

# v7.7 Release Notes for Websense Content Gateway

Topic 60050 / Updated: 1-August-2012

<b>Applies To:</b>	Websense® Content Gateway, version 7.7 (a component of Web Security Gateway (Anywhere), version 7.7)
--------------------	---

Use these Release Notes to get detailed information about Websense Content Gateway version 7.7.

- ◆ [New in Websense Content Gateway v7.7, page 1](#)
- ◆ [Installation and upgrade, page 18](#)
- ◆ [Operating tips, page 21](#)
- ◆ [Resolved and known issues, page 26](#)

## New in Websense Content Gateway v7.7

Topic 60051 / Updated: 23-December-2013

<b>Applies To:</b>	Websense Content Gateway Version 7.7 (a component of Web Security Gateway and Web Security Gateway Anywhere Version 7.7)
--------------------	---

- ◆ [Support for Red Hat Enterprise Linux 6](#)
- ◆ [Additional real-time analytics](#)
- ◆ [SSL Manager enhancements](#)
- ◆ [SIEM integration](#)
- ◆ [Single sign-on and two-factor authentication](#)
- ◆ [FIPS 140-2 mode](#)
- ◆ [Protocol bandwidth information reported to Websense Web Security](#)
- ◆ [Enhancements to WCCP v2 support](#)
- ◆ [Client connection limits](#)
- ◆ [Scanning option: Content delay handling](#)

- ◆ *Low Memory Mode*
- ◆ *Automatic registration with WebDLP and Data Security Management Server*
- ◆ *Enhancements to Content Gateway clustering*
- ◆ *User authentication support for Apple devices*
- ◆ *Support for sites that use a custom header*
  - *Google Apps for Business*
  - *YouTube for Schools*
- ◆ *Support for Skype*
- ◆ *Integrated SOCKS server on V-Series appliances*
- ◆ *Support for IPv6*
- ◆ *Updated user interface look and feel*

## Support for Red Hat Enterprise Linux 6

---

Websense Content Gateway version 7.7 is supported on:

- ◆ Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.0: 2.6.32.71
  - Kernel version for 6.1: 2.6.32.131
  - Kernel version for 6.2: 2.6.32-220

Content Gateway is also supported on:

- ◆ Red Hat Enterprise Linux 5 series, update 3, 4, 5, 6, and 7, 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)
- ◆ V-Series appliances

Websense recommends that the Red Hat Enterprise Linux version that will host Content Gateway be updated to the latest patch before running the version 7.7 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.



#### **Important**

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 [Operating system and software requirements](#).

## **Additional real-time analytics**

---

The following real-time analytics are added to Websense Web Security Gateway (Anywhere). Options are configured on the TRITON – Web Security Scanning Options page. See “Scanning options” in TRITON – Web Security online Help.

### **Malicious IFrame detection**

Malicious IFrame detection is an analytic classification system for detecting malicious behavior or elevated exposure delivered via IFrames.

Research has shown that many IFrame compromises follow a general pattern. The model therefore has the ability to generalize to new malicious pages, whether they are uncategorized or their embedded URLs are uncategorized.

Malicious IFrame detection is trained to classify based on contextual features of a document, such as location, surrounding tags, header information, and other specific attributes.

### **Suspicious PDF detection**

It is well known that many versions of Adobe PDFs can be compromised and used to deliver malware. Signature-based detection is helpful, but Websense Web Security Gateway adds a Suspicious PDF Detection analytic to discover malicious code in inbound PDFs.

## Outbound data theft protection

Data theft protection (enabled by default) looks for and blocks outbound custom encrypted files, password files, and other files containing sensitive or suspicious data. Results from analysis are reported to the Threats dashboard and are included in transaction logs and reports. See [Websense Web Security v7.7 Release Notes](#).

## Dynamically updated file type identification database

The file type identification database that is maintained by Websense Security Labs is now updated dynamically so that Content Gateway always has the most recent mapping of signatures to file types as determined by Security Labs. When Security Labs updates the database, it is automatically downloaded to Content Gateway when the proxy next polls the Websense Database Download Server. For more information about file type blocking, see the section titled “Enhanced file type blocking” in the Websense Web Security v7.7 Release Notes.

## SSL Manager enhancements

---

### Certificates signed with SHA-1

SSL Manager signs dynamically generated certificates with a SHA-1 algorithm. To create and place a certificate with a stronger SHA algorithm, see the Websense knowledge base article [Creating and placing a stronger SHA certificate](#).

