v7.8.1 Release Notes for Websense® Web Security

Topic 43010 | Release Notes | Web Security Solutions | Updated 22-Oct-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.1

Use the Release Notes to find information about what's new and improved for Websense Web Security solutions in version 7.8.1.

New in Websense Web Security v7.8.1

Topic 43012 | Release Notes | Web Security Solutions | Updated 22-Oct-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.1

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

The Web Security Help, however, is available in both English and Japanese. Select your Help system language on the TRITON Settings > My Account page in the TRITON console.

ThreatScope™

ThreatScope is a Websense-hosted, cloud-based sandbox that provides enhanced detection of 0-day attacks. Files that pass Web Security Gateway Anywhere real-time security analytics and that fit a Websense Security Labs profile for suspicious files, are uploaded to the ThreatScope sandbox for activation. ThreatScope observes the behavior of the file and compiles a report. If the file is found to be malicious, the Content Gateway web proxy sends an email alert to the Web Security administrator (configured on the **Setting > Alerts > Enable Alerts** page) that includes information about the threat and links to a ThreatScope report and an Investigative Report generated from your log records.

ThreatScope is not applied to off-premises users whose traffic is going direct to the cloud for security analysis and policy enforcement.

ThreatScope is a premium add-on that requires Web Security Gateway Anywhere. It is enabled in the Web Security manager on the **Settings > Scanning > Scanning Options** page. It uses the Web Security **Email Alerts** feature to send malicious detection messages to the configured administrator's email address.

Files that qualify for ThreatScope sandboxing:

- Are not currently classified as malicious in the Websense Master Database
- Pass all **Security Threats: File Analysis** analytics
- Fit the Websense Security Labs profile for suspicious files
- Are a supported file type. Executable files are always supported. See the knowledge base article titled: ThreatScope Supported File Types.

Because such a file is not detected as malicious, it has been delivered to the requester.

Important

To receive ThreatScope email detection messages, **you must enable and configure email alerts**.

Go to **Settings > Alerts > Enable Alerts**, select **Enable email alerts** and specify an **Administrator email address**.

Important

The Content Gateway web proxy manages ThreatScope traffic.

Traffic is sent to:

- *.websense.com
- *.blackspider.com

The user agent is **ssbc**.

ThreatScope traffic must not be subject to man-in-the-middle decryption.

ThreatScope traffic cannot be challenged for authentication by any device in the network.

Filter.config rules are configured, by default, in Content Gateway. If Content Gateway is in a proxy chain or behind a firewall, those devices may have to be configured to meet the requirements described above.

For complete configuration information, see Security Threats: File Analysis.

What does a ThreatScope transaction look like?

1. An end user browses to a website and either explicitly or implicitly downloads a file.
2. The URL is **not** categorized as malicious and **Security Threats: File Analysis** does **not** find the file to be malicious.
3. The file is delivered to the requester.
4. However, the file fits the Websense Security Labs profile for suspicious files and is sent to ThreatScope in the cloud for analysis.
5. ThreatScope analyzes the file, which may take as long a 5 to 10 minutes, but is typically much quicker.

6. If the file is found to be malicious, Content Gateway sends a ThreatScope malicious file detection message to the configured alert recipient. The alert email includes links to the ThreatScope report and an Investigative Report created from your log records.
7. Upon receipt of the message, Administrators should:
    a. Access and evaluate the ThreatScope report for the file
    b. Examine the Investigative Report for the incident
    c. Assess the impact of the intrusion in their network
    d. Plan and begin remediation
8. Separately, ThreatScope updates the ThreatSeeker® Intelligence Cloud with information about the file, the source URL, and the command and control targets.
9. ThreatSeeker updates the Websense Master Database, ACE analytic databases, and other security components, which are then pulled by Websense deployments.
10. The next time someone tries to browse the site, they and the organization are protected by their Websense Web Security deployment.

