v7.6 Release Notes for Websense Content Gateway

Topic 60025 / Updated: 6-May-2011

Applies To:	Websense® Content Gateway 7.6 Websense Web Security Gateway 7.6 Websense Web Security Gateway Anywhere 7.6

These Release Notes describe new features, best practices, corrections, and known issues in Websense Content Gateway version 7.6.

For detailed information about other Websense components, see their Release Notes:

- TRITON™ Unified Security Center
- Websense Web Security
- Websense Data Security
- Websense Email Security Gateway
- Websense V-Series Appliances

For installation instructions, see Installing Websense Content Gateway.

For upgrade instructions, see Upgrading Websense Content Gateway to 7.6.

Important:
In v7.6, in explicit proxy deployments, when HTTPS is enabled, PAC files and browsers must be configured to send HTTPS traffic to Content Gateway on port 8080. The **ipnat.config** rule that was used in previous releases to redirect traffic from 8070 to 8080 has been removed.

Contents

Introducing Websense Content Gateway version 7.6

Topic 60026 / Updated: 6-May-2011

Applies To:	Websense® Content Gateway 7.6 Websense Web Security Gateway 7.6 Websense Web Security Gateway Anywhere 7.6

> **Important**
> For additional information about new and existing features, see Content Gateway Manager online Help.

Supported platforms

Websense Content Gateway version 7.6 is supported on:

- Red Hat Enterprise Linux 5 series, update 3 and greater, 32-bit, base and Advanced Server
- The corresponding CentOS version (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

> **Note**
> Red Hat Enterprise Linux 6 series is **not** supported at this time.

- V-Series appliances

Websense recommends that the Red Hat Enterprise Linux version that will host Content Gateway be updated to the latest patch level before running the v7.6 Content Gateway installer.

Websense also recommends that Red Hat Enterprise Linux systems that host Content Gateway be registered with Red Hat Network and kept up-to-date with the latest security patches. With Websense Content Gateway, you can update packages on your Red Hat Enterprise Linux installations and patch kernels if the underlying kernel upgrade does not change the kernel ABI.

Important

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.

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

Integration with TRITON - Web Security

TRITON - Web Security is the interface to the configuration, administration, and reporting functions of your Websense Web security software. TRITON - Web Security has been enhanced in several ways to work more closely with Content Gateway.

Subscription key:

Content Gateway shares a subscription key with TRITON - Web Security, which Content Gateway now pulls automatically from TRITON - Web Security on

installation and restart. Unless the proxy is stand-alone with Data Security, the subscription key does **not** need to be entered in Content Gateway Manager.

Note

The TRITON - Web Security instance that is used is determined by the Policy Server that is configured. The configured Policy Server IP address is shown in Content Gateway Manager on the **Monitor** > **My Proxy** > **Summary** page when the **More Details** view is selected.

To configure Policy Server:

- On a V-Series appliance, in Appliance Manager go to **Configuration** > **Web Security Components**.
- On a software install, edit **/opt/WCG/websense.ini** and set the value of **PolicyServerIP**. Then stop and start Content Gateway processes:

```
/opt/WCG/WCGAdmin stop
/opt/WCG/WCGAdmin start
```

Registered instances:

One or more Content Gateway nodes can now be registered in the **Settings** > **Content Gateway Access** screen of TRITON - Web Security. Registered nodes provide a link to the Content Gateway Manager logon portal of that node and also display a system health indicator (a green check mark or a red X icon).

System alerts:

A select set of Content Gateway system alerts are now sent to TRITON - Web Security and can be configured with other alerts on the TRITON - Web Security **Settings** > **Alerts** > **System** screen.

Integrated Windows Authentication

Integrated Windows Authentication (IWA) provides a very secure and robust method of authenticating users who all belong to shared-trust, Windows domains (one or many).

