v7.5 Release Notes for Websense Content Gateway

Topic 600016 / Updated: 17-Jun-2010

Applies To:	Websense Content Gateway 7.5 Websense Web Security Gateway 7.5 Websense Web Security Gateway Anywhere 7.5

Use the Release Notes to find information about what's new and improved in Websense Content Gateway Version 7.5.

New features in version 7.5

Topic 600017 / Updated: 17-Jun-2010

Applies To:	Websense Content Gateway 7.5 Websense Web Security Gateway 7.5 Websense Web Security Gateway Anywhere 7.5

Web Security Gateway Anywhere: Data Security policy engine

Web Security Gateway Anywhere

Supported platforms

Websense Content Gateway version 7.5 is supported on:

- Red Hat Enterprise Linux 5, update 3 and update 4, base or Advanced Platform (32-bit only)

  Although not certified, Websense, Inc. provides “best effort” support for newer versions of Red Hat Enterprise Linux. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion unless the issue is deemed a Red Hat Enterprise Linux-specific issue, at which point you must contact Red Hat directly for assistance.

> **Note**
> At the time of version 7.5.0 release, this known issue is documented: *Installation on Red Hat Enterprise Linux 5, update 5 does not install ARM*. The problem is easily worked around by following the procedure described in the Knowledge Base article titled “Installing the ARM on Red Hat Enterprise Linux 5, update 5”.

> **Note**
> Websense recommends that systems hosting Content Gateway be registered with **Red Hat Network** and kept up-to-date with the latest security patches.

Content Gateway is designed to run on a dedicated machine and is not guaranteed to be compatible with other server applications installed on the same machine.

A direct upgrade from a prior version of Content Gateway to version 7.5 is not possible. To migrate to Content Gateway version 7.5, update your operating system to the required version or obtain a machine running the required operating system. Then, install version 7.5 as a new installation.

For a complete description of platform requirements, see *Hardware* and *Software*.

Client authentication

Authentication realms

In networks with multiple authentication realms, rules can be defined to direct sets of IP addresses to distinct authentication servers (also known as domain controllers). Configuration is performed in the Content Gateway Manager. Rules are stored in the **auth.config** file.

Multiple authentication realms are supported for NTLM and LDAP. Separate rules must be created for NTLM and LDAP. Only one authentication method can be active at a time and only rules for that method are applied. Rules are applied first-match, top down in the list.

For more information, see the section titled *Multiple Authentication Realms* in Websense Content Gateway Online Help.

Additional authentication enhancements

- Transparent authentication configuration settings now have a separate tab in the Content Gateway Manager. Go to **Configure > Security > Access Control > Transparent Proxy Authentication**.
- Filtering configuration rules, stored in **filter.config**, can be written to match User-Agent header data. This allows administrators to write rules for applications that can be identified by User-Agent header data. For example, use a filtering rule to:
  - Allow applications that don't properly handle authentication challenges to bypass authentication
  - Block certain client-based applications from accessing the Internet
- When **NTLM** authentication is configured, the **Fail Open** option can be used to allow requests to proceed when authentication fails due to no response from the domain controller, or because of malformed messages from the client.

  Fail Open provides excellent results when Web filtering is used with the proxy and an XID agent is configured. Then, if NTLM authentication fails, the requester can still be identified by the XID agent and the correct policy applied.

  Fail Open is enabled by default.

  (NTLM Fail Open was introduced into the 7.1 series of releases beginning with 7.1.4.)

Split DNS

Content Gateway can now be configured to use specific DNS servers to meet specific network access and network security requirements. For example, you can configure Content Gateway to use one set of DNS servers to resolve host names on your internal network, while allowing DNS servers outside the firewall to resolve hosts on the Internet. This maintains the security of your intranet, while continuing to provide direct access to sites outside your organization. For more information, see the section titled "Using the Split DNS option" in Websense Content Gateway Online Help.

Proxy chaining

Parent proxy configuration options

In Content Gateway Manager, several configuration options have been added for when Content Gateway is the child in a proxy chain. Options are set on the **Configure > Content Routing > Hierarchies > Parenting** tab.

