v7.7 Release Notes for Websense® Web Security

Topic 50230 | Release Notes | Web Security Solutions | Version 7.7 | Updated 02-Jul-2012

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7

Use the Release Notes to find information about what's new and improved in Websense Web Security Version 7.7.

New in Websense Web Security v7.7

Topic 50231 | Release Notes | Web Security Solutions | Version 7.7 | Updated 02-Jul-2012

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7

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

Enhanced Web Security Dashboard

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

When you log on to TRITON - Web Security, the Threats dashboard is displayed, showing information about suspicious activity in your network (see *Tools to fight advanced persistent threats*, page 3).

The dashboard includes 3 additional tabs:

- **Risks** shows information about blocked and permitted requests for URLs that fall into the Security Risk class. The amount of information depends on your

subscription level. Web Security, Web Security Gateway, or Web Security Gateway Anywhere is required to see information about requests in some security-specific categories.

- **Usage** shows information about traffic patterns in your network, including bandwidth information and filtering summaries.
- **System** shows alert messages, status information, and graphical charts that show the current state of your Web Security solution, focusing on component health and Internet activity in your network.

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

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

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

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

Tools to fight advanced persistent threats

Use the **Threats** tab of the Web Security Dashboard to monitor and investigate suspicious activity in your network that could indicate advanced malware attacks.

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

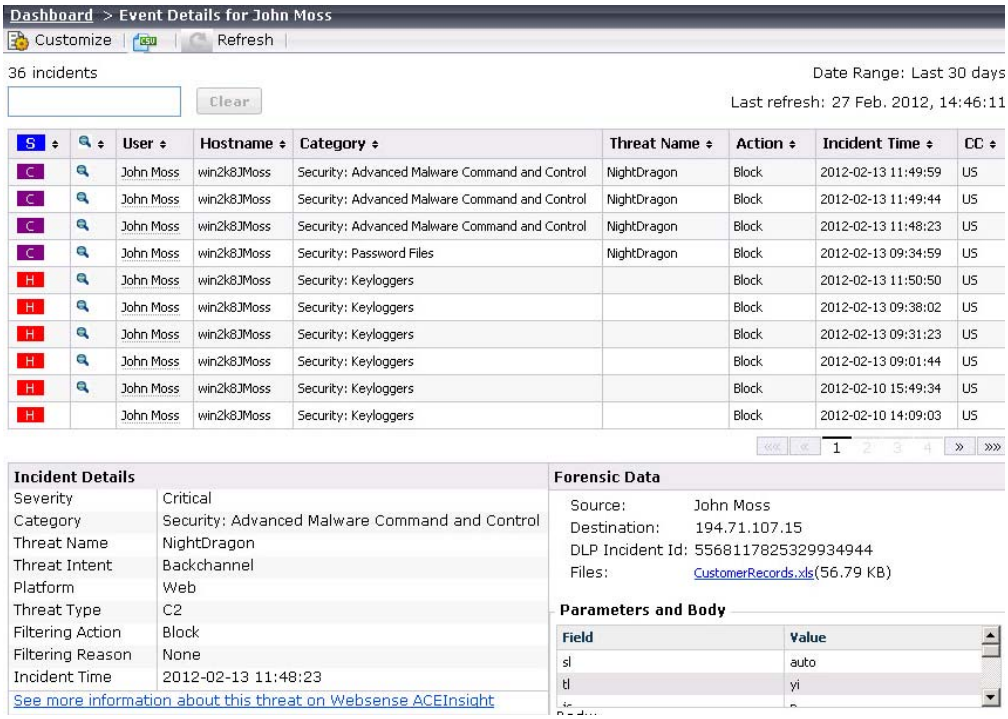
The initial Threats dashboard has 3 main elements:

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

Controls at the top of the tab let you restrict the information displayed to specific severity types (Critical, High, Medium, or Low), directions (inbound or outbound), and time periods (today, 2 days, 7 days, and so on).