Integrated Windows Authentication:

- Uses Kerberos
- Supports Windows Active Directory 2003 and 2008
- Supports NTLM in both explicit and transparent proxy modes
- Supports NTLMv2 with Session Security and NTLMv1 with Session Security
- Supports IE9, 8 & 7, Firefox 4, 3 & 2, Windows Safari 5 & 4, Safari on iPad, Opera 10, and Google Chrome 10, 9, 8, 7, & 6

- Supports UTF-8 user names
- Supports fall back to interactive authentication
- Can be used with *Multiple Realm Authentication*
- Requires that clients be joined to the trusted domain
- Requires that browsers and other proxy clients specify the Fully Qualified Domain Name (FQDN) of Content Gateway as an intranet site or trusted site
- In explicit proxy deployments, browsers must specify the FQDN of Content Gateway

Note

When using Internet Explorer on a Windows XP-based computer, IWA may produce the following error:

```
HTTP Error 401 - Unauthorized: Access is
denied due to invalid credentials.
```

The problem occurs because the workstation is unable to request a Kerberos service ticket if the service SPN is a CNAME record in DNS. The issue is described in detail in this Microsoft knowledge base article:

http://support.microsoft.com/kb/911149

The problem can be corrected for all clients in DNS by changing the FQDN/SPN of Content Gateway from a CNAME record to an A record.

IWA configuration summary:

1. In Content Gateway Manager, enable Integrated Windows Authentication.
2. Join Content Gateway to the Windows domain.
3. If Content Gateway is a transparent proxy, configure Transparent proxy authentication settings (Configure > Security > Access Control > Transparent Proxy Authentication). **Redirect Hostname** is not used with IWA and does not need to be set.
4. Configure the Global Authentication Options.

5. Ensure that all clients are joined to the Windows domain.

Important

Because IWA uses the hostname as a NetBIOS name when registering with Kerberos, the Content Gateway hostname cannot exceed 15 characters (a NetBIOS restriction), or 11 characters on V-Series appliances (V-Series adds 4 characters to the hostname to ensure that the hostname is unique across modules (Web Security, Email Security, etc.)).

Once the join is complete, the hostname cannot be changed without immediately breaking IWA. IWA will not work again until the domain is unjoined and then rejoined with the new hostname.

Multiple Realm Authentication

Multiple realm authentication is for environments that have multiple domains that are essentially isolated for the purposes of user authentication by a lack of mutual inbound and outbound trust relationships. Therefore, users in these domains must be authenticated by a domain controller within their domain. With respect to this feature, these domains are called **realms**.

Multiple realm authentication allows distinct authentication rules to be written for each domain, thereby supporting the ability to use multiple authentication methods (Integrated Windows Authentication, legacy NTLM, LDAP) at the same time. For example, RealmA might be an Active Directory domain for which you want to authenticate users with Integrated Windows Authentication. RealmB might be an LDAP domain for which you must authenticate users with LDAP. This is easy to accomplish with multiple realm authentication.

In explicit proxy environments, authentication rules can be written for traffic inbound on specific ports. This allows for authentication rules that specify the source port, authentication method, and realm.

Note

In multiple realm environments, Content Gateway may authenticate users that Web Security does not know about (are outside User Services primary domain). In these cases, Content Gateway can be configured to send an “alias” name that Web Security does know about. Or, to apply the default policy, send no name. This selection is made in the Advanced Options of each rule you define.

Multiple realm authentication configuration summary:

1. Join all of the Windows domains to be used with Integrated Windows Authentication rules (domains can be added or removed later, but rules cannot be created for a domain that is not joined).
2. If Content Gateway is an explicit proxy and you want to bring in traffic on multiple ports, configure the ports in Content Gateway Manager.
3. If Content Gateway is a transparent proxy, make Transparent proxy authentication settings.
4. Configure the Global authentication options.
5. Create authentication rules.

Multiple ports in explicit deployments

In explicit proxy deployments, you can now specify multiple inbound ports in Content Gateway Manager. Go to **Configure > Protocol > HTTP**. The name of the field is **Secondary HTTP Proxy Server Ports**. (This feature is not applicable to transparent proxy configurations.)

