



Upgrading User Quick Start Tutorial

Websense® Web Security
Websense Web Filter

v7.6

©1996–2011, Websense Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA
Published 2011
Printed in the United States and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners. Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Sun, Solaris, UltraSPARC, Sun Java System, and all Sun Java System based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

eDirectory and Novell Directory Services are a registered trademarks of Novell, Inc., in the U.S and other countries.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries. Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (<http://www.apache.org>).
Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

| | | |
|----------------|--|-----------|
| Topic 1 | Welcome | 7 |
| | The TRITON™ Unified Security Center..... | 7 |
| | Term and concept reference..... | 10 |
| | Finding information within TRITON - Web Security..... | 11 |
| | Third-party product support..... | 12 |
| Topic 2 | What's New in Version 7? | 15 |
| | Monitor filtering status..... | 15 |
| | Review recent filtering activity..... | 16 |
| | Verify your Websense filtering setup..... | 17 |
| | Create reports within TRITON - Web Security..... | 17 |
| | Maintain centralized policy information..... | 18 |
| | Back up and restore policy information..... | 18 |
| | Allow concurrent administrator logons..... | 19 |
| | Identify conditional Super Administrators..... | 19 |
| | Create exceptions to user identification settings..... | 20 |
| | Integrate with Websense Web Security Gateway..... | 20 |
| Topic 3 | What's New in Version 7.1? | 21 |
| | Extended Health Alerts..... | 21 |
| | Safeguards for Save All..... | 22 |
| | Edit presentation reports..... | 22 |
| | New reports for Websense Web Security Gateway..... | 23 |
| Topic 4 | What's New in Version 7.5? | 25 |
| | Websense Web Security Gateway Anywhere..... | 25 |
| | Hybrid Web filtering..... | 26 |
| | Data loss prevention over the Web..... | 27 |
| | Introducing TRITON - Web Security..... | 27 |
| | Security overrides..... | 28 |
| | Improved presentation report generation..... | 28 |
| | Enhanced history page summary..... | 29 |
| | New settings for Websense Web Security Gateway..... | 29 |
| | New reports for Websense Web Security Gateway..... | 30 |

| | | |
|----------------|---|-----------|
| Topic 5 | What's New In Version 7.6? | 33 |
| | Enhanced TRITON Unified Security Center | 33 |
| | Introducing Real-Time Monitor | 34 |
| | New Log Database platforms | 35 |
| | More Today and History page details | 35 |
| | Delegated administration and reporting | 36 |
| | New DC Agent health alerts. | 38 |
| | Block pages | 38 |
| | Filtering based on Security Risk status | 39 |
| | Monitoring Web Security status. | 39 |
| | Remote Filtering Client 64-bit support. | 40 |
| | Policy Server key management | 40 |
| | User Service caching | 40 |
| | IPv6 filtering. | 41 |
| | Usage alert editing | 41 |
| | Internationalized domain name (IDN) support. | 41 |
| | Content Gateway access and alerting. | 42 |
| Topic 6 | Where Do I Find...? | 43 |
| | My Global policy | 43 |
| | My Default Settings category and protocol sets. | 44 |
| | My yes lists. | 44 |
| | My custom URLs | 44 |
| | My directory objects. | 45 |
| | Websense Explorer. | 45 |
| | Websense Reporter. | 45 |
| | My reports | 45 |
| | Real-Time Analyzer | 48 |
| | My server settings. | 48 |
| | My Network Agent local settings. | 48 |
| | Administrator account management. | 48 |
| | The Network Traffic Detector (Traffic Visibility Tool). | 49 |
| | Subscription key management | 49 |
| Topic 7 | How Do I...? | 51 |
| | Download the Master Database | 51 |
| | Add clients | 52 |
| | Create a policy | 52 |
| | Assign a policy to clients | 53 |

Verify that the correct policy is applied53

Generate a presentation report53

Generate an investigative report54

Create or edit a custom category55

Recategorize a URL55

Create an unfiltered URL56

Define keywords56

Work with file types56

Create Websense accounts for administrators57

Allow administrators to log on using network accounts58

Move clients from one role to another58

Manage audit log settings59

Configure hybrid Web filtering59

Prevent data loss over the Web60

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?](#)
- ◆ [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 7, 8, or 9 or Mozilla Firefox 3.x or 4) and enter the following URL:

