tools you can use to monitor suspicious activity often associated with advanced malware attacks. The charts and tables that populate this tab did not exist before v7.7.

My yes lists

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Yes lists have been renamed **limited access filters**. Category, limited access, and protocol filters are all managed via the **Policy Management > Filters** page.

To view or edit the contents of a limited access filter, click its name in the **Limited Access Filters** list.

My custom URLs

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Custom URLs now fall under the general heading of **Filter Components**.

To view and edit **recategorized URLs** (formerly Custom URLs/Recategorized), go to **Policy Management > Filter Components** and click **Edit Categories**. Select a category to see the recategorized URLs in that category.

Unfiltered URLs (formerly Custom URLs/Not Filtered) have been replaced by permitted **exceptions**. See *My unfiltered URLs*, page 59.

My unfiltered URLs

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The functionality formerly offered by unfiltered URLs is now performed by **permitted exceptions**. An exception allows you to permit or block one or more URLs for one or more clients.

On upgrade, unfiltered URLs are translated into permitted, single-role exceptions. The permitted exception is applied to all clients in the role in which the unfiltered URL was defined.

Use the **Policy Management > Exceptions** page to create and manage both blocked and permitted exceptions.

My directory objects

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

In TRITON - Web Security, the general heading **Directory** has replaced Directory Objects. This umbrella term includes, users, groups, domains, and organizational units defined in a supported directory service.

To view, add, or edit these clients, go to **Policy Management > Clients**, and then expand the **Directory** tree.

Websense Explorer

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Websense Explorer has been replaced by investigative reports, which is accessed directly in TRITON - Web Security. Note that this requires that Log Server be installed on a Windows machine. Click **Reporting > Investigative Reports** in the left navigation pane to create, schedule, and run reports in much the same way you did with Websense Explorer.

Websense Reporter

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Websense Reporter has been replaced by presentation reports, which is accessed directly in TRITON - Web Security. Note that this requires that Log Server be installed on a Windows machine. Click **Reporting > Presentation Reports** in the left navigation pane to define custom report filters, schedule reports, and run reports with this tool.

The Log Server Configuration Utility

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The features and functions of the Log Server Configuration Utility have been centralized into TRITON - Web Security.

Navigate to the **Settings > Reporting > Log Server** page to manage Log Database connection information, ODBC and BCP settings, consolidation, hits and visits settings, and User Service connection settings.

WebCatcher settings are now configured on the **Settings > General > Account** page.

My reports

A large number of predefined report templates were provided as part of Websense Reporter. Many of the templates provided substantially similar information, with only slight variations of format or preselected content (users, categories, and so forth).

For presentation reports, the templates have been streamlined so that a particular format and content is presented as a single predefined report. You can copy any predefined report and edit the report filter to select a different combination of clients, categories, protocols, and actions (formerly called dispositions).

Following is a list of reports from the v6.3.x Reporter application, and the presentation report name for the v7 equivalent.

v6.3.x Report	v7 Report
Detail of Destinations by User	User Activity Detail (also replaces the previous User Activity Detail report)
Top Categories by Blocked Internet Access	Top Blocked Categories by Requests (without % figures)
Dispositions by Occurrences	Top Filtering Actions by Requests
Top Categories by Internet Browse Time	Top Categories by Browse Time
Top Categories by Bytes Transferred	Top Categories by Bandwidth
Top Categories by Hits	Top Categories Visited
Top Groups by Internet Browse Time	Top Groups by Browse Time
Top Groups by Bytes Transferred	Top Groups by Bandwidth
Top Groups by Hits	Top Groups Activity by Requests
Top Destinations by Internet Browse Time	Top Sites by Browse Time (without category)
Top Destinations by Bytes Transferred	Top Sites by Bandwidth (without category)
Top Destinations by Hits	Top Sites Visited (without category)
Top Users by Internet Browse Time	Top Users by Browse Time
Top Users by Bytes Transferred	Top Users by Bandwidth
Top Users by Hits	Top Users Activity by Requests
Corporate Risk Summary	(to be added)
Top Destinations by Blocked Internet Access	Top Blocked Sites by Requests (without % and category)

v6.3.x Report	v7 Report
User Activity Detail	User Activity Detail (also replaces the previous Detail of Destinations by User report)
Top Groups by Blocked Internet Access	Top Blocked Groups by Requests (without %)
Top Protocols by Blocked Internet Access	Top Blocked Protocols by Requests (without %)
Protocols by Bytes Transferred	Top Protocols by Bandwidth
User Destination Summary	User Activity Summary (also replaces previous Summary of Destinations by Date and User report)
Top Users by Blocked Internet Access	Top Blocked Users by Requests
Summary of Destinations by Date and User	User Activity Summary (also replaces User Destination Summary report)

