Release Notes

Websense® Content Gateway

Version 7.0.4

Key features in this release

Version 7.0.4 is a maintenance release for the Websense Content Gateway. No significant new features are introduced in this version. Features highlighted in these Release Notes were first made available in Websense Content Gateway version 7.0.0.

Websense Content Gateway supported on RHEL Release 4 Update 5

Starting with version 7.0.0, Websense Content Gateway is available on Red Hat Enterprise Linux Advanced Server Release 4 Update 5. The supported kernel is 2.6.9-55. See the Websense Content Gateway *Installation Guide* for information on requirements.

SSL decryption

Starting with version 7.0.0, Websense Content Gateway supports SSL decryption of HTTPS traffic. This traffic is sent to a dedicated port, decrypted, inspected, and then re-encrypted and sent to its destination.

Websense SSL Manager provides certificate management as well as decryption. Enable SSL decryption to realize the full benefits of proxy interaction with Websense Data Security Suite.

See the Websense Content Gateway *Installation Guide* for information about configuring your router to support a transparent proxy deployment and SSL Manager.

Using ICAP with Websense Data Security Suite

With support for ICAP with Websense Data Security Suite, users can control information leakage that can occur through postings to the World Wide Web.

ICAP facilitates off-loading of content for analysis to designated servers. Outgoing content, such as an upload or posting, is examined, and then either blocked or forwarded to its destination. The proxy acts as an ICAP client communicating with Websense Data Security Suite, which is acting as an ICAP server.

Supported protocols

Protocols supported at this release are HTTP, HTTPS, and FTP over HTTP.

Corrections in version 7.0.4

- When Websense Content Gateway was configured to use LDAP authentication, users who opened a browser and supplied their credentials were sometimes denied Internet access. This typically occurred in a child domain and could prevent authentication in both parent and child domain. This issue has been corrected.
- When Websense Content Gateway was installed in transparent proxy mode, if a user tried to join a WebEx meeting, the browser could hang during the **connecting** message, and an HTTPS tunnel incident could not be added (to allow the WebEx client to connect). This issue has been corrected.
- An interruption in the processing of HTTP requests and responses could occur when Websense Content Gateway reset itself. Resets could be triggered by URL requests that received no response. This issue has been corrected.
- Under rare circumstances, when a user had accessed hotmail.com via the Websense Content Gateway (in an explicit proxy deployment), attempts to delete an email message could result in a seeming endless loop. When the user deleted the email message, the hotmail site could continuously display “Working on your request” at the bottom of the page. This issue has been corrected.
- If the database Download Service for the proxy databases crashed, sometimes the service did not restart automatically, as expected. This issue has been corrected.
- Attempts to buffer a large file with the proxy sometimes caused an internal process to run out of memory and crash. This issue has been corrected. The software no longer attempts to buffer files larger than a maximum scan size you configure in Websense Manager. You can use a setting called `wtg.config.fail_open` in the file **records.config** to specify whether these exceptionally large files (that are not scanned) are allowed (INT=1 means fail open) or not allowed (INT=0 means fail closed).
- If a user attempted to log in with an incorrect password, sometimes the LDAP authentication failed intermittently for other users who logged in afterwards. This could occur for a user whose cache entry had expired. This issue has been corrected.

Operation tips

These tips pertain to all versions 7.0.x.

Proxy installation password: no spaces

Don’t use spaces inside the password you enter for the Websense Content Gateway proxy during installation. Also, do not add a space as a trailing character for the proxy password.

Proxy password: 16 characters or fewer

Use 16 characters or less for the proxy password. Websense Content Manager (management interface) will accept more than 16 characters, but the password will be truncated automatically.

Installation file paths

During the installation of the Websense Content Gateway proxy, when you specify installation file folders and file names:

Use only upper-case and lower-case letters, digits, hyphens, and underscores.

- Do not use spaces in file or folder names.
- Do not use single quotes or other non-standard characters.

Although you may not be prevented from entering quote marks or other special characters in the path name, the installation itself may be unable to complete successfully.

Hardware requirements

CPU	Quad-core running at 2.8 GHz or faster
Memory	4 GB
Disk space	2 disks: • 100 GB for the operating system, Websense Content Gateway, and temporary data. • 100 GB for storage (caching). This disk: – Must be a raw disk – Must be dedicated – Must *not* be part of the RAID.
Router	WCCP 1.0 routers support HTTP only. If your site is processing other protocols, such as HTTPS, your router must be WCCP2-enabled.
or	For SSL Manager, the router must support WCCPv2. See the Websense Content Gateway *Installation Guide* for information on configuring your router.
	A Cisco router must be running IOS 12.2.
Layer 4 switch	You may use a Layer 4 switch rather than a router. A Cisco switch requires the EMI or IP services image of the 12.2SE or later IOS release to support WCCP.

Software requirements

- Red Hat Enterprise Linux Advanced Server Release 4 Update 5, kernel 2.6.9-55
- Ensure that the following RPM is on your system:
  - compat-libstdc++-33-3.2.3-47.3.i386.rpm

    Enter the command

    ```
    rpm -qa > filename
    ```

    to list the RPMs on your system and print the list to a file.
- Websense Web Security or Websense Web Filter v7 (not required when you are running only with Websense Data Security Suite)
- Internet Explorer v7.0 or Firefox v2.0 for running Websense Content Manager
- Windows server for Reporting

For additional requirements, see the Websense filtering *Deployment Guide* or the Websense Data Security Suite *Installation Guide*, depending on your configuration.