New options include:

- Bypass the parent when a request is not cacheable
- Bypass the parent for tunneled requests
- Bypass the parent when traffic is HTTPS

HTTPS traffic in a proxy chain

Routing SSL traffic in a proxy chain involves the same parent proxy configuration settings used with other proxy-chained traffic. You identify the ports on which HTTPS requests should be decrypted and policy applied when SSL is enabled in **Configure > Protocols > HTTP > HTTPS Ports**. Parent proxy rules established in **parent.config** for HTTPS traffic (destination port 443) determine the next proxy in the chain for that traffic.

Tunneled traffic

Traffic on specified ports may be allowed to tunnel to an origin server. Content Gateway allows tunneling to the ports listed in **Configure > Protocols > HTTP > Tunnel Ports**, when SSL is not enabled. When SSL is enabled, traffic to any tunneled port that is also listed in the HTTPS Ports field is not tunneled, but is decrypted and filtering policy is applied.

HTTP privacy options

In Content Manager, on the **Configure > Protocols > HTTP > Privacy** tab, you can now set two common privacy options (set in records.config in prior versions):

- Select **Via** to insert a Via header into the outgoing request. Enabled by default.
- Select **X-Forwarded-For** to insert an X-Forwarded-For header into the outgoing request. Disabled by default.

Web Security Gateway: Scanning features

Scanning feature enhancements are described in more detail in the Websense Web Security/Websense Web Filtering Release Notes. New capabilities include:

- Embedded URL link analysis: During Content Categorization, optional analysis of URL links embedded in the page contribute to categorization of the requested page.
- Content Categorization sensitivity control: A Content Categorization sensitivity control allows the administrator to increase or decrease the sensitivity of the analysis that classifies content.
- Tunneled Protocol Detection: Tunneled Protocol Detection detects protocols tunneling through the proxy using HTTP or HTTPS. This capability augments Network Agent in protocol detection and policy enforcement. Signatures added to the database for tunneled protocol detection allow for the filtering of the Google Wave and Gmail Chat application protocols. These protocols are labeled "WSG only" in the Web Security Manager Protocols window. (Note that Network Agent can no longer filter the Gmail Chat protocol.) See the Knowledge Base article titled *Google Wave and Gmail Chat protocol signatures* for more information.
- Scanning of rich Internet applications: Security Threat scanning of rich Internet applications, such as Flash, to detect and block malicious content.
- Outbound content scanning: Outbound content scanning detects and blocks bot and spyware phone home traffic, and other malicious content.
- Web 2.0 History charts and Presentation reports

Web Security Gateway: SSL decryption bypass

To support organizations using SSL Manager to manage encrypted traffic, and who do not want to decrypt HTTPS sessions that users establish with sensitive sites, such as personal banking or health provider sites, administrators can now specify categories of sites that will bypass SSL decryption. A list of hostnames or IP addresses for which SSL decryption is **not** performed can also be maintained. These capabilities are configured on the **Scanning > SSL Decryption Bypass** page in TRITON - Web Security (Web Security Manager).

Web Security Gateway Anywhere: Data Security policy engine

When Content Gateway version 7.5 is installed, a copy of the Websense Data Security policy engine is also installed (it is disabled until registered). When the Websense Data Security Manager is installed and configured (on a separate system), and then registered with Content Gateway, the combination provides data loss prevention (DLP) over Web channels such as HTTP, HTTPS, FTP, and FTP over HTTP. For a detailed description of Websense Web Security Gateway Anywhere data loss prevention, see the Data Security Deployment Guide. For step-by-step Data Security registration instructions, see the section titled *Working with Websense Data Security* in the Websense Content Gateway Online Help.

As in prior releases of Content Gateway, Websense Data Security Suite is also supported over ICAP.

Web Security Gateway Anywhere

Websense Web Security Gateway Anywhere™ is a Web security solution designed for distributed enterprises with one or more branch offices and multiple remote users.

Web Security Gateway Anywhere offers an alternative to pure service-based or pure appliance-based solutions. Rather than choosing between an all in-the-cloud or all on-premises Web filtering solution, you can deploy a blended solution that encompasses the best of both worlds, and you can manage it from a single user interface—the TRITON™ Unified Security Center.

Web Security Gateway Anywhere includes Websense Web Security and Websense Content Gateway as well as hybrid Web and DLP features. For complete information, see the Websense Web Security Gateway Anywhere Getting Started Guide.

Within the TRITON Unified Security Center, the names of several components are changed.