The following reports, which were available in Websense Reporter v6.3.x, can be substantially recreated in the summary or detail view of investigative reports. Cost and percent values, however, are not supported in v7.

- Detail of Bytes Transferred by Category
- Detail of Bytes Transferred by User
- Detail of Bytes Transferred by Group
- Detail of Users by Category
- Detail of Groups by Category
- Detail of Full URL Destinations by Category and Date
- Detail of Bytes Transferred by Protocol
- Detail of Bytes Transferred by Date and Protocol
- Detail of Destinations by Group
- Categories by Bytes Transferred
- Group Activity Detail—(multiple)
- Detail of Groups by Protocol
- Summary of Groups by Protocol
- Protocol Analysis – Bandwidth
- Protocol Analysis – Hits
- Summary of Categories by Hits
- Summary of Internet Browse Time by Category
- Summary of Internet Browse Time by Destination
- Group Bandwidth Summary
- Group Internet Browse Time Summary
- Group Destination Summary
- User Bandwidth Summary
- User Internet Browse Time Summary
- Summary of Top Destinations by Hits
- Details of Users by Protocol
- Summary of Users by Protocol
- Summary of Bytes Transferred by Category
- Summary of Bytes Transferred by Date and Category
- Summary of Bytes Transferred by User
- Summary of Bytes Transferred by Date and User
- Summary of Bytes Transferred by Group
- Summary of Bytes Transferred by Date and Group
- Summary of Categories by Date and User
- Summary of Categories by Date and Group
- Summary of Destinations by Group
- Summary of Destinations by Date and Group
- Summary of Destinations by Time of Day and Group—(not summary level)
- Summary of Bytes Transferred by Protocol
- Summary of Bytes Transferred by Date and Protocol
- Summary of Top Destinations by User
- Summary of Top Destinations by Bytes Transferred and Category
- Summary of Top Destinations by Bytes Transferred
- Summary of Destinations by User
- Summary of Destinations by Time of Day and User—(not summary level)
- Internet Browse Time Total

Real-Time Analyzer

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Websense Real-Time Analyzer has been replaced with a combination of other tools:

- **Real-Time Monitor** shows what URLs are currently being requested 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. See *Introducing Real-Time Monitor*, page 32.

- Graphical charts on the **Status > Dashboard** page provide an overview of filtering volume, summaries of filtering activity, and filtered request statistics. Also find:
  - Filtering health alerts relating to system resource issues for key components, Master Database download problems, service failures, and more.
  - Information about each Filtering Service instance associated with the active Policy Server, including the status of each service's connection to Network Agent and Content Gateway.

My server settings

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The Websense software configuration options previously accessed via the Server > Settings menu in Websense Manager are now accessed by clicking the **Settings** tab in the left navigation pane of TRITON - Web Security.

My Network Agent local settings

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

To access Network Agent local settings, click the **Settings** tab in the left navigation pane, expand the **Network Agent** section, if necessary, hover the mouse pointer over **Global**, and then click the IP address of the Network Agent instance that you want to configure. This brings up the Local Settings page for the selected Network Agent instance.

Administrator account management

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Both local administrator accounts (formerly Websense user accounts) and network administrator accounts are now managed at the TRITON level, rather than within the Web Security module. Click **TRITON Settings** in the TRITON toolbar, then click **Administrators** in the left navigation pane. Here, you can:

- Add and delete administrator accounts
- Set administrator passwords
- Determine which TRITON modules each administrator can access

Only administrators with Global Security Administrator permissions can create and remove administrator accounts.

A Global Security Administrator determines whether or not an account has unconditional Super Administrator permissions in the Web Security module. A Super

Administrator within the Web Security module must add delegated administrators to one or more roles and set their level of permissions.