Security recommendations

Important Websense recommendations for the physical and operational security of your proxy server are included in Knowledge Base article 3556.

Configuring your router

If your site is running Websense Content Gateway in a transparent proxy deployment, or if your subscription includes Websense SSL Manager, you must configure your router to support WCCPv2. See the *Deployment Guide* for details.

Port configuration

A full deployment of Websense Content Gateway means that several ports will be open. See the Websense Content Gateway *Installation Guide* for information on open ports and on reassigning ports, if necessary, during the installation process.

Email address for receiving proxy alarms: no more than 64 characters

In Websense Content Manager, on the tab **Configure** > **General**, you can provide an email address to receive proxy Alarm email (for example, admin_proxy_one@acme.com).

Email addresses for alarm notifications must be no longer than 64 ASCII characters. The management interface does not enforce this character limitation, but an invalid email address may prevent the proxy from starting.

To correct an email Alert address, manually edit the file
<Install Dir>/config/records.config (usually /opt/WCG/config/records.config)
and modify the line containing the email address string:

CONFIG proxy.config.alarm_email STRING admin_proxy_one@acme.com

Known issues

Requests that go through the proxy to an Intranet site fail IIS authentication

Attempts to access Intranet sites receive an error from IIS (Internet Information Services), indicating that access is denied due to server configuration.

To avoid this authentication failure, do one of the following:

- Configure browsers so that Intranet users can bypass the proxy (and authentication).

  In Internet Explorer, use the **Tools** > **Internet Options** > **Connections** page to specify that Intranet sites not go through the proxy.

  a. Click **LAN Settings**.

  b. Select **Use a proxy server for your LAN**.

  c. Select **Bypass proxy server for local addresses**.

  d. Click **OK** to close the dialog boxes.

  In Firefox 2.0 and later, use the **Tools** > **Options** > **Advanced** > **Network** page to specify that Intranet sites not go through the proxy.

  a. Click **Settings**.

  b. Select **Manual proxy configuration**.

c. Enter the URL in the **No Proxy for** field. You can enter IP addresses or domain names, such as mycompany.com. Separate the entries with a comma.

d. Click **OK** or **Close** to close each dialog box or tab.

- Specify the IP address or URL of the site that should bypass the proxy. This option is available only in Internet Explorer.

  In Internet Explorer, use the **Tools** > **Internet Options** > **Connections** page to specify the IP address or URL of the site that should bypass the proxy.

  a. Click **LAN settings**.

  b. Select **Use a proxy server for your LAN**.

  c. Click **Advanced**.

  d. In the Exceptions area at the bottom of the window, enter the IP address or URL of the site that should bypass the proxy server.

  e. Click **OK** to close the dialog boxes.

- Disable Integrated Windows authentication within IIS. See the Microsoft Support site at http://support.microsoft.com/kb/324274 for information on configuring IIS Web site authentication.

User prompted for credentials when using NTLM single sign-on

In a transparent proxy deployment, users are prompted for credentials when using NTLM single sign-on. Users who need single sign-on through Internet Explorer must set a local Intranet site to the IP address of the proxy. If you do not achieve the desired results using dot notation (xx.xxx.xx.xxx), use the URL that resolves to the IP address of the proxy.

To configure Internet Explorer for single sign-on, you must configure the browser to consider the proxy as a local server.

Follow these steps in Internet Explorer:

1. Select **Tools** > **Internet Options** > **Security** > **Local intranet** > **Sites** > **Advanced**.
2. Enter the URL or IP address of the proxy.
3. Click **Add**.
4. Click **OK** until you have closed all the dialog boxes.

Then:

1. Select **Tools** > **Internet Options** > **Security** > **Internet** > **Custom Level**.
2. Select **Automatic logon with current username and password**. You can find this near the bottom of the settings tree.
3. Click **OK** until you have closed all of the dialog boxes.

Websense Content Gateway services may not start if port conflict exists

Websense Content Gateway services (including Websense Content Manager) do not start if there is a port conflict between Websense Content Gateway processes. Users are not informed that there is a port conflict.

You can reassign the following ports by editing configuration variables in the **records.config** file (default location is **/opt/WCG/config**).

Function	Configuration variable	Default port
Websense Content Gateway proxy port	*proxy.config.http.server_port*	8080
Web interface port	*proxy.config.admin.web_interface_port*	8081
Overseer port	*proxy.config.admin.overseer_port*	8082
Auto config port	*proxy.config.admin.autoconf_port*	8083
Process manager port	*proxy.config.process_manager.mgmt_port*	8084
Logging server port	*proxy.config.log2.collation_port*	8085
Clustering port	*proxy.config.cluster.cluster_port*	8086
Reliable service port	*proxy.config.cluster.rsport*	8087
Multicast port	*proxy.config.cluster.mcport*	8088

You can reassign the following ports only by uninstalling and reinstalling Websense Content Gateway, and reassigning ports during the installation process.

Function	Default port
SNMP encapsulation port	8089
Download Service port	30900

Enter the following commands for to reassign the ports associated with SSL Manager.