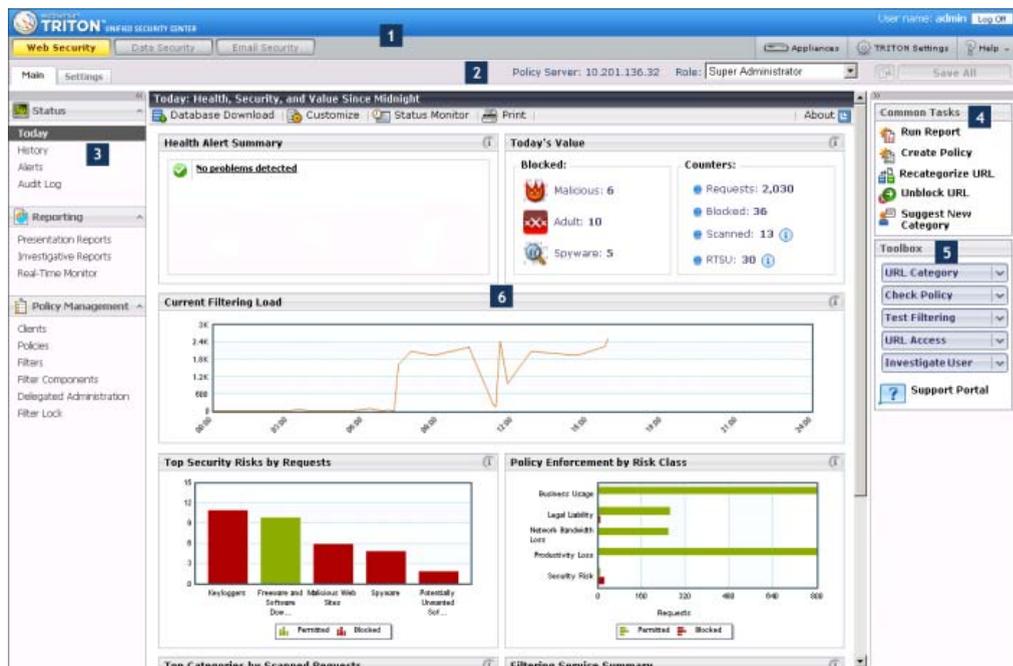
```
https://<IP address or host name>:9443/triton/
```

Replace <IP address or host name> 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 > Today page after logon. (The administrator may be prompted to enter a subscription key or launch a quick start tutorial before the Today page appears.)

The Status > Today page provides an overview of the current status of your Websense Web Security software. Boxes at the top of the screen show whether any errors or warnings have been generated by Websense components, and provide a quick overview of Internet request totals and key block totals. If Log Server is installed, additional charts provide a graphical overview of today's filtering behavior. See [Monitor filtering status, page 15](#).

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 17](#).



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 current 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 All** 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 17](#).
- 6 Each time you open TRITON - Web Security, the **Status > Today** page provides an overview of the current status of your Websense software. Boxes at the top of the screen show whether any errors or warnings have been generated by Websense components, and provide a quick overview of Internet request totals and key block totals. If Log Server is installed, additional charts provide a graphical overview of today's filtering behavior. See [Monitor filtering status, page 15](#).

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 7.6.

| Original Term | New Term |
|---|--|
| Always Block (category set) | Block All (category filter) |
| category set | category filter |
| continue (filtering option) | confirm (filtering action) |
| Custom URLs (Not Filtered) | unfiltered URLs |
| 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 | <ul style="list-style-type: none"> • Policies • Filters (category filters, protocol filters, and limited access filters) • Filter Components (categories, protocols, custom URLs, keywords, and file types) |
| filtering option | action <i>or</i> filtering action |
| *Global policy | Default policy |
| hits (used in reporting) | hits, <i>also</i> requests (generic term for hits and visits) |
| Network Traffic Detector (<i>also</i> , Traffic Visibility Tool) | [discontinued] |
| Never Block (category set) | Permit All (category filter) |
| pattern | regular expression |
| protocol set | protocol filter |
| Real-Time Analyzer | [discontinued], <i>replaced by</i> Real-Time Monitor |