A delegated administrator who has been granted Web Security access by a Global Security Administrator but who has not yet been added to any roles can see some parts of the Status > Dashboard page, but is unable to access any other Web Security features.

The former Manage Administrator Accounts page in TRITON - Web Security is now called **View Administrator Accounts** and lists administrators with Web Security access and shows which roles, if any, they are assigned to. Only administrators listed on this page (and **admin**, the default Global Security Administrator account) can be added to TRITON - Web Security roles.

The Network Traffic Detector (Traffic Visibility Tool)

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The Network Traffic Detector (formerly Traffic Visibility Tool) is no longer included with Network Agent. Instead, Websense, Inc., recommends using a third-party packet sniffing tool, like Wireshark, to verify that each Network Agent instance is able to see traffic from the IP addresses that it is assigned to monitor.

Subscription key management

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Policy Server subscription key management has been expanded.

- If no subscription key has been entered (for example, directly after installation), a popup message prompts subscription key entry.
- If the popup is not used, the key for the current Policy Server can be entered on the Settings > General > Account page.
- In multiple Policy Server environments, use the **Settings > General > Policy Servers** page to manage keys for all of your Policy Server instances.
  - If multiple Policy Server instances share a key, designate one as the primary, and enter the key. Designate the remaining Policy Server instances as secondary Policy Servers.

    This allows them to inherit subscription key settings from the primary server (to simplify key management), but does not affect their function.

    If a new key is entered for the primary Policy Server, key information for all secondary Policy Server instances is updated automatically.
  - If each Policy Server instance has its own key, designate each as a primary. Key and subscription level information is shown for each primary Policy Server separately.

8 How Do I...?

Although there have been some significant changes to the management interface, the basic steps involved in performing most filtering, reporting, and configuration tasks are not dramatically different than in previous versions.

Use this section as a quick reference to help you resume your accustomed tasks in TRITON - Web Security.

Download the Master Database

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

The **admin** account and members of the Super Administrator role can manually initiate a download of the Websense Master Database at any time from the **Status** > **Dashboard** page in TRITON - Web Security.

1. Click **Database Download** in the toolbar at the top of the content pane.

   A list of Filtering Service instances associated with the current Policy Server is displayed.
2. Click the **Update** button to the right of any Filtering Service IP address, or click **Update All** to download a Master Database update on all Filtering Service machines.
3. Click a Filtering Service IP address in the list on the left to view the progress of the download, or click **Close** to return to the dashboard.

If you are logged on to TRITON - Web Security with policy permissions when the Master Database update adds or removes categories or protocols, the category or protocol changes are not shown in TRITON - Web Security until you log off and log on again.

Configure automatic downloads on the **Settings** > **General** > **Database Download** page.

Add clients

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Use the **Policy Management** > **Clients** page to add clients to TRITON - Web Security.

1. Click **Add** (below the Clients list).
2. Identify the clients that you want to add:
   - If you have configured Websense software to communicate with your network directory service, browse the **Directory** tree to locate users, groups, or domains (OU) to add as clients.

     If you are using an LDAP directory service, you can also use **Search** to identify user, group, or domain (OU) clients.
   - To add a single machine in your network as a client, enter the IP address or host name of the machine under **Computer**.
   - To add a group of machines with contiguous IP addresses as clients, enter the starting IP address and ending IP address under **Network**.
3. Click the appropriate right arrow (>) button to add the clients to the **Selected** list.
4. Click **OK** to cache your changes and return to the Clients page. Changes are not implemented until you click **Save and Deploy**.

Create a policy

Use the **Policy Management > Policies** page to add policies in TRITON - Web Security.

1. Click **Add** below the list of policies.
2. Enter a unique **Policy name** (maximum 50 characters) for the new policy.
3. Enter a **Description** (maximum 255 characters) for the policy. This should clearly state the policy's purpose to help with maintenance over time.
4. If you want to use an existing policy as the basis for the new policy, mark **Base on existing policy**, and then select a policy from the drop-down list.
5. Click **OK** to cache your changes and go to the Edit Policy page.
6. Use the Edit Policy page to make changes to the policy schedule and the filters enforced by the policy.