1. Export your library path.

   ```
   export LD_LIBRARY_PATH=/opt/WCG/sxsuite/lib
   ```

2. To reassign the HTTPS *inbound* port: (default port 8070):

   ```
   /opt/WCG/sxsuite/bin/oemtool inbound_port port
   ```

3. To reassign the HTTPS management port, which displays the SSL Manager interface (default port 8071):

   ```
   /opt/WCG/sxsuite/bin/oemtool cas_port port
   ```

4. To reassign the HTTPS *outbound* port: (default port 8090):

   ```
   /opt/WCG/sxsuite/bin/oemtool outbound_port port
   ```

NOTE

You need to export your library PATH only once per session. You can reassign none or all of these ports.

See the Websense Content Gateway *Installation Guide* for information on uninstalling Websense Content Gateway and assigning ports.

Client cannot access Intranet site with an explicit proxy deployment

If your client cannot access your Intranet site, verify that your operating system has been correctly configured to resolve all internal and external host names. Use the **nslookup** command to verify that a domain is listed in your DNS server:

For internal-facing servers:

```
nslookup intranet.mycorp.com
```

For external Web sites:

```
nslookup www.websense.com
```

If your corporation has multiple DNS domains, verify that a host name in each domain resolves correctly. If you are unable to resolve host names, verify the contents of the **/etc/resolv.conf** file, which provides search rules for how domain names are resolved in DNS.

Subsequent requests to a bypassed destination cause the browser to hang

If a browser page is opened after the proxy is dynamically bypassed, subsequent requests to the same page cause the browser to hang.

Set the system parameter */proc/sys/net/ipv4/ip_forward* to **1** on the proxy server to ensure that the proxy forwards all bypassed requests.

Disabling cache during installation does not persist

If you disable caching during installation of Websense Content Gateway, Websense Content Manager (the management interface) indicates that HTTP caching and FTP over HTTP caching are enabled. To see this after a successful installation, go to **Configure** > **Protocols** > **HTTP** > **Cacheability**. Note that HTTP caching and FTP over HTTP caching still show as enabled by default. To work around this issue, turn caching off in Websense Content Manager.

Proxy IP address should never be entered as a Virtual IP in your browser

Do not set up the IP address of the Websense Content Gateway proxy to be a Virtual IP in any network settings on your browser.

Virtual IP address not enabled or disabled on nodes in a cluster

When a Virtual IP address is enabled or disabled on one node in a cluster, this change does not propagate until the nodes are restarted.

Restart proxy after protocol settings change

If you change your protocol settings in Websense Content Manager (for example, with **Configure** > **SSL** > **Decryption/Encryption** > **Inbound** > **Protocol Settings**) you must restart the proxy for the new settings to take effect.

Restart of Websense Content Gateway can cause warning message

When you restart the proxy, you may see this message: “Warning: Form data out of date. Press Cancel to reload page and try again.”

Simply press **Cancel** to reload the page and try the restart again.

Limited access filter conflicts with Real-Time Content Stripping

In Websense Web Security, a list of individual Web sites (called a limited access filter) can be active in a Web filtering policy. When a limited access filter is active in a policy, users assigned that policy can visit only sites in the list. All other sites are blocked.

When a limited access filter is in effect, Websense software checks to see only if a requested site appears in the list. No other checking is performed.

However, an exception exists in version 7 of Websense Content Gateway.

If you enable Real-Time Content Stripping for ActiveX, JavaScript, and VBScript, and then add the hostname of a URL from a limited access list to the Always Scan List for Content Stripping in Websense Content Manager, then ActiveX, JavaScript, and VBScript content is stripped from that URL, even when the limited access list is active in the users' policy.

To work around this exception, so that no content is stripped, remove the URL hostname from the Always Scan List for Real-Time Content Stripping.

Websense Data Security Suite block page is not served with gmail

The Websense Data Security Suite block page is not served within AJAX-based Web pages.

Websense Data Security Suite is monitoring outgoing traffic and protecting against policy violations; however, the block page is not being displayed. Refer to the Websense Data Security Suite v7 *Release Notes* for additional information.

Count for SOCKS connections does not change

On the **Monitor** > **Security** > **SOCKS** tab, the count for SOCKS connections in progress does not change. This information is also not available from the command line.

Alarm indicates that connection throttle is too high

Websense Content Manager (the Websense Content Gateway management interface) may display a warning that the throttle connection of 10,000 is too high.

This should occur only after the initial installation of Websense Content Gateway and is resolved by rebooting the proxy server.

Parent proxy not authenticating

In a hierarchical caching environment, users cannot access the Internet if the proxy is running in a transparent proxy deployment, and NTLM or LDAP authentication is through the parent proxy.

For best results, authentication should take place on the proxy closest to the browser. A parent cache may contain child proxies that perform authentication. If authentication is through the child proxy, ensure that users/browsers do not have access to the parent proxy; otherwise they will be able to bypass authentication.

Websense Content Gateway service may stop when running print_bypass command

Running the `./print_bypass` command (located in **/opt/WCG/ bin**) can cause the Websense Content Gateway service to stop. To see the bypass rules in effect, review the **bypass.config** file located in the Websense Content Gateway **config** directory (default location is **/opt/WCG/config**).