| Original Term | New Term |
|---|--|
| Remote Administrator | conditional Super Administrator (Some administrator permissions have changed. See <i>Delegated administration and reporting</i> , page 36.) |
| Save Changes | Save All |
| Super Administrator | unconditional Super Administrator (Web Security access only), <i>also</i> Global Security Administrator (access to all TRITON modules) |
| Traffic Visibility Tool (<i>also</i> , Network Traffic Detector) | [discontinued] |
| URL pattern | regular expression |
| visits | visits, <i>also</i> 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], <i>replaced by</i> 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 6 types of Help:

- 1 Most pages include a brief, expandable and collapsible overview. Initially, these About boxes are collapsed for all administrators. Super Administrators can change this behavior so that the boxes are opened by default for all administrators.
 - If this page overview box is hidden, click  in the toolbar to show it.
 - To hide an About box, click .

The About button is not available on the Settings pages. Brief overview information appears at the top of each Settings page, and cannot be hidden.
- 2 An  icon accompanies many important product features. Position your mouse over this icon for a brief explanation of the feature.
- 3 For complex or advanced tasks, help text appears directly on the page, providing usage guidelines or other pointers for using a tool or field.

| | |
|---|--|
| 4 | 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 . |
| 5 | 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.) |
| 6 | 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 Websense Web Security installation and deployment materials. This section provides brief information about recently added product and platform support.

Browser support

In version 7.6, the TRITON Unified Security Center (including all reporting tools) can be accessed using the following supported browsers:

- ◆ Microsoft Internet Explorer versions 7, 8, and 9
- ◆ Mozilla Firefox versions 3.x and 4

When accessing the TRITON console from a Linux machine, use Firefox 3.5.x or later for best results.

Windows Active Directory 2008

Websense Web Security support for Active Directory 2008 allows you to:

- ◆ Add users, groups, and domains (OU) defined in Active Directory 2008 as clients in TRITON - Web Security.
- ◆ Use supported transparent identification agents (DC Agent and Logon Agent) to identify these directory clients without prompting them for logon information.
- ◆ Use manual authentication to ensure that these users provide correct logon information before accessing the Internet.

- ◆ Allow administrators to access TRITON using their network logon accounts. This requires configuring administrator access on the TRITON Settings > User Directory page and the Settings > General > Logon Directory page



Important

If you are using Active Directory (Mixed Mode), or if you are using a Websense transparent identification agent with Active Directory (Native Mode), you **must** turn on the Windows Computer Browser service on the machine running Active Directory 2008 to enable communication with Websense software.

1. Go to **Administrative Tools > Services**.
2. Double-click the **Computer Browser** service to open the Properties dialog box
3. Set the **Startup Type** to **Automatic**.
4. Click **Start**.
5. Click **OK** to save and apply the change.

Other supported products and platforms

This release adds support for the following operating systems:

- ◆ Microsoft Windows Server 2008 (32-bit)
Components can be installed and run on a machine running Windows Server 2008, 32-bit version. It may be necessary to turn on the Windows Computer Browser service to support communication with the directory service.
- ◆ Microsoft Windows Server 2008 (64-bit)
This is the preferred platform for the TRITON Unified Security Center. Standalone installations of TRITON - Web Security are still supported on Windows 2003 Server platforms, but to add TRITON modules, the management server must be a Windows 2008 R2 64-bit system.

In this release, Filtering Service adds the ability to integrate with the following products:

- ◆ Citrix XenServer 5 (32-bit mode)
- ◆ Microsoft Forefront TMG (ISA Server 2008)

The Log Database can now be hosted by:

- ◆ Microsoft SQL Server 2005 Standard and Enterprise (32- and 64-bit)
- ◆ Microsoft SQL Server 2008 and R2 Standard and Enterprise (32- and 64-bit, but not IA64)
- ◆ Microsoft SQL Server 2008 R2 Express. This replaces support for MSDE. See your installation and deployment materials for details.