   Go to **Help > Explain This Page** on the Edit Policy page for detailed instructions.
7. When you are finished making changes, click **OK** to cache your changes and return to the Policies page. Changes are not implemented until you click **Save and Deploy**.

Assign a policy to clients

There are 2 ways to assign policies to clients:

- On the **Policy Management > Policies > Edit Policy** page for the policy you want to assign to clients, click **Apply to Clients** in the toolbar at the top of the page. Select one or more clients from the tree, and then click **OK**.
- On the **Policy Management > Clients** page, select one or more clients in the tree, and then click **Edit**. Under Policy, click **Change**, and then select a new policy from the drop-down list. When you are finished, click **OK**.

When you are finished assigning policies to clients, click **Save and Deploy** in the right shortcut pane to save and implement your changes.

Verify that the correct policy is applied

1. Click **Check Policy** in the right shortcut pane.
2. Identify the client whose filtering policy you want to verify:

- For users, groups, domains, and organizational units, enter the fully qualified distinguished name of the user, or click **Find User**.

  If you are using an LDAP-based directory service, clicking Find User gives you the option to either browse or search the directory.
- For computer clients, enter an IP address.

3. Click **Go**.

A pop-up window displays the policy currently applied to the client.

Generate a presentation report

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Use the **Reporting > Presentation Reports** page to generate a presentation report.

1. Expand the entries in the Report Catalog and highlight the report that you want to generate.
2. Click **Run**, and then select the dates to include and the output format.
3. Under Report Generation, use the **Schedule the report to run in the background** check box to determine how the report is run:
   - If the checkbox is marked, when you click **Run**, the report is scheduled to run immediately, and starts running in the background. If you supply an email address, the report is sent to one or more recipients when complete. The report can also be accessed from the Reporting > Presentation Reports > Review Reports page.
   - If the checkbox is deselected, when you click **Run**, a new browser window opens, showing the progress of the report generation process. When the report is ready, it is either displayed in the browser window, or you are prompted to open or save the file. The report is not stored automatically, and does not appear on the Review Reports page.
4. When you have selected how the report will be run, click **Run**.

To select a different combination of data for the report:

1. Highlight a predefined report or existing custom report, and then click **Save As**.
2. Enter a display name for the report. This is the name that will appear in the Report Catalog.
3. Click **Save and Edit**.
4. Fill in the tabs of the **Edit Report Filter** page to select exactly the users, categories, protocols, and actions to be included.
5. Choose whether to just save the new report definition for future use, save and run the report immediately, or save and schedule it to run on a delayed or repeating basis.

To schedule presentation reports, click **Scheduler** at the top of the Presentation Reports page. Then, fill in the tabs of the **Scheduler** page to define the job.

Generate an investigative report

The **Reporting > Investigative Reports** page displays a bar chart showing hits by risk class. Since this page is virtually identical to the main page in Websense Explorer for previous versions, use the familiar techniques to generate a report.

- Click a risk class name in the left column, and then choose **Categories**, for example, to show information for all the categories associated with the selected risk class.
- Make selections in the gray bar above the chart to create a multi-level report, showing, for example, the top 5 users in each of the top 10 categories.
- Click a bar or number to generate a detail report showing the associated data.
- Click **Favorite Reports** to save the current report as a Favorite, and access scheduling options.
- Click **Outliers** to find the users whose Internet usage is statistically different from others in the organization.

Create or edit a custom category

Use the **Policy Management > Filter Components > Edit Categories** page to create and modify custom categories.

The existing categories, both Websense-defined and custom, are listed in the left portion of the content pane. To see current custom settings associated with a category, or to create new custom definitions, first select a category from the list.

To see a list of all custom URLs, keywords, and regular expressions associated with all categories, click **View All Custom URLs / Keywords** in the toolbar at the top of the page.

- To create a new category, click **Add**.

  To remove an existing custom category, select the category, and then click **Delete**. You cannot delete Websense-defined categories.
- To change the name or description of a custom category, click **Rename**.
- To change the filtering action (Permit, Block) associated with a category in all category filters, click **Override Action**.