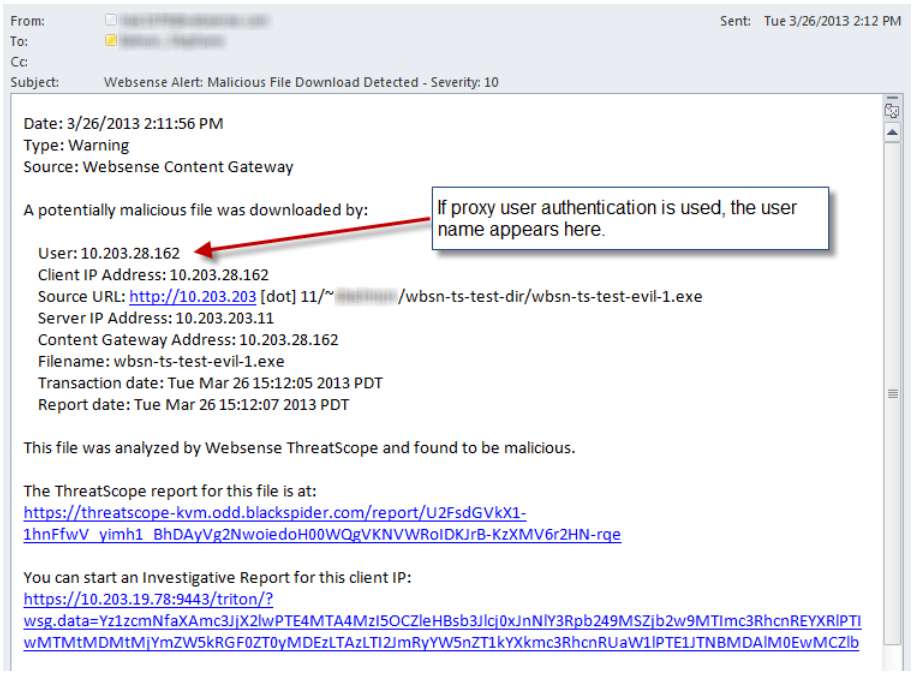
ThreatScope alert messages and reports

When Content Gateway learns that ThreatScope has detected a malicious file, it sends a ThreatScope alert email to the configured administrator. The message is plain text. An example is shown below.

In the body, the **User** field includes the user name only if Content Gateway user authentication was used to identify the client. Otherwise, the client IP address appears in the field.

Two links are included. The first links to a detailed ThreatScope report on the file and its malicious contents. The second launches an Investigative Report, using your log records, for the time period in which the file download occurred. Note that you may receive the ThreatScope alert message before Web Security Gateway Anywhere has written all of the transaction records in the log database. Periodically refresh the report to include pending records.

A typical alert message looks like:



A typical ThreatScope report looks like:

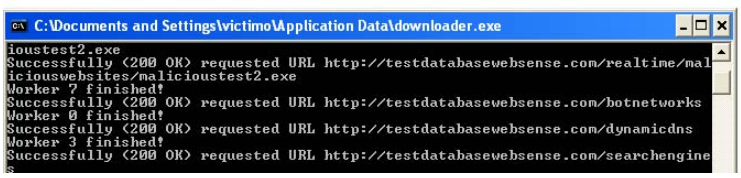
ThreatScope Analysis Report

For file with ID **23f9baa1f9873090d49b073d1e1309a1f2aa955e**

Assessment details:

Threat	Rating	Freq	Description
PROC_DROPPER_APPDATA	10		Drops and runs executable file(s) in a directory of the user profile often used by malware
CAT_BOTNET	10	1	Traffic to known botnet C&C server
CAT_MWS	10	1	Traffic to server hosting malicious content
REG_AUTORUN	8	1	Adds a registry key to automatically start an executable when the system starts
FS_DROPPER	8		Drops executable file(s)
PROC_POSSIBLE_INJECTED	6		Possibly injects code into remote process(es)
CAT_PDC	6	2	Traffic to server hosting potentially malicious content
FS_APPDATA	4	2	Writes to the filesystem in a directory of the user profile often used by malware

Screenshots



Deployment status viewer

The new **Status > Deployment** page provides a status and connection overview for your Web Security components. The Deployment page includes up to 3 tabs:

- **Policy Server Map** gives a visual overview of all of the Policy Server instances in your deployment. Click any instance to see status information for secondary components (like Filtering Service and User Service) that connect to that Policy Server.