Management interface does not start if ARM Security is enabled

If the proxy is restarted after ARM security is enabled, the management interface cannot be opened and traffic does not pass as designated in the **arm_security.config** file. The management interface opens if ARM security is disabled on the **Configure** > **Security** > **Connection Control** > **ARM Security** page.

Internet requests filtered by the real-time scanning options available in Websense Content Gateway or Websense Web Security Gateway are logged for reporting purposes only when Websense reporting components are installed on a Windows server. If your organization is using Websense Explorer for Linux for reporting, the reports do not contain any data resulting from threat-based scanning. If your organization has installed Websense Manager on a Linux server, or uses the Websense Explorer for Linux reporting program (instead of the reporting components that run on Windows), see the *Explorer for Linux Administrator's Guide* for information on installing that program and running reports

No reverse proxy

Websense Content Gateway v7 does not function as a reverse proxy.

Proxy caching PAC data

When the proxy is configured using a PAC (proxy auto-configuration) file, Internet Explorer may cache that data and not block sites appropriately. Consider disabling automatic proxy caching in Internet Explorer. For information, see http://support.microsoft.com/?kbid=271361.

Browsing to site with self-signed certificate (Websense Manager) may generate an error

Attempting to browse to any Web site that has a self-signed certificate will generate a certificate incident if the SSL certificate verification engine is enabled.

(By default, the SSL certificate verification engine is disabled.)

If the certificate verification engine is enabled, you can add the domain/URL of the site with the self-signed certificate as an exception.

Other options:

- If the browser is configured for explicit proxy, you can remove the explicit browser entries.
- If the browser is configured using WPAD or a PAC file, then that configuration can be disabled.
- If your site is using WCCP, there is no workaround.

Users may receive a certificate error from Internet Explorer when visiting secure sites

When Websense Content Gateway is running in a transparent proxy deployment with SSL Manager, users may receive a certificate error from Internet Explorer before they receive the certificate verification result from SSL Manager, when certain secure sites are visited.

This can occur when a user attempts to access a site whose CA (certificate authority) is not listed on the **Configure** > **SSL** > **Certificates** > **Certificate Authorities** page. CAs are added to this list when a user attempts to access a site requiring a certificate; however CAs are added with **deny** status by default. The administrator must change the status to **allow**.

If a user attempts to visit the site before the status has been changed, the user receives a certificate error. See the Websense Content Manager Help system for information on incidents and changing the status of a certificate.

This can also occur when the common name of the certificate (for example, company_name.com) does not match the URL (for example, www.business_name.com).

This does not occur when you are running in an explicit proxy deployment.

Users may receive garbled content when content stripping is on and a Web page contains non-ASCII content

If you use Content Stripping, then Web content that is not ASCII-encoded (not UTF-8 encoded) is transcoded to UTF-8 before it is scanned for possible content stripping. The content that is not stripped can be returned garbled to the client, unless you have set an option in Websense Content Manager:

1. Open your Web browser.
2. Enter the following URL in your browser to start Websense Content Manager (the Websense Content Gateway management interface):
   - **Standard**: `http://`*`nodename`*:*`adminport`*

     where *`nodename`* is the name of the proxy node and *`adminport`* is the number assigned to the Websense Content Manager port (the default value for *`adminport`* is 8081).
3. Navigate to **Configure** > **Protocols** > **HTTP** > **Privacy** > **Remove Headers** > **Remove Others**.
4. Add **Accept-Encoding**.
5. Click **Apply**, and then click **Restart**.

Users not prompted for authentication when browsing HTTPS sites

Users are not prompted for authentication when they are browsing HTTPS sites with the proxy running in a transparent proxy deployment and SSL Manager turned off.

This does not occur when SSL Manager is enabled. If your subscription includes SSL Manager:

1. Open your Web browser.
2. Enter the following URL in your browser to start Websense Content Manager (the Websense Content Gateway management interface):
   - **Standard**: `http://`*`nodename`*:*`adminport`*

     where *`nodename`* is the name of the proxy node and *`adminport`* is the number assigned to the Websense Content Manager port (the default value for *`adminport`* is 8081).
3. Navigate to the **Configure** > **My Proxy** > **Basic** > **General** page.
4. Click HTTPS **On**.
5. Click **Apply** and then click **Restart**.
6. See *Working With Encrypted Data* in the Websense Content Manager Help system for additional information on configuring SSL Manager.

If your subscription does not include SSL Manager, users are not prompted for authentication when they are browsing HTTPS sites and the proxy is in a transparent proxy deployment.

Internet Explorer does not display block page when HTTPS is disabled

If HTTPS is disabled, and an Internet Explorer browser is configured to send both HTTP and HTTPS traffic to port 8080, when a user browses to a secure site that should result in a blocked or quota page, then Internet Explorer does not send the block or quota page.

This happens the first time a user tries to access a secure site in a browser session. After the user visits a non-secure site in the same category, future visits to secure sites in a quota-blocked category result in the user's viewing the page if quota time remains. However, for sites that should be blocked, the user does not receive a block page.

This occurs only in Internet Explorer; it does not occur in Firefox.

HTTPS configuration not synchronized in a cluster

HTTP configuration is synchronized in a cluster; HTTPS configuration is not. In a Websense Content Gateway deployment with multiple servers, one server should be devoted to HTTPS traffic, and the nodes can be devoted to HTTP traffic.