TRITON Unified Security Center name	Version 7.1 name
TRITON - Web Security	Websense Manager
TRITON - Data Security	DSS Manager
***Content Gateway Manager - *cannot be accessed within TRITON Unified Security Center in version 7.5**	Websense Content Manager

Corrected in version 7.5

Topic 600017 / Updated: 17-Jun-2010

Applies To:	Websense Content Gateway 7.5 Websense Web Security Gateway 7.5 Websense Web Security Gateway Anywhere 7.5

The following problems have been corrected.

- After creating a very large list of access configuration rules (>300), clicking Apply to save the rules resulted in an empty list.
- In a proxy chain in which Websense Content Gateway was the downstream proxy, the "No DNS and Just Forward to Parent" option was enabled, the proxy handled explicit traffic, and the traffic was HTTPS, the proxy would return a Server Hangup error.

- When the proxy handled explicit traffic, ARM was enabled, and NTLM authentication was configured, NTLM authentication was not always performed when Internet Explorer was the browser.
- Sometimes when Websense Content Gateway connected to the Database Download Server, the connection timed out.
- When Websense Content Gateway was connected to an origin server using HTTP 1.0, the connection was not closed until the connection with the server timed out.
- When Websense Content Gateway serviced transparent traffic, HTTP 1.0 clients could not connect to HTTPS sites.
- Microsoft Windows Update failed when sent through the proxy.
- When hosted on an HTTPS site, some CRLs (certificate revocation lists) would not download through the proxy.
- When SSL was enabled with the certificate validation option enabled and the client certificate create incident option enabled, sometimes no incident was created when an HTTPS site requested a client certificate.
- Caching was enabled even though it had been disabled during installation.
- Enabling both SOCKS and NTLM caused the proxy to reset.
- Upgrading failed if /tmp became full.
- Snapshots were not preserved across upgrades.

Operation tips

Topic 600018 / Updated: 17-Jun-2010

Applies To:	Websense Content Gateway 7.5 Websense Web Security Gateway 7.5 Websense Web Security Gateway Anywhere 7.5

Hardware

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.
	• 147 GB for caching
	If caching will not be used, this disk is not required.
	The caching disk:
	  • Should have minimum size of 2 GB, maximum 147 GB for optimal performance
	  • Must be a raw disk, not a mounted file system
	  • Must be dedicated
	  • Must *not* be part of a software RAID
	  • For best performance, use a 10K RPM SAS disk on a controller that has at least 64MB of write-through cache.

Network Interfaces	2

To support transparent proxy deployments:

Router	WCCP v1 routers support redirection of HTTP only. If your deployment requires additional protocols, such as HTTPS, your router must support WCCP v2. A Cisco router must run IOS 12.2 or later. The clients, the destination Web server, and Websense Content Gateway must reside on different subnets.
—or—	
Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). Websense Content Gateway must be Layer 2 adjacent to the switch. The switch must be able to rewrite the destination MAC address of frames traversing the switch. The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Software

Linux operating system:

- Red Hat Enterprise Linux 5, update 3 and update 4, base or Advanced Platform (32-bit only)

  Although not certified, Websense, Inc. provides “best effort” support for newer versions of Red Hat Enterprise Linux. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion unless the issue is deemed a Red Hat Enterprise Linux-specific issue, at which point you must contact Red Hat directly for assistance.

  - Only kernels shipped with the above Linux versions are supported by Websense Content Gateway. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

    ```
    /bin/uname -r
    ```

    

    Important

    If SELinux is enabled, disable it before installing Websense Content Gateway.

  - PAE (Physical Address Extension)-enabled kernel required
    - By default, Red Hat Enterprise Linux 5, update 3 and later has PAE enabled. If you are running the non-PAE kernel, reboot with the PAE-enabled kernel before installing Websense Content Gateway.
  - RPM compat-libstdc++-33-3.2.3-47.3.i386.rpm (or higher version of this package)

- To display a list of RPMs installed on your system with the string “compat-libstdc” in their name, enter the command:

  ```
  rpm -qa |grep compat-libstdc
  ```

- GNU C library (glibc) version 2.5-42
  - Note that Red Hat Enterprise Linux 5, update 3 ships with glibc version 2.5-34. Be sure to update it to version 2.5-42.
  - Example command to update this library (running as `root`): `yum update glibc`.

Websense Web filtering products:

- Version 7.5

> **Important**
> Websense filtering software must be installed prior to Websense Content Gateway. When the filtering software is installed, Content Gateway must be specified as the integration product.