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 10](#)

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

- ◆ [Monitor filtering status, page 15](#)
- ◆ [Review recent filtering activity, page 16](#)
- ◆ [Verify your Websense filtering setup, page 17](#)
- ◆ [Create reports within TRITON - Web Security, page 17](#)
- ◆ [Maintain centralized policy information, page 18](#)
- ◆ [Back up and restore policy information, page 18](#)
- ◆ [Allow concurrent administrator logons, page 19](#)
- ◆ [Identify conditional Super Administrators, page 19](#)
- ◆ [Create exceptions to user identification settings, page 20](#)
- ◆ [Integrate with Websense Web Security Gateway, page 20](#)

For late-breaking news about what has changed in this version, see the [Release Notes](#), available from the [Websense Technical Library](#).

Monitor filtering status

When you open TRITON - Web Security, the **Status > Today** page gives an overview of Websense software status and Internet usage and filtering since midnight. At the top of the page:

- ◆ The **Health Summary** list alerts you to system status issues. Click a message to see more detailed messages, and links to possible solutions.

- ◆ The **Today's Value** area highlights how Websense filtering is protecting your network from categories commonly considered high risk.

At the bottom of the page, the **Filtering Service Summary** lists the IP address and current status of each instance of Websense Filtering Service associated with the current Policy Server.

Health Summary, Today's Value, and Filtering Service information is visible to all administrators (Super Administrators and delegated administrators) logging on to TRITON - Web Security.

Up to 4 additional charts can be displayed on the page, showing information about Internet usage and filtering activity. The default administrator account (**admin**) and other members of the Super Administrator role with reporting permissions can view these charts, but they may not be visible to all delegated administrators.

- ◆ Click any chart to open an investigative report showing related data.
- ◆ Anyone with unconditional Super Administrator permissions can change which charts appear on the Today page by clicking **Customize** in the toolbar at the top of the page.

Review recent filtering activity

Use the **Status > History** page (accessed by clicking **History** under Status on the Main tab of the left navigation pane) to review filtering activity for the recent past. Depending on your reporting setup, this page may show activity for up to the past 30 days.

At the top of the page, the **Value Estimates** area provides an estimate of time and bandwidth saved due to blocked Internet requests. It also shows the number of sites blocked in categories that are of particular concern to Websense software users.

Up to 4 additional charts can be displayed on the page, showing information about Internet usage and filtering activity. If your organization uses delegated administration, the charts are visible only to administrators that have reporting permissions.

- ◆ Click any chart to open an investigative report showing related data.
- ◆ Anyone with unconditional Super Administrator permissions can change which charts appear on the History page by clicking **Customize** in the toolbar at the top of the page.

Verify your Websense filtering setup

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 a user name or IP address, and then click Go . An investigative report showing the client's usage history is displayed. |

Create reports within TRITON - Web Security

All Websense Web Security reporting tools have been integrated into the TRITON console. Like the charts on the Today and History pages, 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 34.)

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

- ◆ Run a report from the list of predefined report templates.
- ◆ Use the Save As button to copy a report template, and then edit the report filter for the custom 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 for Windows. 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

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 available to 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

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

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** 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*)
- ◆ Basic monitor access (Status > Today, History, and Alerts pages only)

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

Identify conditional Super Administrators

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.
- ◆ 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

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 filtering to the next level, where, depending on your configuration, you can enable scanning to analyze online files and Web site content when they are requested. When activated, scanning occurs only for sites not blocked by Websense Web Security.

The available scanning options depend on your subscription, and may include both content categorization and security real-time scanning.

- ◆ Use **content categorization** to review the content of sites that are not blocked (based on the site's Master Database category and the active policy), and return a category for use in filtering.
- ◆ Also take advantage of up to 3 security real-time options (based on your subscription):
 - **Content scanning** looks at Web content to find security threats such as phishing, URL redirection, Web exploits, and proxy avoidance.
 - **File scanning** inspects file content to determine a threat category, such as viruses, Trojan horses, or worms.
 - **Content stripping** removes active content from requested Web pages.

3

What's New in Version 7.1?