Port 8090 binds to additional interfaces

Port 8090 binds to all interfaces, rather than only to connections originating from Websense Content Gateway.

Enter the following command in iptables to ensure that port 8090 is bound properly.

```
iptables -A INPUT -p tcp -s 0/0 --destination-port 8090 -j DROP
```

See the Websense Content Gateway *Installation Guide* for additional information about opening ports.

Titles of real-time reports

The following reports contain information on real-time activity (content and application scanning and content stripping). These reports are available in the Security Threats area of the Presentation Reports.

Blocked Downloads by Security Threat	Blocked Security Risk Downloads by Group
Blocked Security Risk Downloads by User	Blocked Security Risk Sites by Group
Blocked Security Risk Sites by Requests	Blocked Security Risk Sites by User
Detail of Blocked Download Requests by Security Threat Type	Detail of Blocked Security Risk Downloads by user
Detail of Blocked Security Risk Sites by User	Stripped Content Types by User
Top Blocked Download Requests by Security Threats	Top Blocked Groups by Security Risk Download Requests
Top Blocked Security Risk Sites by Requests	Top Blocked Security Threats by Requests
Top Blocked Users by Security Risk Download Requests	Top Groups Blocked from Security Risk Sites
Top Users Blocked from Security Risk Sites	

Server address appears with a value of 0 in real-time reports

The IP address of the proxy server may appear as 0 in real-time reports. See the list of reports in *Titles of real-time reports* to see which reports are affected.

To display the address of the proxy server in real-time reports, enter the IP address of the proxy server as the first entry in the /etc/hosts file.

Extended characters may not appear in reports

When authentication is done via the proxy, usernames containing extended characters may not appear correctly in reports.

If this occurs, use a Websense filtering transparent identification (XID) agent (instead of the proxy) for user identification.

Enabling IP forwarding

By default, IP forwarding is disabled when Websense Content Gateway is installed. Rebooting the Websense Content Gateway server after installation is recommended, and enables IP forwarding. Note that IP forwarding must be enabled if you are setting up a router or gateway.

You can also enable IP forwarding via the command line.

1. Become root and enter the root password.
2. Add the following line to the **/etc/sysctl.conf** file:

   ```
   net.ipv4.ip_forward = 1
   ```

3. Enable the changes:

   ```
   sysctl -p /etc/sysctl.conf
   ```

Then edit the **bypass.config** file as appropriate. See the Websense Manager Help system for details on **bypass.config**.

Updating the list of Certificate Authorities

After an initial deployment of SSL decryption and re-encryption only, you may choose to verify certificates. For peak performance, the Certificate Authorities (CAs) listed on the **Configure > SSL > Certificates > Certificate Authorities** page should match the certificates available in Internet Explorer 7. Follow these steps in Internet Explorer and then in Websense Content Manager to import those certificates into SSL Manager.

In Internet Explorer

1. Navigate to the **Tools > Internet Options > Content** page.
2. Select **Certificates**, and then select the **Trusted Root Certificate Authorities** tab.
3. Double-click a CA, such as America Online Root Certification Authority 1, and then click **Details**.
4. Click **Copy to File** to launch the Export Certificate wizard.
5. In the wizard:
   a. Click **Next**.
   b. Select **Base-64 encoded X.509 (.CER)**.
   c. Click **Next**.
   d. Click **Browse**.

      In the **Save As** window, browse to the location where certificates are stored and enter a name for the certificate. Ensure that the file type is Base64 Encoded X.509. Then click **Save**.

   e. Click **Next**.
   f. Click **Back** if you must make changes, or click **Finish**.
6. After you receive a message that the import was successful, close the windows of the dialog box.

In Websense Content Manager

1. Navigate to the **Configure > SSL > Certificates > Add Root CA** page.
2. Click **Browse** and navigate to the location where certificates are stored. This is the location in Step 5.
3. Select the certificate and click **Open**.
4. Click **Add Certificate Authority**.

You can confirm the successful import by navigating to the **Configure** > **SSL** > **Certificates** > **Certificate Authorities** page, and checking that the Certificate Authority is listed there.

Using reports

You can access real-time data from both Investigative Reports and Presentation Reports. Note the following important differences between standard reports and reports that document real-time scanning.

The Websense Web filtering software offers several options for reducing the size of the Log Database as it relates to standard Web filtering activity:

- Visits - Enable this option to log only one record for each Web site requested.
- Consolidation - Enable this option to combine into a single log record multiple requests with certain common elements.
- Full URL logging - Disable this option to log only the domain name (www.domain.com) for each request, and not the path to the specific page in the domain (\products\productA).
- Selective category logging - Use this feature to limit logging to selected categories that are crucial for your organization.

The real-time scanning features are only partially bound by these settings. When real-time scanning analyzes a Web request, it creates 2 separate log records.

- Web filter records, which take advantage of any size reduction settings that have been implemented, and are available for all Web filter reports.
- Real-time records, which ignore most size reduction settings. Every separate hit is logged, requests to all categories are logged, and no records are consolidated. A real-time record is generated regardless of whether the site is blocked or permitted as a result of real-time scanning.

If you have enabled any size reduction settings, the numbers reported on real-time reports may not match the numbers reported on Web Filter reports, when the report is configured for the same user, time period, categories, and so forth.