### Expanded SSL Decryption bypass options

The Web Security SSL decryption bypass feature now supports:

- ◆ Client bypass by IP address and IP address range
- ◆ Destination bypass by hostname, IP address, and IP address range. A wildcard (“\*”) can be specified in the hostname to match subdomains.

For example, “\*.example.com” to match “www.example.com”, “mail.example.com”, “videostream.example.com”, etc.

See “SSL decryption bypass” in TRITON – Web Security online Help.

### Server Name Indication (SNI) connection retry

If the SSL connection handshake fails with SNI enabled (default), then another attempt is made without SNI. This provides added support when attempting to connect to servers that are not SNI-compliant and reduces the number of related errors.

## SSL certificate verification engine (CVE) enhancements

- ◆ **Updated trusted certificate store.** The updated trusted certificate store reduces the number of new CAs added to the store when clients browse the Web, which reduces the number of errors that can result after a new CA is added to the store.
- ◆ **Fewer “Unknown revocation state” errors.** The logic for “Block certificates with no CRL URI and no OCSP URI” has been improved to be more consistent with administrator expectations, which reduces the number of incorrect “Unknown revocation state” failures.

See the updated [SSL Manager Certificate Verification Engine](#) guide for best practices when using the CVE.

## SIEM integration

---

If your organization uses a supported Security Information and Event Management (SIEM) solution, you can configure Websense software to forward log data from Filtering Service to the SIEM product. This includes log records sent to Filtering Service for traffic managed by Content Gateway.

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

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

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

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

## Single sign-on and two-factor authentication

---

### Single sign-on

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

When single sign-on access is enabled, Super Administrators with Content Gateway single sign-on permissions can navigate to the **Settings > General > Content Gateway Access** page in TRITON - Web Security and click **Log On** next to the IP address or hostname of a Content Gateway instance. The administrator is taken directly to Content Gateway Manager without seeing a logon page or having to enter credentials. For more information and configuration details, see TRITON – Web Security Help.

Content Gateway administrators can still access Content Gateway Manager by specifying the IP address in the browser; the administrator is prompted for credentials.



---

**Note**

When log on is by single sign-on, clicking **Log Off** terminates the session and causes a logon screen to display.

If you use the **Click here** button to log on again, you are prompted for credentials; the session is not single sign-on. Clicking **Log Off** causes the message “To complete your logout, please close all open browser windows” to display. This is consistent with Content Gateway Manager logons that use basic authentication.

To log on again using single sign-on, go through TRITON – Web Security.

---

## Two-factor authentication

TRITON console can be configured as the access point for two-factor, certificate-based authentication.

Two-factor authentication:

- ◆ Is configured for and applies to TRITON Unified Security Center logon only.
- ◆ Requires administrators to provide 2 forms of identification to log on.
- ◆ **Can be made to apply to Content Gateway Manager** by forcing administrators to log on to TRITON Unified Security Center before accessing Content Gateway Manager **through TRITON – Web Security**.
- ◆ Requires single sign-on (direct access) to be configured in TRITON – Web Security for administrators allowed access to Content Gateway Manager.
- ◆ Requires that the password logon capability be disabled on Content Gateway, preventing administrators not configured for single sign-on from accessing Content Gateway Manager via its IP address. See the section titled “Configuring Content Gateway for two-factor authentication” in Content Gateway Manager online Help. If Content Gateway is deployed on an appliance, password access is disabled using an Appliance Manager command. See “Disabling and enabling password logon” in V-Series Appliance Manager online Help.

For complete information about configuring two-factor authentication, including limitations and restrictions, see “Configuring certificate authentication” in TRITON console online Help and the Websense knowledge base article [insert title link here].

## FIPS 140-2 mode

---

FIPS (Federal Information Processing Standard) 140-2 is a U.S. government security standard for hardware and software cryptography modules. Modules built and certified against the standard assure government and other users that the cryptography in the system meets the stringent standard.

The cryptographic library used in Content Gateway version 7.7 has been submitted for FIPS 140-2 certification. Visit the [Cryptographic Module Validation Program \(CMVP\) validation page](#) for more information.

By default, FIPS 140-2 is not applied to SSL connections.

You can configure Content Gateway to enforce FIPS 140-2 on HTTPS connections, ensuring that HTTPS connections use TLSv1 and FIPS 140-2 approved algorithms. However, once enabled, the option is not reversible without a complete reinstall of Content Gateway. If Content Gateway is on an appliance, the appliance must be reimaged.