Recategorize a URL

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

1. Do either of the following:
   - Click **Recategorize URL** in the right shortcut pane.
   - Go to **Policy Management > Filter Components**, and then click **Edit Categories**.
2. Select a category from the list. Category information, including a list of recategorized URLs and keywords associated with the category, appears to the right of the category tree.
3. Click **Add URLs** in the Recategorized URLs box.
4. Enter the URLs or IP addresses that you want to associate with the selected category, one per line.
5. Click **OK** to return to the Edit Categories page, and then click **OK** again to cache your changes. Changes are not implemented until you click **Save and Deploy**.

Permit a URL for all clients

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Super Administrators can use the following steps to permit a URL for all clients:

1. Click **Create Exception** in the right shortcut pane.
2. Enter a unique **Name** for the exception.
3. Enter the **URL** that you want to permit.
4. By default, the exception is set to apply to all clients (**Global** is selected).
5. By default, the exception is set to **Block** the URL. To change this, set the **Type** to **Permit**.
6. Set an expiration date, if applicable.
7. Click **OK**, then **Save and Deploy**.

Define keywords

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

1. Navigate to **Policy Management > Filter Components** and click **Edit Categories**.
2. Select a category in the Categories tree. The right portion of the screen displays recategorized URLs and keywords currently associated with the category.
3. Under Keywords, click **Add Keywords**.

4. Enter one keyword per line. Click **Test** to verify that a keyword matches the intended strings.
5. When you are finished adding keywords, click **OK** to return to the Edit Categories page.
6. Click **OK** again to cache your changes. Changes are not implemented until you click **Save and Deploy**.

To block sites based on keywords, you must also:

- Make sure that keyword blocking is enabled globally. Go to **Settings > Filtering**, and then enable **Keyword search options** under General Filtering.
- Enable keyword blocking for the category in an active category filter.

Work with file types

1. Navigate to **Policy Management > Filter Components** and click **File Types**.
2. Select a file type from the list to view file extensions associated with the type, or click **Add File Type** to define a new file type.

   To add file extensions to an existing file type, click **Add Extensions**.

To block sites based on file type, enable file type blocking for individual categories in an active category filter.

Create Websense accounts for administrators

You can define local accounts used only for logging on to the TRITON Unified Security Center. Administrators can use these accounts, instead of their network directory accounts, to access TRITON - Web Security.

Local accounts are especially helpful in distributed environments, where delegated administrators may authenticate to different directory services. For more information, see *Allow administrators to log on using network accounts*, page 74.

To create local accounts:

1. Go to **TRITON Settings > Administrators**.
2. Click **Add Local Account**.
3. Enter a **User name**, contact **Email address**, and **Password** for the new account.

   The email address is used as part of an automated password recovery process.

4. Use the check boxes under the Confirm password field to indicate whether or not to **Notify administrator of the new account via email**, using the email address provided in the previous step, and whether to **Force administrator to create a new password at logon**.
5. Assign permissions to the account to access one or more TRITON modules.
   - **Global Security Administrators** have full, unlimited access to all TRITON modules, including TRITON Settings.
   - The **Custom** option allows you to assign either **access** privileges or **access and modify** privileges.
     - **Access** privileges let the administrator log on and see only a subset of the Status > Dashboard page until the account is assigned to a role as a delegated administrator or conditional Super Administrator.
     - **Access and modify** privileges grant the account unconditional Super Administrator permissions in the Web Security module.
6. Click **OK** to save your changes.

Any new account with Web Security permissions is added to the **Policy Management > Delegated Administration > View Administrator Accounts** page in TRITON - Web Security.

After adding an account with only access privileges, add that user to one or more delegated administration roles via the **Policy Management > Delegated Administration** page.

Allow administrators to log on using network accounts

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

If administrators are to access TRITON - Web Security by entering their network logon credentials, you must configure a directory service to use for authentication.

The directory service must be the one through which all administrators authenticate, or it must have a trusted relationship with their directory services.

Configure the directory service in TRITON Settings:

1. Go to **TRITON Settings > User Directory**.
2. Configure a connection to the supported directory service that you want to use to authenticate administrator logons.
3. Click **OK** to save your changes.

Move clients from one role to another

Moving a client from one delegated administration role to another requires unconditional Super Administrator permissions. You must first delete the client from the current role. Then, you can add that client to the new role.