For example, if you are logging visits for Web filtering, and a user requests a site be analyzed by real-time scanning features, that request appears in the Web Filter reports as one visit, but may appear as multiple hits on real-time reports. If you require comparable data for Web Filter and Security Gateway, you must disable the Log Database size reduction settings.

Investigative reports

1. Select **Investigative Reports** from the Main tab.
2. At the top of the screen, select **Names** to display user names in the reports, or select **Anonymous** so that user information is not displayed in the report.
3. In the **Internet Use by** drop-down list, select **Action**.

4. From the choices on the **View** bar, select a date range for the report.
5. Select any real-time action, for example, **Category blocked real time**.

   The setting for **Internet Use by** determines the report topics that are available.
6. Select a category.

   You can continue to click entries for additional details.
7. Click **Hits** for detailed information.

You can export the report into PDF or Excel format using the icons just below the help icon on the right.

Presentation reports

NOTE

Real-time security threats are not included in the real-time categorization reports. See *Real-time security threats*, page 14 for details on creating real-time security reports.

Real-time categorization

1. Select **Presentation Reports**.
2. Expand any one of the headings, such as **Internet Activity**.
3. Select a report, such as, **Summary of Destinations by User**.
4. Click **Copy** to make a copy of the default report.

   This ensures that you have the original report format available.
5. Select the title of the copied report, and then click **Edit Report Filter**.

   The title of the copied report is followed by a number in brackets, such as **Summary of Destinations by User [1]**.
6. Click **Actions** at the top of the page.
7. Expand both the **Permitted** and **Blocked** actions. Depending on the topic of the report, some reports may contain either **Permitted** or **Blocked**, rather than both selections.
8. Select the real-time actions (you may need to scroll down to see them), and click the > button to move them to the Selected pane.
9. Click **Options** at the top of the page.
10. Provide the information requested on this page. It is recommended that you include “Real Time” in the title of the report and in the catalog name for the report.
11. Click **Next**.
12. Click **Save and Run**, and the click **Finish** on the Confirm page.
13. Select the date range and format, and then click **Run**.
14. Indicate if you want to open or save the report. If you are saving the report, indicate the location.

Real-time security threats

When you select Presentation Reports, the Real-time security threat reports are all listed under the Real-Time Security Threats heading.

1. Select **Presentation Reports**.
2. Expand **Real-Time Security Threats**.
3. Select a report, such as **Blocked Downloads by Security Threat**. See *Titles of real-time reports* for a listing of the real-time reports.
4. Click **Run**.
5. Select the date range and format, and then click **Run**.
6. Indicate if you want to open or save the report. If you are saving the report, indicate the location.

Further assistance

Create a support request on the Web site at:

www.websense.com/support/

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

Location	Contact information
North America	+1-858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200
Latin America and Caribbean	+1-858-458-2940

For telephone requests, please have ready:

- Websense subscription key
- Access to Websense Manager

- Access to the machine running Filtering Service, the machine running reporting tools, and the database server (Microsoft SQL Server or MSDE)
- Permission to access the Websense Log Database
- Access to the machines running Websense Content Gateway
- Specifications of the machines running Websense Content Gateway
- Familiarity with your network's architecture, or access to a specialist
- Specifications of machines running Filtering Service and Websense Manager
- A list of other applications running on the Filtering Service machine

Subscription agreement

IMPORTANT - THIS SOFTWARE IS PROVIDED ONLY ON THE CONDITION THAT THE SUBSCRIBER (REFERRED TO IN THIS AGREEMENT AS "SUBSCRIBER") AGREES TO THE TERMS AND CONDITIONS SET FORTH IN THE FOLLOWING LEGAL AGREEMENT BY WEBSENSE, INC. AND/OR ONE OF ITS SUBSIDIARIES (REFERRED TO IN THIS AGREEMENT AS "WEBSENSE"). READ THIS AGREEMENT CAREFULLY BEFORE ACCEPTING IT. BY CLICKING ON THE "I AGREE" BUTTON BELOW OR BY USING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND UNDERSTAND IT, AND YOU, ON BEHALF OF YOURSELF OR THE SUBSCRIBER, IF THE SUBSCRIBER IS A BUSINESS, AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. Subscription and Grant of Right to Use