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

Click a user name, IP address, or host name in the summary table to see a detail page with information about all incidents associated with the selected client, including the forensics data (if any) collected. The detail page also includes a link to ACEInsight that administrators can use to perform further research on the threats associated with the incident.



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

Severity-based alerting on suspicious Internet activity

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

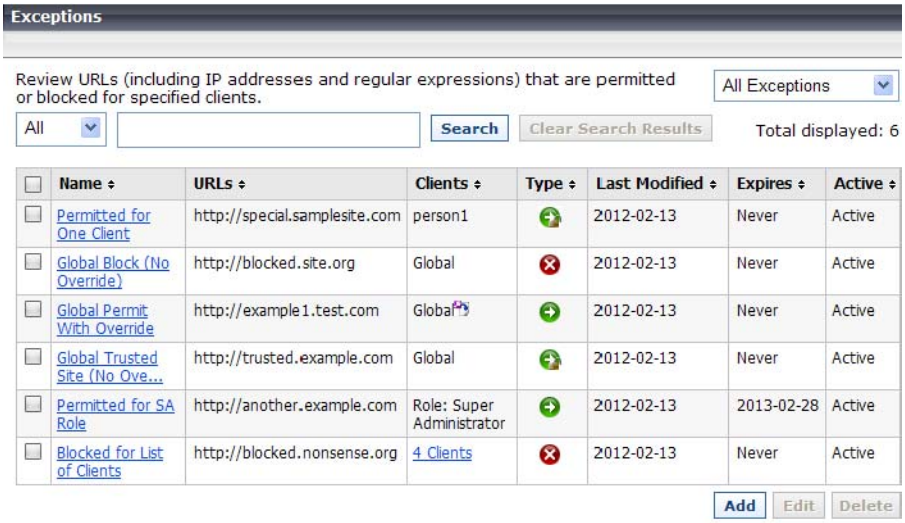
- Define alerts for permitted requests and blocked requests at each severity level.
- Each alert message includes a link to the Dashboard > Threats > Event Details page that you can use to investigate the associated incidents.

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

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

Exceptions: URL black and white lists

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



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

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

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

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

Exceptions can be created for:

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

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

- All clients in a delegated administration role

Enhanced presentation reporting

Presentation reporting has been enhanced to offer:

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

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

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

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

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

Browse time available in investigative detail reports

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

Although **Browse Time** always appears as an available column when you are creating or modifying v7.7 investigative detail reports, you must enable the detailed browse time calculation for data to be available.

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

Create a new database partition when you enable or disable detailed browse time calculations.

Enhanced file type blocking

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

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

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

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

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

Extended information on block pages

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

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

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

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

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

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

Centralized Log Server configuration

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

Use this page to:

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

Note

The enhanced logging feature, used to control how Log Server resumes logging after it has been stopped, can now be configured only via the **logserver.ini** file.

By default, this option is disabled, and Log Server begins processing at the beginning of the oldest log cache file after a stop. This can result in some duplicate entries in the Log Database, but speeds Log Server processing.

WebCatcher configuration is now performed on the **Settings** > **General** > **Accounts** page. In addition, WebCatcher now uses the proxy server settings configured on the **Settings** > **General** > **Database Download** page when sending data.

Enhanced Log Database configuration

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

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

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

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

  Enabling detailed browse time calculations increases Log Database size.

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

  Enabling trend data storage increases Log Database size.

Extended support for non-standard SQL Server ports

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

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

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

Support for SQL Server SSL encryption

If your Microsoft SQL Server installation is configured to use SSL encryption, you can configure Websense components to encrypt their connection to the Log Database via the:

- TRITON Unified Installer (select **Encrypt connection**)
- Web Security module installer (select **Use SSL to connect to the Log Database**)

- **Settings** > **Reporting** > **Log Server** page in TRITON - Web Security (select **Use SSL to connect to the Log Database**)

> **Important**
> Configure encryption in Microsoft SQL Server before enabling this feature in either the installer or the TRITON console. See the Deployment and Installation Center for more information.