Some clients cannot be deleted directly from the managed clients list (Delegated Administration > Edit Role). This occurs when the administrator has applied a policy to the client on the Clients page. It also occurs if the administrator has applied a policy to one or more members of the network, group, domain, or organizational unit to be moved.

In this situation, the unconditional Super Administrator should:

1. Go to the **Role** list in the toolbar, and select the role from which managed clients are to be deleted.
2. Go to **Policy Management > Clients** to see a list of all the clients to which the delegated administrator has explicitly applied a policy.

   This may include both clients that are specifically identified on the managed clients list for the role and clients who are members of networks, groups, domains, or organizational units on the managed clients list.
3. Delete from the Clients page any clients to be deleted from the role, and individual members of any networks, groups, domains, or organizational units to be deleted from the role.
4. Click **OK** to cache your changes, and then click **Save and Deploy** to implement the changes.
5. Go to the **Role** list in the toolbar, and select the **Super Administrator** role.
6. Go to **Policy Management > Delegated Administration** and click the role name from which the managed clients are to be deleted. The **Edit Role** page appears.
7. Delete the appropriate clients from the managed clients list.
8. Click **OK** to cache your changes.
9. On the Delegated Administration page, edit the new role for these clients and add them as managed clients.
10. Click **OK** to cache your changes. Changes are not implemented until you click **Save and Deploy**.

Delegated administrators can now move the new managed clients to their Clients page and assign policies to them.

Until a policy is assigned to the clients, they are managed by the role's Default policy.

Manage audit log settings

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

Super Administrators can view an audit trail of which administrators have accessed TRITON - Web Security and the changes they have made by clicking **Status > Audit Log**.

When the page opens, the most recent records appear. Use the scroll bar and the paging buttons above the log to view additional records.

Audit records are saved for 60 days, and then deleted from the log. Unlike previous releases, you do not have to configure any size or time limits for saving audit records.

Use the export option if you need to preserve the records for longer than 60 days. (Exporting does not remove records from the audit log.)

Configure hybrid Web filtering

Upgrading User Quick Start | Websense Web Security Solutions | v7.7

In Websense Web Security Gateway Anywhere deployments, before members of your organization can be filtered by the hybrid service, you must first activate hybrid filtering. Once your account is active, you can configure who is filtered by the hybrid service, identify any sites that should not be filtered, and determine how often user data is sent to the hybrid service.

The general steps are:

1. Go to the **Settings > Account** page and provide a **Contact email address** to activate your hybrid filtering account.
2. Use the **Settings > Hybrid Configuration > Filtered Locations** page to define the domains, IP addresses, and subnets to be filtered by the hybrid service. These are the IP addresses of the branch offices you want to protect.
3. Use the **Unfiltered Destinations** page to define any domains, IP addresses, and subnets that should **not** be filtered by the hybrid service. These include intranet sites not visible to the hybrid service, and external sites, like your organization's Web mail site, that you want users to be able to access even when hybrid filtering is not available.
4. Use the **User Access** page to define how users are identified and authenticated, which time zone to use in applying policies, and whether requests are permitted or blocked when the hybrid service is unable to apply policies.
5. Use the **Shared User Data** page to configure Websense Directory Agent to collect user and group data for the hybrid service.
6. Use the **Scheduling** page to determine how often directory data is sent to, and how often reporting data is retrieved from, the hybrid service.

Complete information about all of these configuration steps can be found in the TRITON - Web Security Help topic, “Configure Hybrid Filtering.”

Prevent data loss over the Web

Complete installation and configuration instructions for setting up data loss prevention over the Web can be found in the Deployment and Installation Center.

The general steps include:

1. Install the Content Gateway, Websense Web Security, and Websense Data Security modules of your Websense Web Security Gateway Anywhere product.
2. Register the Content Gateway Manager policy engine with the Data Security Management Server.
3. Configure the Content Gateway agent on the Data Security Management Server.
4. Log on to TRITON - Data Security and run the first-time policy wizard.
5. Still in TRITON - Data Security, enable linking to give Websense Data Security access to user names and Master Database categories provided by Websense Web Security.

For instructions on linking Websense Data and Web Security software, and on creating custom policies, refer to the TRITON - Data Security Help.