  If your deployment only has one Policy Server, this tab is not displayed.
- **Component List** shows the name, location, Policy Broker, version, and status (started or stopped) for all of the Web Security components in your network. Administrators with appropriate permissions can stop or start component services or daemons from the list.
- **Directory Performance** provides connection and lookup speeds for each LDAP directory server that User Service queries for user and group information. Use this information to troubleshoot browsing delays or problems applying user-based policies in your network.

  If your network uses Windows Active Directory in mixed mode, this tab is not displayed.

New delegated administrator permissions determine which administrators can view information on the Deployment page, and which administrators can stop and start services from the Deployment page.

Policy Broker replication

Websense Policy Broker is the component that controls access to global configuration information and policy data consumed by other components.

In previous 7.x versions of Websense Web Security products, there could be a maximum of one Policy Broker per deployment.

Beginning in version 7.8.1, you can deploy Policy Broker in either of 2 configurations:

- In a **standalone** configuration, there is one Policy Broker for the entire deployment, as in v7.7.x and earlier. All Policy Servers connect to the same Policy Broker.

  In a standalone deployment, Policy Broker can reside on a Windows or Linux server, or a Websense appliance.
- In a **replicated** configuration, there is one **primary** Policy Broker, to which configuration and policy changes are saved, and one or more **replica** instances, each with their own read-only copy of the configuration and policy data. Each Policy Server can be configured to determine whether it attempts to connect to the primary Policy Broker or a replica instance at startup.

In a replicated configuration, Policy Broker cannot reside on a Websense appliance. Both the primary and replica instances must be hosted by a Windows or Linux server.

When Policy Broker replication is enabled, should the primary Policy Broker machine fail, all components connect to replica Policy Broker instances and continue to run normally, using the read-only configuration and policy data stored by the replica.

After a failure, in order to enable configuration changes, administrators can:

- Repair or restore the original primary Policy Broker.
- Reconfigure one of the replica instances to become the new primary Policy Broker.
- Install a new primary Policy Broker, then restore existing configuration information to the new Policy Broker (either from the original primary or from a replica).

When installing replica instances of Policy Broker, keep in mind that each Policy Broker needs an instance of Policy Server on the same machine. This requirement is not reciprocal; you can still have Policy Server instances that do not have a Policy Broker on the same machine. In fact, even in very large deployments with a large number of Policy Servers, it is unlikely that have more than 2 or 3 replica Policy Broker instances would be useful.

User Service: Configurable directory timeout

In environments with high directory service latency, users may experience browsing delays when User Service attempts to perform user lookups, but cannot connect to the directory in a timely manner.

To address this issue, a configurable parameter, BindConnectionTimeout (introduced in v7.7.3), allows you set an appropriate directory service connection timeout value for your network environment. In v7.8, the default timeout value is **10 seconds**.

- The longer the timeout period, the more browsing delays a user may experience when directory service latency is high.
- The shorter the timeout period, the greater the likelihood that the user request will be managed based on the Default policy or an IP address-based policy, rather than the appropriate user or group policy.

To configure this value:

1. Navigate to the Websense **bin** directory on the User Service machine (/opt/Websense/bin/ or C:\Program Files\Websense\Web Security\bin\).
2. Open the **websense.ini** file in a text editor.
3. Locate the **[DirectoryService]** section of the file, or, if it does not exist, add it to the file.

4. Under [DirectoryService], add the following parameter:

   ```
   BindConnectionTimeout=<value_in_seconds>
   ```

   In most cases, a value between 5 and 30 seconds is appropriate.

   If the value is set to 0, User Service uses the default OpenLDAP timeout period (currently 2 minutes).
5. Save and close the file.
6. Restart the Websense User Service service or daemon.

User Service: Improved domain mapping behavior

When a user name is sent to User Service, it may contain the NetBIOS domain name. In environments where there are many domains and domain controllers, User Service uses the domain name information to query the correct domain controller for user and group information.

In previous versions, when the NetBIOS domain name was very different from the DNS domain name, administrators needed to provide a file mapping one to the other. Starting in v7.8, User Service will query the NetBIOS and DNS domain names from the Configuration partition in Active Directory to create the mapping automatically.