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

Note that when SSL encryption is enabled:

- BCP cannot be used to add records to the Log Database.
- Log Database connections are slower, affecting reporting performance.
- If you are running TRITON - Web Security on a Websense appliance, the connection from the console to the database cannot be encrypted. This means that if the Microsoft SQL Server **Force Protocol Encryption** option is set to **Yes**, no data appears in the Web Security Dashboard or other reporting tools.

Enhanced DC Agent configuration

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

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

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

As in previous versions, these settings can also be configured manually in the **transid.ini** file for each DC Agent instance.

New transparent identification and logging health alerts

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

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

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

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

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

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

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

  The ETL (Extract, Transform, and Load) job is responsible for processing data into the partition database. It requires sufficient disk space, disk speed, and other system resources to run efficiently.
- There are multiple Log Server instances associated with the same Policy Server.

  While it is possible to include multiple Log Server instances in a deployment, there can be only one Log Server instance associated with each Policy Server. Attempting to connect multiple Log Server instances to the same Policy Server can interfere with reporting.

Enable time-based (stateful) filtering in deployments with multiple Filtering Service instances

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

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

State Server is typically installed on a Policy Server machine, and only one State Server instance is required per **logical deployment**. A logical deployment is any

group of Policy Server and Filtering Service instances that might handle requests from the same set of users.

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

To install or enable State Server for a logical deployment:

- In software deployments, use the Custom installation option to install Websense State Server.
- On Websense appliances, use the **Administration > Toolbox > Command Line Utility** to enable **state-service**.

Filtering Service support for YouTube in Schools

Educational institutions with a software deployment of Websense Web Security or Web Filter can use a Filtering Service configuration parameter to enable YouTube for Schools. This YouTube service provides access to educational videos from inside the school network, even when other YouTube content is blocked.

> **Note**
> In Web Security Gateway and Gateway Anywhere software or appliance deployments, you can enable YouTube for Schools via Content Gateway, rather than via Filtering Service.

Once you have enrolled in the program and received a school account code or ID, the general steps are:

1. In TRITON - Web Security, navigate to the Settings > General > Filtering page, and verify that **Enable search filtering** is selected at the bottom of the page.

   You must enable search filtering to use the YouTube in Schools feature.
2. Make sure that the YouTube is permitted for the clients that will be granted YouTube in Schools access.
3. Edit the **eimserver.ini** file for each Filtering Service instance in your network to include the following lines:

   ```
   [SafeSearchCustomValues]
   YouTubeEDUFilter=<school_account_code>
   ```

   Note that after making this change, you must restart Filtering Service.

Network Agent support for 802.1Q VLAN tags

In this version, Network Agent can capture and filter traffic encapsulated with 802.1Q VLAN protocols.

- A single Network Agent instance can support VLAN and non-VLAN protocols simultaneously.
- Network Agent can record and replay VLAN protocol traffic.

If you plan to make use of this feature, keep in mind the following deployment considerations:

- Only 802.1Q VLAN tagging is supported in this release.
- The monitor NIC (the network card used to monitor Internet activity) connects to the switch port with a 802.1Q protocol header.
- The blocking NIC (used to send block pages or block messages) does not need to include the 802.1Q protocol header. As a result, it cannot be connected directly to access ports.

Integration with third-party SIEM solutions

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

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

- In software deployments, use the Custom installation option to install Websense Multiplexer on each Policy Server machine.
- On Websense appliances, use the **Administration > Toolbox > Command Line Utility** to enable **mux-service** on the full policy source and each user directory and filtering machine.

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

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

IPv6 client and URL filtering

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

deployments. This includes both URL filtering (IPv6 addresses categorized in the Master Database or defined in an exception) and filtering of IPv6 clients (computers and networks).

- Network Agent (standalone mode) or Content Gateway (Websense Web Security Gateway or Gateway Anywhere) is required to enable IPv6 filtering.
- The hybrid service does not support IPv6 filtering.

No special configuration is required to enable this functionality.