Subject to the terms and conditions set out in this Agreement, Websense agrees to provide the Subscriber the subscription services ("Subscription") as described in the purchase commitment mutually agreed upon between the parties ("Order"). Websense grants to the Subscriber as part of the Subscription a non-exclusive, nontransferable right to use certain proprietary software applications ("Software"), proprietary database(s) of URL addresses, applications and other valuable information ("Databases"), changes to the content of the Databases ("Database Updates") and certain modifications or revisions to the Software ("Software Upgrades"), together with applicable documentation and the accompanying media, if any, (collectively, the "Products"). The Products are provided for the number of Seats or servers for use in Subscriber's own internal business operations (not for the benefit of any other person or entity) for the time period set forth herein or in the applicable Order ("Subscription Term"), provided the Subscriber has and continues to pay the applicable fees for the Products ("Subscription Fees"). Subject to compliance with the terms of this Agreement, Subscriber may relocate or transfer the Product for use on a different server within its location. All fees paid for the Products are nonrefundable. "Seat" means each computer, electronic appliance or device that is authorized to access or use the Products, directly or indirectly. Subscriber may exceed the number of ordered Seats only upon payment of additional Subscription Fees. Websense may, at any time, audit the use of the Products remotely or, upon reasonable notice, at the Subscriber's site. Unless specifically authorized in writing in advance by Websense, the Subscriber may not rent, lease or timeshare the Products or provide subscription services for the Products or permit others to do so. Any source code provided to the Subscriber by Websense is subject to the terms of this Agreement. Subject to the terms of this Agreement, the Subscriber may allow its agents and independent contractors to use the Products solely for the benefit of the Subscriber; provided, however the Subscriber remains responsible for any breach of this Agreement. Any other use of the Products by any person, business, corporation, government organization or any other entity is strictly forbidden and is a violation of this Agreement. Evaluation copies of the Products are provided for use by the Subscriber only for evaluation purposes to facilitate Subscriber's subscription decision for up to thirty (30) days unless otherwise authorized in writing by Websense. At the end of such thirty (30) day period, the Subscriber must pay the applicable Subscription Fees or this Agreement will automatically terminate and the Subscriber must comply with the terms of Section 7 below.

2. Technical Support

Websense provides its standard technical support for Subscriptions to Products pursuant to the terms of this Agreement. Enhanced support offerings and services are available for additional cost and are also subject to the terms of this Agreement. As part of its standard technical support, WEBSENSE regularly makes available Database Updates and Software Upgrades. WEBSENSE may require Subscriber to install Software Upgrades up to and including the latest release. Database Updates and Software Upgrades will be provided to Subscriber only if Subscriber has paid the appropriate Subscription Fee for Subscriber's Seats and/or Subscriber's servers.

3. Intellectual Property Rights

The Products and all intellectual property rights therein and related thereto are the sole and exclusive property of Websense and any third party from whom Websense has licensed software for incorporation in or distribution with the Products. All right, title and interest in and to the Products and any modifications, translations, or derivatives thereof, even if unauthorized, and all applicable rights in patents, copyrights, trade secrets, trademarks and all intellectual property rights in the same shall remain exclusively with Websense and its licensors. The Products provided hereunder are valuable, proprietary, and unique, and Subscriber agrees to be bound by and observe the proprietary nature thereof. The Products contain material that is protected by patent, copyright and trade secret law, and by international treaty provisions. The Subscriber may make a sufficient number of copies of the Software for its authorized use and make one (1) copy of the Software for backup purposes only. The Subscriber may not remove any proprietary notice of Websense or any third party from any copy of the Products. All rights not granted to the Subscriber in this Agreement are reserved to Websense. No ownership of the Products passes to the Subscriber. Websense may make changes to the Products at any time without notice. Except as otherwise expressly provided, Websense grants no express or implied right under Websense patents, copyrights, trademarks, or other intellectual property rights.

4. Protection and Restrictions

The Subscriber agrees to take all reasonable steps to safeguard the Products to ensure that no unauthorized person shall have access thereto and that no unauthorized copy, publication, disclosure or distribution, in whole or in part, in any form shall be made. The Subscriber acknowledges that the Products contain valuable, confidential information and trade secrets and that unauthorized use and/or copying is harmful to Websense. The Subscriber may not directly or indirectly transfer, assign, publish, display, disclose, rent, lease, modify, loan, distribute, or create derivative works based on the Products or any part thereof. The Subscriber may not reverse engineer (except as required by law for interoperability), decompile, translate, adapt, or disassemble the Products, nor shall the Subscriber attempt to create the source code from the object code for the Software. Any third party software included in the Products may only be used in conjunction with the Products, and not independently from the Products. Subscriber may not, and shall not allow third parties to, publish, distribute or disclose the results of any benchmark tests performed on the Products without Websense's prior written approval. Subscriber represents and warrants that it will comply with all laws, rules and regulations which apply to its use of the Products. Subscriber further represents and warrants that the Products will not be used to filter, screen, manage or censor Internet content for consumers without (a) permission from the affected consumers and (b) Websense's express prior written approval which may be withheld in Websense's sole and absolute discretion.

5. Limited Warranty

For the term of the Subscription, Websense warrants that the Products will operate in substantial conformance with the then current Websense published documentation under normal use. Notwithstanding the previous sentence, Websense does not warrant that: (i) the Products will be free of defects; (ii) the Products will satisfy all of the Subscriber's requirements; (iii) the Products will operate without interruption or error; (iv) the Products will always locate or block access to or transmission of all desired addresses, applications and/or files; (v) the Products will identify every transmission or file that should potentially be located or blocked; (vi) addresses and files contained in the Products will be appropriately categorized; or (vii) that the algorithms used in the Products will be complete or accurate. Websense shall use reasonable efforts to remedy any significant non-conformance in the Products which is reported to Websense that Websense can reasonably identify and confirm. Websense or its representative will repair or replace any such non-conforming or defective Products, or refund the Subscription Fees paid for the then current term, in Websense' discretion. This paragraph sets forth the sole and exclusive remedy and Websense' exclusive liability for any breach of warranty or other duty related to the Products. Any unauthorized modification of the Products, tampering with the Products, use of the Products inconsistent with the accompanying documentation, or related breach of this Agreement shall void the aforementioned warranty. EXCEPT AS EXPLICITLY SET FORTH HEREIN AND TO THE EXTENT ALLOWED BY LAW, THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE PRODUCTS.