HTTPS URL filtering when not decrypting in transparent proxy deployments

Beginning in version 7.6, Content Gateway performs HTTPS URL filtering in transparent proxy deployments even when SSL Manager is not enabled and HTTPS is not decrypted. This means that for every HTTPS request, a URL lookup is performed and policy is applied. (This has long been a feature of explicit proxy deployments.)

In explicit proxy mode, when SSL Manager is turned off, Content Gateway performs URL filtering based on the Host name in the request. If the site is blocked, Content Gateway serves a block page. Note that some browsers do not support display of the block page.

In transparent proxy mode, when SSL Manager is turned off, Content Gateway performs URL filtering based on the common name present in the certificate from the origin server. If the common name contains wildcards, then filtering is based on the destination IP address (the address to which the client tried to make a connection). If the site is blocked, the connection with the client is dropped; no block page is served.

Expanded support for WCCP v2

Support for transparent interception with WCCP v2-enabled routers and switches has been expanded. Support for WCCP v1 has been deprecated.

Content Gateway supports the following WCCP v2 features:

- Multiple routers in a proxy cluster
- Multiple ports per service group
- Multiple service groups per protocol.
- Dynamic load distribution in a proxy cluster through *assignment method* HASH or MASK, and *weight*
- MD5 password security per service group
- Multicast mode

In a Content Gateway cluster, it is recommended that you **not** enable virtual IP failover in WCCP environments. In a transparent proxy deployment, in the case of a node failure the WCCP protocol handles the reassignment of traffic to the remaining nodes in the cluster. (In an explicit proxy deployment, the Content Gateway virtual IP address feature can be used to provide a failover mechanism whereby clients are configured to send traffic to a pool of virtual IP addresses.)

Content Gateway also supports cache affinity. If a node becomes unavailable and then recovers, the node's cache does not need to be repopulated.

SSL Manager configuration clustering

When the HTTPS feature (SSL Manager) is enabled in a cluster, SSL Manager configuration information can also be propagated around the cluster. However the mechanism is different than that used by other cluster information, and it requires separate configuration.

To configure SSL Manager to propagate configuration information around the cluster, one node is selected as the **primary** node on which all SSL Manager configuration changes are made. The primary is known as the **SSL Manager Configuration Server**. All other nodes are **secondaries**.

- Settings made on the primary are propagated to the secondaries.
- Secondaries periodically poll the primary to see if changes are pending. If changes are pending, each secondary pulls them down.
- If configuration changes are made on a secondary, they are overwritten when the configuration is pulled from the primary.
- Should the primary go down, an alarm is generated and the secondaries continue to operate with their current configuration until the primary returns to service or a new primary is configured.

When SSL Manager clustering is configured, the following configuration settings are propagated:

- The IP address of the primary
- Configure > SSL > Certificates > Certificate Authorities
- Configure > SSL > Certificates > Add Root CA
- Configure > SSL > Certificates > Restore Certificates

- Configure > SSL > Decryption / Encryption: all settings
- Configure > SSL > Validation: all settings
- Configure > SSL > Client Certificates: all settings
- Configure > SSL > Logging: all settings
- Configure > SSL > Internal Root CA > Import Root CA
- Configure > SSL > Internal Root CA > Create Root CA
- Dynamically generated certificates and incidents

See Content Gateway Manager online Help for complete configuration details.

FTP filtering and scanning

TRITON - Web Security file scanning options can now specify scanning of inbound and outbound FTP files for malicious content and threats, and apply policy.

Support for Skype with explicit proxy deployments

Special support is provided for Skype traffic when SSL is enabled. If Content Gateway is an explicit proxy and you want to allow Skype traffic, enable the **Tunnel Skype** option in Content Gateway Manager on the **Configure > Protocols > HTTPS** page.