In this release:

- Source and destination IPv6 addresses are not recorded in the Log Database, with one exception. If no user name information is available for an IPv6 client, the IPv6 address is recorded in the user name field. As a result, dashboard charts, investigative reports, and presentation reports include only limited IPv6 address information.
- DC Agent, eDirectory Agent, and RADIUS Agent do not support IPv6 addresses. (Logon Agent, however, **does** support IPv6.)

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

The machines hosting Websense Web Security components, and any network infrastructure (like DNS servers and domain controllers) that Websense components use, must have an IPv4 address.

Super Administrator direct access to Content Gateway Manager

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

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

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

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

Enhanced Directory Agent configuration and performance

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

> **Note**
>
> In version 7.7, Websense Directory Agent is installed but not enabled on Websense appliances.
>
> To enable Directory Agent, go to the **Administration > Toolbox > Command Line Utility** in Appliance Manager and enable **directory-agent-service**.

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

This helps administrators to more easily:

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

In addition, a limitation that prevented Directory Agent from processing more than 1500 attribute values for an LDAP record has been removed. Directory Agent can now process LDAP records with any number of attribute values.

Hybrid user agent reporting and custom authentication

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

- User agents that have requested authentication.

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

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

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

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

On-premises failover to the hybrid service

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

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

Other hybrid Web Security enhancements

- The **Settings > Hybrid Configuration > Filtered Locations** page has been enhanced to more clearly distinguish between locations filtered by on-premises components and locations filtered by the hybrid service.
- The **Settings > Hybrid Configuration > Hybrid User Identification** page now includes the option to create or change the Web Endpoint anti-tampering password. There is still an option to create the password in the Unified Endpoint Package Builder when a Web Endpoint installation package is being configured.
- The **Settings > Hybrid Configuration > Hybrid User Identification** page now includes an additional method for user identification and authentication. In addition to NTLM and basic authentication, secure form authentication can be used.
- For sites that want to use the default PAC file, but have port 8082 or 8081 locked down, the Proxy Auto-Configuration File section of the **Settings > Hybrid Configuration > User Access** page now offers 2 options:
  - The default PAC file URL, retrieved over port 8082 (also requires port 8081)
  - An alternate PAC file URL, retrieved over port 80
- The hybrid service now supports SSL decryption bypass settings for IP address and range for both clients and destinations as defined on the **Settings >**

Scanning > SSL Decryption Bypass page in TRITON - Web Security. There are 3 exceptions:

- Bypass specifications for IPv6 addresses and ranges are not supported. Sync Service does not pass these addresses and ranges to the hybrid service.
- Bypass specifications for client machine private IP addresses are not supported. Sync Service does send these IP addresses, but they are disregarded by the hybrid service.
- Bypass specifications for client machine hostnames are not supported. Sync Service does not pass these hostnames to the hybrid service.

- The **Session Timeout** period configured on the Settings > Hybrid Configuration > User Identification page in TRITON - Web Security determines how long user credentials are assumed valid by Websense Authentication Service and secure form authentication.

  Organizations that require a longer timeout period can now request the option to extend the timeout period beyond its current maximum (30 days). When enabled, this allows the timeout period to be extended to 3, 6, or 12 months.

Removed in this version

This version ends support for:

- Integration with Microsoft ISA Server (Microsoft Forefront TMG is still supported.)
- Integration with Squid Web proxy cache
- Integration with Citrix Presentation Server (XenApp is still supported.)
- Microsoft Windows 2003 and 2003 R2
- Red Hat Enterprise Linux version 4.x
- Microsoft Internet Explorer version 7
- Mozilla Firefox version 3

Installation and upgrade

Topic 50232 | Release Notes | Web Security Solutions | Version 7.7 | Updated 02-Jul-2012

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7

Requirements overview

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

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

The following components run on Windows platforms only:

- TRITON Unified Security Center

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

Websense Content Gateway is a Linux-only component.