Websense Data Security:

- On-box policy engine: Version 7.5
- ICAP: Any 7.x version

When Content Gateway is used with Websense Data Security only (no Web filtering) the order of installation does not matter.

Supported browsers:

- Content Gateway is configured and maintained with a Web-based user interface called the Content Gateway Manager. Supported browsers include:
  - Internet Explorer 7 and 8
  - Mozilla Firefox 3

Cache size

Cache size should be restricted to 147 GB. This size provides optimal resource utilization while also providing an excellent end-user experience. Because today’s Internet sites are often composed of dynamic, uncacheable content, caching is a less significant factor in the end user’s Web browsing experience.

Software installation cannot be completed without Internet connectivity

It is recommended that the Content Gateway host computer have Internet connectivity before starting the software installation procedure. The software will install without Internet connectivity, but Websense license keys (and licensed features) cannot be validated until Internet connectivity is available.

Proxy ‘admin’ password restrictions

The password you enter for the Content Gateway administrator during installation (default name: admin) must be 15 characters or fewer.

To create a strong password (recommended), use 8 or more characters, with at least 1 each of the following: capital letter, lower-case letter, number, special character.

The password **cannot** contain the following special characters:

- space
- $ (dollar symbol)
- : (colon)
- ‘ (backtick; typically shares a key with tilde, ~)
- \ (backslash)
- “ (double-quote)

Installation file paths

During installation, 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 quotation marks or other special characters in the path name, the installation itself may be unable to complete successfully.

Security recommendations

Websense recommendations for the physical and operational security of your proxy server are included in the Websense Content Gateway Installation Guide and in 2

Knowledge Base articles: *Proxy security and hardening recommendations*, and *Configuring IPTables for Websense Content Gateway.*

Port configuration

A full deployment of Content Gateway requires that several ports be open. See the Websense Content Gateway Installation Guide for information about open ports and reassignment ports, if necessary.

Configuring your router

If your site is running Content Gateway in a transparent proxy deployment and you intend to proxy HTTPS or FTP traffic, you must use the SSL Manager and you must configure your router to support WCCP v2. See Websense Content Gateway Online Help.

Configuring multiple ports for the HTTP WCCP v2 service group

When using WCCP v2 routers to support transparent proxy traffic, administrators can configure multiple ports for the HTTP service group in **records.config**.

Configuration Variable Data Type	Default Value	Description
`proxy.config.wccp2.HTTP_svc_port` `STRING`	`80`	Specifies multiple HTTP ports. Ports are given in a comma-separated list, i.e.: 80,81,82,99 To use this variable you must add it to **records.config**.

Virtual IP address must not match any real IP address

When configuring the Virtual IP feature, make sure that the Virtual IP addresses do not conflict with any existing IP addresses assigned to the system.