Version 7.1 introduces:

- ◆ New Health Alert messages on the Status > Today page (see [Extended Health Alerts](#), page 21)
- ◆ Enhanced **Save All** functionality (see [Safeguards for Save All](#), page 22)
- ◆ Simplified process for creating and editing custom presentation reports (see [Edit presentation reports](#), page 22)
- ◆ New Status > Today and History charts for Websense Security Gateway (see [New reports for Websense Web Security Gateway](#), page 23)
- ◆ New presentation reports for Websense Security Gateway (see [New reports for Websense Web Security Gateway](#), page 23)

Extended Health Alerts

To help you monitor the status of your Websense software deployment, new Health Alert messages on the Status > Today page provide errors or warnings 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 ApacheTomcatWebsense service cannot connect to Log Server.

When this occurs, presentation report jobs being scheduled are not saved properly, and are lost when the ApacheTomcatWebsense service is restarted. In addition, reports on the Status > Today and History pages, 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 All

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

The Save All 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

Using presentation reports has been simplified. To help clarify which reports can be edited, and which are fixed, predefined reports are now called *report templates*, and are marked with a template icon. Like before, you can generate a report from the report template 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 report template 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 custom icon. Select any custom report and click **Edit** to modify the report filter.

New reports for Websense Web Security Gateway

New reports provide additional insight into how the Websense Web Security Gateway the impact and value of the scanning features.

The Value Estimates area on the Status > Today page now includes information about the number of sites that were filtered differently as a result of scanning. Additionally, by default, the Today and History pages include charts of scanning activity. If you have upgraded from version 7.0.x, and previously customized the charts displayed on the page, your custom settings are preserved.

You can customize the page again after upgrading to view the new charts.

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 scanned 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 scanned 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 scanning. 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 scanned 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:

- ◆ *Websense Web Security Gateway Anywhere*
 - *Hybrid Web filtering*
 - *Data loss prevention over the Web*
- ◆ *Introducing TRITON - Web Security*
- ◆ *Security overrides*
- ◆ *Improved presentation report generation*
- ◆ *Enhanced history page summary*
- ◆ *New settings for Websense Web Security Gateway*
- ◆ *New reports for Websense Web Security Gateway*

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 categorize content, analyze sites and files to find malicious content, and 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 filtering

Web Security Gateway Anywhere offers an alternative to pure service, software, or appliance-based Web filtering 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 filtering 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 filter off-site users, you now have the option to use the hybrid service, as well.

Hybrid filtering 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 **Status > History** page can be displayed to provide an overview of Internet activity by the members of your organization filtered by the hybrid service.

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

You can generate 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

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 and Websense Web Security, install Websense Data Security, and 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

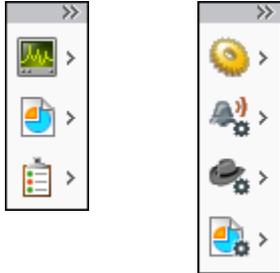
As the Websense data, email, and Web security solutions continue to interoperate more closely, the TRITON Unified Security Center provides a centralized approach to managing Websense software.

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 global TRITON toolbar (just under the Websense banner; moved in v7.6). The Select Policy Server and Save All 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, a narrow icon bar 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

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 39.

Improved presentation report generation

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 immediately.

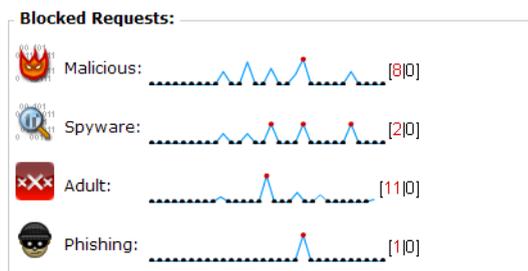
- ◆ Run the report in the foreground to generate the report in a new window without scheduling it.

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

The **Blocked Requests** section of the Status > History page 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 chart to open an investigative report 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

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 > History page charts and presentation reports provide information about Web 2.0 sites requested by users in your organization and scanned by Websense Web Security Gateway.