In appliance-based deployments, in addition to the Windows-only components, the following components, when used, must be installed off-appliance:

- Sync Service
- Remote Filtering Server and Client

  Note that while the Remote Filtering Client Pack option no longer appears in the installer, the utility used to configure Remote Filtering Client is included automatically on any Windows server that includes Web Security compoents. See the Deployment and Installation Center or “Remote Filtering Software” technical paper for details.
- Transparent identification agents (eDirectory Agent, Logon Agent, RADIUS Agent)

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

- Microsoft SQL Server 2008 or 2008 R2 Standard or Enterprise
- Microsoft SQL Server 2005 SP4 Standard or Enterprise

- Microsoft SQL Server 2008 R2 Express (installed using the TRITON Unified Installer)

Websense Web Security and Web Filter can be integrated with the following third-party firewall, proxy, and caching applications:

Product	Versions
Microsoft Forefront TMG	2008 or later
Cisco PIX Firewall	v5.3 or later
Cisco ASA	PIX v7.0 or later
Cisco Content Engine	ACNS v5.5 or 5.6
Cisco Router	IOS v12.3 or later
Check Point	Firewall-1 NGX or NGX 65; UTM-1 (VPN-1) Edge
Citrix XenApp	5.0 or 6.0

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

This version does **not** support:

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

See System requirements for this version in the Deployment and Installation Center for detailed hardware and software requirements.

Installation overview

The number of steps required to install Websense Web Security Solutions depends on the hardware platforms used in your environment, the size of your network, and how widely you plan to deploy components.

As a best practice, for software component installation, log in as a domain and local administrator to run the installer.

At simplest, a software installation requires you to:

1. Download the TRITON Unified Installer (see *Downloading the installer*, page 23).
2. Run the installer on a robust Windows Server 2008 (32-bit) or 2008 R2 machine.
3. Select the **Web Security All installation** option.

All components required for a basic Websense Web Security deployment are installed on the selected machine, including the TRITON Unified Security Center and, if no other Microsoft SQL Server instance is identified in your network, SQL Server 2008 R2 Express.

A simple appliance deployment requires you to:

1. Run the **firstboot** script and configure the full policy source appliance.
2. Download the TRITON Unified Installer (see *Downloading the installer*, page 23).
3. Run the installer on a Windows 2008 R2 server.
4. Select the **TRITON Unified Security Center** radio button, and the **Web Security** check box beneath it.

   Installing the TRITON Unified Security Center requires Microsoft SQL Server. If an existing SQL Server instance is not available, SQL Server 2008 R2 Express is installed.
5. Run the TRITON Unified Installer again (on the TRITON Management Server or another machine) and select **Custom**, then **Web Security** to install off-appliance components that are not part of the TRITON console, like transparent identification agents.

For a typical software deployment, expect to run the TRITON Unified Installer (or the TRITON Unified Installer plus the Web Security Linux Installer) on at least 3 machines:

1. Use the TRITON Unified Installer or Web Security Linux Installer to perform a **Custom** installation for core filtering components (Policy Broker, Policy Server, Filtering Service, Network Agent, User Service, Usage Monitor) on a supported Windows or Linux machine.
2. Use the TRITON Unified Installer to perform a **TRITON Unified Security Center > Web Security** installation to install core management components and reporting tools on a supported Windows machine.

   Installing the TRITON Unified Security Center requires Microsoft SQL Server. If an existing SQL Server instance is not available, SQL Server 2008 R2 Express is installed.
3. Use the TRITON Unified Installer to perform a **Custom > Web Security** installation of Web Security Log Server on a supported Windows machine.

See the Deployment and Installation Center for more detailed information.

Installing Web Filter components on Red Hat Linux 6.2 64-bit

If you plan to install Web Filter on a Red Hat Linux v6.2 machine, you must first install compatibility modules. In v6.2, Red Hat packages 32-bit versions of its system libraries in an add-on module rather than installing them by default as in previous releases.