Email address for receiving proxy alarms

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

Email addresses for alarm notifications cannot be 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 ***<Install_Dir>*/config/records.config**
(default location: /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
```

Restart the proxy after protocol settings change

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

Reverse proxy

Content Gateway **does not** function as a reverse proxy.

Reverse DNS

In prior versions of Content Gateway, by default the proxy performed reverse DNS lookup whenever a URL contained an IP address and there was a rule in **filter.config**, **cache.config**, or **parent.config**. In version 7.5, reverse DNS lookup is disabled by default. If you have rules in **filter.config**, **cache.config**, or **parent.config** that are based on destination hostname or domain name, you need to enable reverse DNS lookup on the **Configuration > Protocols > HTTP > General** tab.

Registering with the Data Security Management Server

When Content Gateway is **not** located on a V-Series appliance (is installed on a separate Linux server):

- Registration with Data Security Management Server requires that the Content Gateway host system have an IPv4 address assigned to the eth0 network interface. After registration, the IP address may move to another network interface on the host; however, that IP address is used for data security configuration deployment and must be available as long as the two modules are registered.

- The Content Gateway host system must have a unique fully qualified domain name (FQDN) specified in the **/etc/hosts** file. (This is done automatically as part of the setup process on V-Series appliances.)

The process of registering Content Gateway with the Data Security Management Server is described in detail in the Websense Content Gateway Online Help.

Browser limitations

Not all Web browsers support all authentication modes.

The browsers that provide the most complete support are: **Internet Explorer 7 and 8**, and **Mozilla Firefox 2 and 3**. Other browsers have limitations, especially when the configured mode is NTLM (Integrated Windows Authentication/Single Sign-on). Transparent NTLM authentication is **not** supported by Google Chrome, Opera or Windows Safari.

<table>
<tr><th rowspan="2">Browser</th><th colspan="2">When the client request originates on a different domain than the proxy (prompt for credentials)</th><th colspan="2">When the client request originates on the same domain as the proxy (transparent authentication; no prompt)</th></tr>
<tr><th>HTTP</th><th>HTTPS</th><th>HTTP</th><th>HTTPS</th></tr>
<tr><td>Internet Explorer 7 and 8</td><td colspan="4">Full support</td></tr>
<tr><td>Mozilla Firefox 2 and 3</td><td colspan="4">Full support</td></tr>
<tr><td rowspan="2">Google Chrome</td><td colspan="4">NTLM transparent authentication: Not supported.
The user is prompted for credentials.</td></tr>
<tr><td colspan="4">Explicit authentication: Supported.
The user is prompted for credentials.</td></tr>
<tr><td rowspan="3">Opera 10</td><td colspan="4">NTLM transparent authentication: Not supported.
The user is prompted for credentials.</td></tr>
<tr><td colspan="4">Explicit authentication:</td></tr>
<tr><td>Supported.
The user is prompted for credentials.</td><td>Not supported.</td><td>Supported.
The user is prompted for credentials.</td><td>Not supported.</td></tr>
</table>

Browser	When the client request originates on a **different domain** than the proxy (prompt for credentials)		When the client request originates on the **same domain** as the proxy (transparent authentication; no prompt)	
	HTTP	**HTTPS**	**HTTP**	**HTTPS**
Windows Safari 4	NTLM transparent authentication: Not supported. The user is prompted for credentials.			
	Explicit authentication:			
	Supported. The user is prompted for credentials.	Supported. When LDAP authentication is configured, the user is prompted twice for credentials.	Supported. The user is prompted for credentials.	Supported. When LDAP authentication is configured, the user is prompted twice for credentials.

When prompted for credentials, if the user does not enter a domain name, a “session timeout” error can result, or the user may be re-prompted.

Mozilla Firefox users browsing from the same domain as the proxy may sometimes be prompted multiple times for authentication. The user should configure the browser as follows:

1. Open Firefox and enter “about:config” in the location bar.
2. Click the “I will be careful I promise” button.
3. In the **Filter** entry field enter “ntlm”.
4. Double click “network.automatic-ntlm-auth.trusted-uris” and enter: http://<*proxy_name*>:8080

   For example: http://XYZProxy1:8080
5. Click OK and close and reopen the browser.

Active Directory 2008 with NTLM

As in past version 7-series releases, support is provided for Windows Active Directory 2008 with NTLMv1.

If you plan to authenticate users with NTLM and Active Directory 2008, you must use port 445 or turn on the Windows Computer Browser service on the Active Directory servers. Also, the Windows **Network Security: LAN Manager Authentication level** must be set to **Send NTLM response only**. See your Windows Server 2008 documentation for details.

To enable the Windows Computer Browser service, perform the following procedure on each machine running Windows Server 2008 and Active Directory:

1. Make sure that Windows Network File Sharing is enabled.

a. Go to **Start > Network > Network and Sharing Center**.
b. In the **Sharing and Discovery** section, set **File Sharing** to **On**.

2. Go to **Control Panel > Administrative Tools > Services**.
3. Double-click **Computer Browser** to open the Properties dialog box.
4. Set the **Startup type** to **Automatic**.
5. Click **Start**.
6. Click **OK** to save your changes and close the Services dialog box.

NTLM load balancing and failover

When NTLM is configured and multiple domain controllers are specified, even if load balancing is *disabled*, when the load on the primary domain controller reaches the maximum number of connections allowed, new requests are sent to a secondary domain controller as a short-term failover provision, until such time that the primary domain controller can accept new connections.

Accessing Intranet sites in an explicit proxy deployment

If your clients cannot access your Intranet sites, 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.

Known issues

Topic 600020 / Updated: 17-Jun-2010

Applies To:	Websense Content Gateway 7.5 Websense Web Security Gateway 7.5 Websense Web Security Gateway Anywhere 7.5

A list of known issues in this release of Websense Content Gateway is available to customers with a current MyWebsense account.

If you are not currently logged in to MyWebsense, the link above takes you to a login prompt. Log in to view the list.