On the History page, you now have the option to display following 2 new charts. Use the Customize button at the top of the page to change which charts appear.

| Chart Name | Description |
|--------------------------------------|---|
| Top 5 Web 2.0 Categories by Requests | Shows the top 5 most frequently requested categories within the set of Web 2.0 sites. Use this information to learn more about Internet usage patterns and to discover potential productivity issues. |
| Top 5 Web 2.0 Sites by Bandwidth | Shows the top 5 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*
- ◆ *Introducing Real-Time Monitor*
- ◆ *New Log Database platforms*
- ◆ *More Today and History page details*
- ◆ *Delegated administration and reporting*
- ◆ *New DC Agent health alerts*
- ◆ *Block pages*
- ◆ *Filtering based on Security Risk status*
- ◆ *Monitoring Web Security status*
- ◆ *Remote Filtering Client 64-bit support*
- ◆ *Policy Server key management*
- ◆ *User Service caching*
- ◆ *IPv6 filtering*
- ◆ *Usage alert editing*
- ◆ *Internationalized domain name (IDN) support*
- ◆ *Content Gateway access and alerting*

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 administration Web Security, Data Security, and Email Security, 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 64-bit 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 still be installed on a Windows Server 2003 machine. TRITON modules are no longer supported on Linux platforms, however.

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**.

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

- ◆ Microsoft Internet Explorer 7, 8, and 9
- ◆ Firefox 3 or higher

Introducing Real-Time Monitor

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 from the TRITON - Web Security Help.

New Log Database platforms

Version 7.6 introduces support for Microsoft SQL Server Express 2008 R2. The Log Database can now also be hosted by:

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

Support for MSDE has been discontinued.

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.

More Today and History page details

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

On the Today page, the affected counters are:

- ◆ Malicious
- ◆ Spyware
- ◆ Adult
- ◆ Requests

- Blocked
- Scanned
- Real-Time Security Updates

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

Delegated administration and reporting

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.

In environments that allow delegated administrators to use their network accounts to access the TRITON console, directory service communication is now done in 2 places: TRITON Settings and the Settings > General > Logon Directory page.

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

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

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

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

Block page in small screen areas

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

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

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

Account override

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

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

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

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

Filtering based on Security Risk status

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

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

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

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

Remote Filtering Client 64-bit support

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

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

In additions, an updated Remote Filtering Client configuration utility 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

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

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

To improve performance, clearing the User Service cache is no longer performed as part of every Save All action. Instead, the cache is cleared at save time only 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

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

Usage alert editing

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

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

Internationalized domain name (IDN) support

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

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

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



Important

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

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

In addition:

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

The page displays the status (running or stopped), IP address and host name, cluster name, and description for each Content Gateway instance that has registered with the selected Policy Server.

- ◆ Important Content Gateway health alerts are displayed in TRITON - Web Security.

As with other health alerts, a short alert is shown on the Status > Today page, with a longer message appearing on the Alerts page.

- ◆ Use the Settings > Alerts > System page to configure both Web Security and Content Gateway system alerts.

As with existing Web Security alerts, you can configure which Content Gateway conditions cause alert messages to be sent, and which methods (email, pop-up, or SNMP) are used to send the alert.

6

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](#), page 43
- ◆ [My Default Settings category and protocol sets](#), page 44
- ◆ [My yes lists](#), page 44
- ◆ [My custom URLs](#), page 44
- ◆ [My directory objects](#), page 45
- ◆ [Websense Explorer](#), page 45
- ◆ [Websense Reporter](#), page 45
- ◆ [My reports](#), page 45
- ◆ [Real-Time Analyzer](#), page 48
- ◆ [My server settings](#), page 48
- ◆ [My Network Agent local settings](#), page 48
- ◆ [Administrator account management](#), page 48
- ◆ [The Network Traffic Detector \(Traffic Visibility Tool\)](#), page 49
- ◆ [Subscription key management](#), page 49

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, you are not prompted to provide complete coverage. When you edit the Default policy, however, you will not be permitted to save changes until all gaps are filled.

My Default Settings category and protocol sets

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 yes lists

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

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.

To view and edit **unfiltered URLs** (formerly Custom URLs/Not Filtered), go to **Policy Management > Filter Components** and click **Unfiltered URLs**. Existing URLs, IP addresses, and regular expressions currently defined as unfiltered URLs appear in the Permitted Sites list.

My directory objects

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

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

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.