In order for this automatic mapping to work:

1. For each forest in the network, the forest root must be one of the directories configured on the Settings > General > Directory Services page in the Web Security manager.
2. For the forest root, one of the following must be true:
   - The root context is entered in the **Context** field on the Directory Services page.
   - The Context field is left empty, and the administrator account provide on the Directory Service page is a user in the domain that is the forest root.
3. User Service can communicate with port 389 on the forest root.

If any of these is not true, administrators who use the **domains.txt** file must still create it manually.

User Service reads the contents of the **domains.txt** file and runs the query to get NetBIOS and DNS domain names. It then combines the lists, using the DNS domain name as the unique key, and uses the combined mapping for all user name lookups. The list is written to the domains.txt file.

- Values from the file take precedence over the values returned by the query. As a result, if a.b.c=XYZ exists in the file, and a.b.c=NMO is returned by the query, XYZ is used in the combined list and a diagnostic message indicates that a duplicate was found.

  If you change the NetBIOS domain name for any domains, but keep the same DNS domain name, edit **domains.txt** by hand to update the mapping.

- This process takes place on startup, and every time Directory Service settings change in the Web Security manager.

The new domain mapping behavior is enabled by default. You can disable it via the **UseDomainMap** parameter in the **websense.ini** file.

User Service: Improved domain caching

When it performs a user name lookup, if the user name contains domain information, User Service first queries each domain controller in its list to find the correct domain controller for the domain.

Starting in this version, the domain controller to domain correlation information is cached, reducing the need to search for the correct domain controller each time User Service is passed a fully-qualified domain name (FQDN) for a user. This improves the speed of user lookup requests.

These cache entries have the same timeout as the user cache (3 hours, by default) and are cleared when Directory Service settings change or when the User Service cache is cleared.

Improved reporting on directory service latency

The **Directory Performance** tab of the Deployment status viewer (described at the start of this v7.8 overview) tracks how quickly User Service is able to connect to and perform lookups using the directories in your network.

Each entry shows the average bind (connection) and lookup times in milliseconds, the speed of the most recent bind and lookup, and the maximum (slowest) bind and lookup times for each User Service instance. It also shows how many bind and lookup attempts have occurred in the time period selected at the top of the tab (one hour, by default), and how many bind or lookup failures have occurred.

Use this information to identify network and directory latency problems that could impede user identification and slow responses to users' web requests.

Information on the Directory Performance page is updated every 5 minutes.

If average latency over the most recent 5 minute period is 5 seconds or more, a health alert is displayed on the Status > Alerts page. The alert includes the IP addresses of up to 3 directory servers that have high response times.

Application reporting

A new reporting tool, accessed from the **Reporting** > **Applications** page, offers reports on browsers and operating system platforms in your network based on user agent headers.

The user agent header is a string that web applications, including web browsers, use in HTTP communication to identify themselves and their capabilities.

Application reports require that web traffic be managed by Content Gateway (in Web Security Gateway and Gateway Anywhere deployments) or Network Agent (in Web Security and Web Filter standalone deployments). Third-party integration products do not forward the user agent information required to enable this tool.

The Applications page is divided into 3 tabs:

- The **Browser** tab gives an overview of the desktop and mobile web browsers in your network from which requests have been made. Click a browser family or version to see a detail report with more information about who is using the selected browser type.

  Use this information to reduce network vulnerabilities by making sure users are keeping their browsers up to date.

  Available browsers include Internet Explorer, Firefox, Chrome, Safari, Opera, Safari Mobile, Opera Mobile, Chrome Mobile, and Internet Explorer Mobile.
- The **Source Platform** tab gives an overview of the desktop and mobile operating systems from which web requests have been made. Click a platform or version to see a detail report about who is running on the selected operating system.

  Available platforms include Windows, Linux (including Ubuntu, Google Chrome OS, Red Hat, CentOS, Fedora, Suse, NetBSD, OpenBSD, Debian, and GNU/Linux), UNIX, Mac OS X, iOS, Android, BlackBerry, Symbian OS, Java ME, and Windows Phone.
- The **Search** tab lets you search for specific strings within the user agent headers logged in your network.