6. Limitation of Liability

TO THE FULLEST EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES WILL WEBSENSE, ITS AFFILIATES, ITS LICENSORS OR RESELLERS BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, PUNITIVE OR INCIDENTAL DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE, ARISING OUT OF OR RELATED TO THIS AGREEMENT INCLUDING, BUT NOT LIMITED TO CLAIMS FOR LOSS OF DATA, GOODWILL, OPPORTUNITY, REVENUE, PROFITS, OR USE OF THE PRODUCTS, INTERRUPTION IN USE OR AVAILABILITY OF DATA, STOPPAGE OF OTHER WORK OR IMPAIRMENT OF OTHER ASSETS, PRIVACY, ACCESS TO OR USE OF ANY ADDRESSES OR FILES THAT SHOULD HAVE BEEN LOCATED OR BLOCKED, NEGLIGENCE, BREACH OF CONTRACT, TORT OR OTHERWISE AND THIRD PARTY CLAIMS, EVEN IF WEBSENSE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL WEBSENSE'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT ACTUALLY PAID BY THE SUBSCRIBER TO WEBSENSE FOR THE APPLICABLE PRODUCTS OVER THE ONE YEAR PERIOD PRIOR TO THE EVENT OUT OF WHICH THE CLAIM AROSE FOR THE PRODUCTS THAT DIRECTLY CAUSED THE LIABILITY.

7. Termination

This Agreement is effective until the end of the Subscription Term for such use as is authorized, or until terminated by either party. The Subscriber may terminate this Agreement at any time by uninstalling the Software and destroying or returning to Websense all copies of the Products in the Subscriber's possession or under the Subscriber's control. However, Subscriber shall not be entitled to a refund of any prepaid or other fees. Websense may terminate this Agreement if Websense finds that the Subscriber has violated the terms hereof. Upon notification of termination, the Subscriber agrees to cease using and destroy or return to Websense all copies of the Products and to certify in writing that all known copies thereof, including backup copies, have been destroyed. Section 2-7, 9 and 11 shall survive the termination of this Agreement.

8. Government Restricted Rights

The Products are provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in FAR52.227-14 and DFAR252.227-7013 et seq. or its successor. Use of the Products by the Government constitutes acknowledgment of Websense's proprietary rights therein. Contractor or Manufacturer is Websense.

9. Third Party Products

The Products include software products licensed from third parties. Such third parties have no obligations or liability to the Subscriber under this Agreement but are third party beneficiaries of this Agreement.

10. Export

Certain Products provided under the Agreement are subject to export controls administered by the United States and other countries. Export or diversion contrary to U.S. law is prohibited. U.S. law prohibits export or re-export of the software or technology to Cuba, Iran, North Korea, Sudan and Syria or to a resident or national of those countries. It also prohibits export or re-export of the software or technology to any person or entity on the U.S. Department of Commerce Denied Persons List, Entities List or Unverified List; the U.S. Department of State Debarred List; or any of the lists administered by the U.S. Department of Treasury, including lists of Specially Designated Nationals, Specially Designated Terrorists or Specially Designated Narcotics Traffickers. U.S. law also prohibits use of the software or technology with chemical, biological or nuclear weapons, or with missiles. Subscriber warrants that it is not located in, or a resident or national, of any such country; that it is not on any such list; that it will not use the software or technology for any such use; and that it will otherwise comply with export controls.

11. General

Websense may periodically send the Subscriber messages of an informational or advertising nature via email. The Subscriber may choose to "opt-out" of receiving these messages by sending an email to optoutlegal@websense.com requesting the opt-out. The Subscriber acknowledges and agrees that by sending such email and "opting out" it will not receive emails containing messages concerning upgrades and enhancements to Products. However, Websense may still send emails of a technical nature. Subscriber acknowledges that Websense may use Subscriber's company name only in a list of Websense customers. The Subscriber may not transfer any of the Subscriber's rights to use the Products or assign this Agreement to another person or entity, without first obtaining prior written approval from Websense. Notices sent to Websense shall be sent to the attention of the General Counsel at 10240 Sorrento Valley Road, San Diego, CA 92121 USA. Any dispute arising out of or relating to this Agreement or the breach thereof shall be governed by the laws of the State of California, USA for all claims arising in or related to the United States, Canada, or Mexico and Dublin, Ireland for all other claims, In either case, without regard to or application of choice of laws, rules or principles. Both parties herby consent to the exclusive jurisdiction of the state and federal courts in San Diego, California, USA, for all claims arising in or related to the United States, Canada or Mexico and Dublin, Ireland for all other claims. Both parties expressly waive any objections or defense based upon lack of personal jurisdiction or venue. This Agreement shall constitute the entire Agreement between the parties hereto. Any waiver or modification of this Agreement shall only be effective if it is in writing and signed by both parties. If any part of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this Agreement shall be interpreted so as to reasonably affect the intention of the parties. Websense is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Websense.

Copyright and Trademarks

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 6,606,659 and 6,947,985 and other patents pending.

Every effort has been made to ensure the accuracy of this document. 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.

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.

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.