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 for the copy 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) |
| 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) |

| v6.3.x Report | v7 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

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 34.
- ◆ Graphical charts on the **Status > Today** page provide an overview of filtering volume, summaries of filtering activity, and filtered request statistics. Also use the Today page to 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.
- ◆ Graphical charts on the **Status > History** page display filtering summary information for a longer time period (up to 30 days).

My server settings

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

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

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 > Today 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)

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

Policy Server subscription key management has moved from the Settings > General > Account page to the **Settings > General > Policy Servers** page. Once a key has been entered, information about the corresponding subscription is displayed on the Account page.

The Policy Servers page is now the primary management interface for subscription keys, allowing you to enter keys for each Policy Server instance in your network, regardless of which instance TRITON - Web Security is currently connected to. You can also establish hierarchical relationships between Policy Server instances that share a key to ensure that if the key changes, all affected Policy Server instance receive the update.

7

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 the new TRITON - Web Security.

- ◆ [Download the Master Database, page 51](#)
- ◆ [Add clients, page 52](#)
- ◆ [Create a policy, page 52](#)
- ◆ [Assign a policy to clients, page 53](#)
- ◆ [Verify that the correct policy is applied, page 53](#)
- ◆ [Generate a presentation report, page 53](#)
- ◆ [Generate an investigative report, page 54](#)
- ◆ [Create or edit a custom category, page 55](#)
- ◆ [Recategorize a URL, page 55](#)
- ◆ [Create an unfiltered URL, page 56](#)
- ◆ [Define keywords, page 56](#)
- ◆ [Work with file types, page 56](#)
- ◆ [Create Websense accounts for administrators, page 57](#)
- ◆ [Allow administrators to log on using network accounts, page 58](#)
- ◆ [Move clients from one role to another, page 58](#)
- ◆ [Manage audit log settings, page 59](#)
- ◆ [Configure hybrid Web filtering, page 59](#)
- ◆ [Prevent data loss over the Web, page 60](#)

Download the Master Database

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 > Today** page in TRITON - Web Security.

1. Click **Database Download** in the toolbar at the top of the Today page.
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 to view the progress of the download, or click **Close** to return to the Today page.

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 > Database Download** page.

Add clients

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 All**.

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 All**.

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 All** in the right shortcut pane to save and implement your changes.

Verify that the correct policy is applied

1. In TRITON - Web Security, 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

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 determine how the report will be 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 to generate a detail report of the data for the selected bar.

- ◆ 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 within the selected parent category, click **Add**. You must select a parent category to enable the Add Category function.
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

1. In TRITON - Web Security, 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 All**.

Create an unfiltered URL

1. In TRITON - Web Security, do either of the following:
 - Click **Unblock URL** in the right shortcut pane.
 - Go to **Policy Management > Filter Components**, and then click **Unfiltered URLs**.
2. Under **Enter one URL or IP address per line**, list the URLs or IP addresses of sites that you want to define as unfiltered URLs, and then click the right arrow (>) button to move them to the Permitted sites list.
3. Select a **Category** for each URL in the Permitted sites list.
4. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Define keywords

1. In TRITON - Web Security, go 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 All**.

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. In TRITON - Web Security, go 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 58.

To create local accounts:

1. Go to **TRITON Settings > Administrators**.
2. Click **Add Local Account** in the toolbar at the top of the content pane.
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 > Today 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 the local account has been added, if it has only access privileges, add that user to one or more delegated administration roles via the **Policy Management > Delegated Administration** page in TRITON - Web Security.

Allow administrators to log on using network accounts

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

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

Currently, the directory service used to validate administrator logons is configured in 2 places.

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.
4. Open the Web Security module and go to **Settings > General > Logon Directory**.
5. Make sure that **Use a directory service for administrator authentication** is selected, and then:
 - If you want to use the same directory service information that appears on the Settings > Directory Services page, click **Get Settings**.
 - Otherwise, configure a connection to the directory service that authenticates administrators, or has a trusted relationship with those directory services.
6. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

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 All** 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 All**.

Manage audit log settings

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

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," or see the *Websense Web Security Gateway Anywhere Getting Started Guide*.

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 *Websense Web Security Gateway Anywhere Getting Started Guide*.

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.