1. On the machine where you are installing Web Filter, set up a Yum repository for the 32-bit compatibility libraries.

a. Mount the Red Hat Enterprise Linux installation DVD to the folder **/mnt/cdrom**.

b. Create a file named **RH62-Media.repo** in the **/etc/yum.repos.d** folder.

c. Add following content to **RH62-Media.repo** and save the file.

```
[RH62-Media]
name=RedHat-$releasever - Media
baseurl=file:///mnt/cdrom
gpgcheck=0
enabled=1
```

d. Run the following command:

```
# yum clean all
```

2. Install the required library packages:

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

Upgrade overview

To upgrade directly to Websense Web Security Version 7.7:

- Your current deployment must be at Version 7.5 or later.
- All components that you want to upgrade (rather than install separately after core components are upgraded) must be on a supported operating system. This may require:
  1. Reinstalling your existing version of Policy Broker and Policy Server on a platform supported in v7.7.
  2. Migrating policy and configuration settings to the new installation on the new platform. (See [LINK]).
  3. Running the upgrade process.
- If your Web Security solution is integrated with a third-party firewall, proxy, or cache, make sure that it is supported in this version. If you are using an integration product that is no longer supported, update the integration product before starting the upgrade process.
- If you are using MSDE, or a version of Microsoft SQL Server prior to 2005 SP4, upgrade the database to a supported version.

Once all components are on a supported platform, the third-party integration (if any) is up-to-date, and a supported database engine is in place, upgrade your Web Security components in the following order:

1. Upgrade the Policy Broker machine (or full policy source appliance).

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

Downloading the installer

To download the TRITON Unified Installer or Web Security Linux Installer:

1. Go to mywebsense.com and log in to your account.

   You are taken to the My Products and Subscriptions page.
2. Click the **Downloads** tab.
3. Under Download Product Installers, select your **Product** and **Version** (7.7).

   The available installers are listed under the form.
4. Click the plus sign ("+") next to an installer entry for more information about the installer.
5. Click the **download** link to download the installer.

Note that the TRITON Unified Installer is very large (approximately 1.6 GB), so if you have a slower network connection, it may take some time to download.

Installation and upgrade tools and references

- Deployment and Installation Center: Web Security Installation
- Deployment and Installation Center: Web Security Upgrade
- Web Security Default Ports

Operating tips

Topic 50233 | Release Notes | Web Security Solutions | Version 7.7 | Updated 02-Jul-2012

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7

To improve your experience with TRITON - Web Security:

- Disable all browser pop-up blocking features.
- Make sure that Internet Explorer Enhanced Security Configuration (IE ESC) is disabled.
- Make use of the quick start tutorials offered when you launch TRITON - Web Security.
  - If this is your first experience with Websense Web Security, use the New User Quick Start tutorial to learn about policy creation and reporting.
  - If you have used previous Web Security versions, use the Upgrading User Quick Start tutorial to orient yourself to what has changed in this version.
- Avoid using the browser Back and Refresh buttons. Instead, use the breadcrumbs at the top of the page or the left and right navigation panes.
- **Click OK at the bottom of each page in TRITON - Web Security to cache changes made on the page.**

  In some instances, when you are performing secondary tasks, you must click OK on the secondary page, and then click OK again on the main page to cache your changes. Make sure you see the “Changes have been cached” success message.
- Click **Save and Deploy** to implement cached changes.

  It can take up to 30 seconds for all Websense components to be updated with the changes.

To improve your experience with Websense reporting tools:

- If you install TRITON - Web Security first, and then install Log Server, you must manually restart the **Websense TRITON - Web Security** service on the TRITON Management Server machine. This ensures that reporting data appears in TRITON - Web Security, and that scheduled jobs are properly stored in the Log Database.
- If you are using Internet Explorer 8, make sure that Compatibility View (the button between the URL and the Refresh button in the browser address bar) is turned **off**.

Resolved and known issues

Topic 50234 | Release Notes | Web Security Solutions | Version 7.7 | Updated 02-Jul-2012

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.7

A list of resolved and known issues in this release is available to Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere customers.

If you are not currently logged in to MyWebsense, clicking the link brings up a login prompt. Log in to view the list.