This option is necessary because, although Skype presents an SSL handshake, Skype data flow does not conform to the SSL standard. Unless the traffic is tunneled, the connection is dropped.

Important

This option is effective only if Content Gateway is an explicit proxy.

To complete the configuration, ensure that all users allowed to use Skype have a Filtering policy that allows **uncategorized** and **internet telephony**. This is required regardless of whether Skype is used with SSL enabled or not.

Also, if Skype is not prevented, after the handshake it will route traffic over a non-HTTP port. To force Skype traffic to go through Content Gateway, a GPO should be used as described in the Skype IT Administrators Guide.

Multiple ICAP servers

For deployments that use ICAP for additional processing, Content Gateway can now be configured with multiple ICAP servers (URIs) for failover or load distribution.

New performance graphs

Several new performance graphs are added to provide visual assistance in monitoring and analyzing the performance of Content Gateway. The graphs include:

Graph title	Description
HTTP and HTTPS Transactions Per Second	Shows the number of HTTP and HTTPS transactions per second.
HTTP POST and FTP PUT Transactions Per Second	Shows the number of outbound HTTP POST and FTP PUT transactions per second against the total number of outbound transactions per second.
Web Security Scanned Transactions (Percentage):	Shows the percentage of transactions scanned by Web Security (inbound and outbound) against the total number of transactions.
Web Security Slow Transactions	Shows the number of HTTP and HTTPS transactions that took more than 1 second to complete, against the total number of all transactions.
Web Security Slow Scanned Transactions	Shows the number of HTTP and HTTPS transactions that took more than 1 second to scan, against the total number of scanned transactions.
SSL Manager Memory Usage	Shows the amount of RAM used by the SSL Manager Inbound process and Outbound process.
Data Security Module Memory Usage	Shows the amount of RAM used by the Data Security Policy Engine process, and the Data Security Fingerprint Repository process.
Transaction Buffer Memory Usage	Shows the total amount of dynamic RAM allocated by the proxy to hold HTML response data while it is being received for processing. It also shows the amount of that allocated RAM that is in use.

Support is added for TLS1.0 and SSL 3.0 Java security for browsers connecting to Content Gateway Manager to view the performance graphs. In Microsoft Windows the setting is made in **Control Panel** > **Java** > **Advanced** > **Security**.

Deprecated features

- Full clustering. In software installation, on upgrade Full clustering is automatically reconfigured to Management clustering. In appliance installations, Management clustering must be configured after upgrade is complete.

- WCCP v1. On upgrade, WCCP v1 is disabled. Use WCCP v2.
- FTP caching. On upgrade FTP caching is disabled.
- ARM Security. On upgrade ARM Security is disabled.
- Congestion Control. On upgrade Congestion Control is disabled.
- ICP Peering. On upgrade ICP Peering is disabled. Consider moving to an HTTP cache hierarchy before or after upgrade.

Operation tips

Topic 60027 / Updated: 6-May-2011

Applies To:	Websense® Content Gateway 7.6 Websense Web Security Gateway 7.6 Websense Web Security Gateway Anywhere 7.6

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. • 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 (for instructions on creating a raw disk from a mounted file system.) – Must be dedicated – Must *not* be part of a software RAID – Should be, for best performance, 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	Must support WCCP v2, or Policy Based Routing (PBR). A Cisco router must run IOS 12.2 or later. Client machines, 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 requirements

Linux operating system:

- Websense Content Gateway version 7.6 is certified on Red Hat Enterprise Linux 5 series, updates 3, 4 and 5, base or Advanced Platform (32-bit only) and the corresponding CentOS version (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers).
  - 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

  Red Hat Enterprise Linux 6 series is **not** supported at this time.