  Use search to find user agents associated with specific apps or vulnerabilities, or to find information about browser types and operating system platforms not supported by the graphical charts on the Browser and Source Platform tabs.

A nightly Log Database job (the Trend job) is responsible for parsing new user agent strings to determine whether they correspond to a browser or source platform. Only after new user agents have been parsed do they appear in charts on the Browser and Source Platform tabs. As a result:

- When you initially install this version, a “No data to display” message appears on the Browser and Source Platform tabs, even after the system begins handling web traffic. The charts on these tabs are populated only after the nightly job runs.
- After the Browser and Source Platform charts are populated, if a new user agent (never previously seen in your deployment) is detected in your network, it will not appear in charts until after the nightly job has run.

In both cases, though the charts may not be updated until the next day, new user agents appear on the Search tab as soon as they are logged.

Enhanced user assistance

This release introduces expanded options for accessing user assistance, like checklists, worksheets, Help, tutorials, webinars, and videos from within the Web Security manager.

- In new deployments, until a Super Administrator enters the subscription key, the **Initial Setup Checklists** offers configuration guidance for new Web Security administrators. The checklist offers a combination of direct guidance, interactive tutorials, and step-by-step instructions for completing tasks like entering the key, setting up policies, and defining clients.
- The area above the Web Security Toolbox in the right, shortcut pane now helps you **Find Answers** to your questions.
  - **Top Picks** link to current content hosted on the Websense eSupport website, or to pages in the Web Security manager where common tasks are done. Position the mouse over a link for a tooltip with more information.
  - **Show Me How** tutorials walk you through key tasks, from editing the Default policy to configuring Network Agent.
  - Enter search terms in the **Search eSupport** box to find information in any part of the Websense Knowledge Base. The search is performed based on your current Web Security product and version.

  A remote update function allows the Websense User Assistance team to update links in the Find Answers box in response to questions or issues that arise, or in response to customer feedback. The Web Security manager checks for updates once a day.

Logon application support for Mac OS X 10.8.2 and later

Logon Agent communicates with the logon application (LogonApp) on client machines to identify users as they log onto or off of Windows domains.

In this version, the logon application is available for:

- Mac OS X 10.8.2 (64-bit) and later
- Windows 64-bit platforms
- Windows 32-bit platforms

In a change from previous versions, during Logon Agent installation, each version of the logon application is placed in a subdirectory under:

```
Websense\Web Security\bin\LogonApp\
```

The Mac version of logon application, for example, resides in the **Mac** subdirectory, in the form of a tar file called **LogonApp.tar.gz**.

To install the logon application on Mac clients, first untar the file:

```
tar -zxf LogonApp.tar.gz
```

To install the logon application on the local machine, use the command:

```
./LogonApp.install -ah <Agent1,Agent2> -sp <sudo_password>
```

To install the logon application on one or more remote clients, use the command:

```
./LogonApp.install -ah <Agent1,Agent2> -cl <client1,client2>
-u <ssh_username> -p <ssh_password> -sp <sudo_password>
```

In these examples:

Parameter	Value	Value Example
-ah	Comma-separated list of Logon Agent IPv4 addresses	10.50.1.2,10.50.1.12, 10.50.1.22
-cl	Comma-separated list of client IPv4 addresses or hostnames, *or* Name of file containing list of client IPv4 addresses or hostnames	10.100.17.3,10.100.17.4, 10.100.17.5 *or* @mac_client_list.txt
-u	SSH user name for connecting to remote hosts	username
-p	SSH password for connecting to remote hosts	password
-sp	The sudo password for the machine on which the install command is run	password
-r	(none) Prompts the installer to restart the client after successful installation.	(none)

On Mac clients, the logon application supports fast switching, allowing for identification and proper policy application for multiple users on the same machine. The logon application runs as a Mac launch agent for every user logged onto the machine.

If Active Directory authenticates the user, the logon application:

- Determines the host's IPv4 and IPv6 addresses
- Subscribes with the operating system to be notified of IP address changes
- Subscribes with the operating system to be notified when the host machine sleeps or wakes up
- Forwards HTTP requests to Logon Agent

If Active Directory fails to authenticate the user, the logon application exits.