  - 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
    ```

- 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
    ```
- libgdbm.so.2 required
- RPM krb5-workstation-*.rpm

  This must be the version of the krb5-workstation RPM that is bundled with your version of Red Hat Enterprise Linux.
  - To display a list of RPMs installed on your system with the string "krb5-workstation" in their name, enter the command:
    ```
    rpm -qa |grep krb5-workstation
    ```
- GNU C library (glibc) version 2.5-42 or later
  - 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 or later.
  - Example command to update this library (running as `root`): `yum update glibc`.
- SELinux must be set to disabled or permissive

Websense Web filtering components (Websense Web Security Gateway, Websense Web Security, Websense Web Filter):

- Version 7.6

  

  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.

Integration with Websense Data Security:

- Version 7.6 (to take advantage of the co-located Data Security policy engine)

  The order of installation does not matter. Websense Data Security may be installed before or after Websense Content Gateway.
- Any version can be used via the ICAP interface. See the Content Gateway Manager Help for configuration instructions.

Web browsers:

- Websense Content Gateway is configured and maintained with a Web-based user interface called the Content Gateway Manager. Content Gateway Manager supports the following Web browsers:
  - Internet Explorer 7, 8, and 9

- Mozilla Firefox 3 and later

> **Note**
>
> The browser restrictions mentioned above apply only to the Content Gateway Manager and not to client browsers proxied by Websense Content Gateway.

Installation file path and file ownership

Content Gateway is installed in /opt/WCG. The installation script does **not** prompt for an alternate location. If Content Gateway is being upgraded and the existing installation location is **not** /opt/WCG, the location is automatically moved to /opt/WCG by the upgrade program.

Content Gateway files are installed with root ownership. Content Gateway processes are run as root. The “Websense” user is no longer used.

In explicit proxy deployments, send HTTPS traffic to port 8080

In explicit proxy deployments, when SSL is enabled, browsers should be configured to send HTTPS traffic to the proxy on port 8080. The **ipnat.config** rule that was used to redirect traffic from 8070 to 8080 has been removed.

Client browser limitations

Not all Web browsers fully support transparent authentication (no-prompt).

Internet Explorer 7, 8, and 9

- Full support of transparent authentication

Mozilla Firefox 3 and 4

- Full support of transparent authentication

Google Chrome 6, 7, 8, 9, and 10

- Transparent authentication supported with IWA
- Not supported with Legacy NTLM; always challenges users for credentials

Opera 10

- Transparent authentication **not** supported; always challenges user for credentials
- HTTPS with IWA not supported.

Windows Safari 5 and Safari for iPad iOS 4

- Transparent authentication not supported; always challenges users for credentials
- When SSL Manager is enabled, HTTPS pages are only partially displayed

Corrections from version 7.5.3

Due to the timing of Content Gateway releases 7.5.3 and 7.6.0, a handful of 7.5.3 corrections could not be included in 7.6.0. These include:

- Hotfix 1 - NTLM: prompt for credentials when user is outside of the configured domain
- Portions of hotfix 6 - proxy chaining; LDAP authentication; mobile users
- Hotfixes after hotfix 6 (none as of commercial release of 7.6)

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.

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.

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)

Port configuration

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

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.

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.

SSL Manager configuration changes

After making SSL Manager configuration changes, if the changes do not take effect quickly (within 30 seconds), restart Content Gateway.

Reverse proxy

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

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

When Content Gateway is on a V-Series appliance, the domain of the hostname is automatically added to **/etc/resolv.conf**. For example, if the hostname of the appliance is vseries.example.com, then Content Gateway treats “intranet” requests as “intranet.example.com”.

Using extended event logging

To investigate unexpected system behavior, it is sometimes helpful to enable the **Log Transaction and Errors** option (extended event logging) in Content Gateway Manager (Configure > Subsystems > Logging). However, extended event logging adds significant load to Content Gateway processes. Therefore you should **not** enable extended event logging when Content Gateway is at the high end of its processing capacity.

Resolved and known issues

Topic 600028 / Updated: 6-May-2011

Applies To:	Websense® Content Gateway 7.6 Websense Web Security Gateway 7.6 Websense Web Security Gateway Anywhere 7.6

A list of resolved and 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.