For more information about Logon Agent and the logon application, see the Using Logon Agent for Transparent User Identification white paper.

Third-party platform and product support

This version introduces support for:

- Citrix XenApp 6.5
- Microsoft Active Directory 2012
- Microsoft SQL Server 2012
- Microsoft Windows Server 2012

  Note that installing Web Security components on Windows Server 2012 requires Microsoft .NET Framework v3.5. Install .NET Framework v3.5 before running the TRITON Unified installer.

Removed in this version

This version ends support for:

- Microsoft Windows 2008 (32-bit)

  Note that Windows Server 2008 R2, a 64-bit platform, is still supported.
- Websense Web Security and Web Filter integration with:
  - Check Point products
  - Cisco PIX
  - Cisco Content Engine
- Web Endpoint for Mac OS, 32-bit

  Note that 64-bit Web Endpoint for Mac OS is still supported.

In addition, Microsoft SQL Server 2005 SP 4 is no longer certified for use with Websense Web Security solutions. For those who continue to use SQL Server 2005 SP 4, best-effort support will still be provided.

Installation

Topic 43013 | Release Notes | Web Security Solutions | Updated 22-Oct-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.1

Requirements overview

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

- Microsoft Windows Server 2008 R2 or R2 SP1, or 2012 (64-bit)

  Important
  Before installing any components, make sure that .NET Framework 3.5 is installed on the machine.

- Red Hat Enterprise Linux 6.x (64-bit)

The following components run on Windows platforms only:

- TRITON Unified Security Center
- Linking Service
- Web Security Log Server
- DC Agent
- Real-Time Monitor

Websense Content Gateway is a Linux-only component that requires Red Hat Enterprise Linux 6.2 or 6.3.

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

- Sync Service
- Remote Filtering Server and Client

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

To enable Web Security reporting tools, use one of the following certified database engines:

- Microsoft SQL Server 2012 Standard, Business Intelligence, or Enterprise

> **Important**
> SQL Server 2012 uses a different security model than previous versions. To successfully create the Log Database in SQL Server 2012, you must either:
>
> - Install the database in the default SQL Server folder.
> - Grant the database engine full control over the folder that will host the database before you install Log Server.

- Microsoft SQL Server 2008 or 2008 R2 Standard or Enterprise
- Microsoft SQL Server 2008 R2 SP2 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 ASA	v8.0 or later
Cisco Router	IOS v15 or later
Citrix XenApp	5.0, 6.0, or 6.5

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

This version does **not** support integration with Check Point products.

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 (**WebsenseTRITON781Setup.exe**).
2. Run the installer on a robust Windows Server 2008 R2 or 2012 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 SP2 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 (**WebsenseTRITON781Setup.exe**).
3. Run the installer on a Windows Server 2008 R2 or 2012 machine.
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 SP2 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 SP2 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.

Start-to-finish installation instructions covering most typical deployments are available in PDF format:

- Installation Instructions: Web Security Gateway Anywhere
- Installation Instructions: Web Security Gateway
- Installation Instructions: Web Security or Web Filter

Operating tips

Topic 43014 | Release Notes | Web Security Solutions | Updated 22-Oct-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.1

To improve your experience with the Web Security manager:

- Disable all browser pop-up blocking features.
- If you have problems accessing the console from Internet Explorer:
  1. Make sure that Internet Explorer Enhanced Security Configuration (IE ESC) is disabled.
  2. If problems continue, reset Internet Explorer to its default configuration. To do this, in Internet Explorer, go to **Tools** > **Internet Options** and select the **Advanced** tab, then click **Reset**. When prompted, click **Reset** again.
- Make use of the quick start tutorials offered from the Getting Started section of the TRITON console Help menu.
  - If this is your first experience with Websense Web Security, use the New Admin Quick Start tutorial to learn about policy creation and reporting.
  - If you have used previous Web Security versions, use the Upgrading Admin 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 the Web Security manager 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 the TRITON management server 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 the Web Security manager, 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 43015 | Release Notes | Web Security Solutions | Updated 22-Oct-2013

Applies to:	Websense Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.1

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.