### Note

If you intend to use FIPS mode, it is recommended that you enable the mode soon after installation. Root CAs added to the CA tree and configured “Allowed” before FIPS mode is turned on, are re-added to the CA tree in the default “Denied” state when FIPS mode is enabled. As a result, you will have to change the state to “Allowed” again before you can access sites offering those certificates.

For configuration information, see “FIPS 140-2 mode” in Content Gateway Manager online Help.

## Protocol bandwidth information reported to Websense Web Security

---

Beginning with version 7.7, Content Gateway can report bandwidth usage for individual protocols detected tunneling in HTTP. Measurement and reporting parameters are consistent with those used by Network Agent so that bandwidth reporting information can be combined from both sources. For details on configuring Websense Web Security to include Content Gateway data in bandwidth-based

protocol filtering, see “Using Bandwidth Optimizer to manage bandwidth” in TRITON – Web Security online Help.

## Enhancements to WCCP v2 support

---

- ◆ **Content Gateway can accept traffic from multiple subnets.** To support network topologies that need to send traffic to Content Gateway via routers located on different subnets, each service group now requires specification of the Ethernet interface used by the service group. By specifying and binding the Ethernet interface to each service group, routers on different subnets can be used to route traffic to Content Gateway.
- ◆ **Full support for GRE encapsulation on the return path.** In past versions of Content Gateway, GRE on the return path was not fully supported.



### Note

If you are upgrading from an earlier version of Content Gateway:

- ◆ The existing configuration continues to function as it did in v7.6.x. Content Gateway Manager will produce an alarm suggesting that you update your configuration. Updating the configuration migrates the configuration to the new GRE support infrastructure. You do not have to change your configuration unless you want to add the GRE Return Method.
- ◆ **If you are using WCCP with Cisco ASA**, after the upgrade your configuration continues to perform as it did with v7.6.x. Due to a Content Gateway issue, you should not change your configuration after upgrade. Should you need to reconfigure Content Gateway to work with your ASA device, set the Forward and Return Method to L2. This forces Content Gateway to negotiate the correct supported method.



### Important

Mixing services groups with GRE forward/L2 return and GRE forward/GRE return is **not** supported.

---

## WCCP configuration settings propagate around the cluster

Content Gateway Manager Help states that 3 configuration settings **do not** propagate around a management cluster when, in version 7.7, they do. These settings include:

- ◆ Service group **Status** enabled/disabled



- ◆ Service group **Network Interface** value (eth#)
- ◆ Service group **Weight** (Advanced setting)

Because service group **Status** is propagated, it is a **global** enabled/disabled control for the service group. It is not possible to disable a service group on an individual node in the cluster.

Because **Network Interface** is propagated, all nodes in the cluster must use the same network interface for the service group.

Because the value of **Weight** is propagated around the cluster, it prevents the feature from supporting proportional load distribution.

## Client connection limits

---

Intentionally or unintentionally, some clients open many more connections than can be considered normal or supportable. Sometimes a client opens so many connections that system performance is critically affected.

Examples of unintended, high-connection-rate behavior include:

- ◆ Virus-infected clients
- ◆ Clients configured to auto-update, but the site is not responding appropriately, causing very large numbers of drop/reopen actions

To limit the impact of this behavior, Content Gateway allows you to specify:

- ◆ **A client concurrent connection limit** (default = 1000). This is the absolute limit of the number of connections that a single client can have at one time.
- ◆ **A client connection rate limit** (default = 100 per second, averaged over 1 minute). This is the absolute limit of the number of connections that a client can establish per second, averaged over 1 minute.
- ◆ **The proxy response when a limit is exceeded.** You can configure the proxy to close connection requests above the limit, alarm on the condition, or both.
- ◆ **A list of clients exempt from the limits** (by IP address). You can create a list of clients, by IP address, exempted from the limits.

Connection limits apply to HTTP traffic only.

Client connection limits are configured on the **Configure > Network > Connection management > Client Connection Control** page.

## Scanning option: Content delay handling

---

Sometimes load conditions, very large files, streamed transactions, or slow origin servers result in clients waiting for content. The **Content Delay Handling** option,

located in the **Advance Options** section of the **Scanning Options** page of TRITON – Web Security, helps provide a better client experience.

The **Content Delay Handling** feature provides a mechanism for delivering a portion of buffered content to the client **before scanning is complete**. Scanning is performed when all data is received, or the scan size limit is exceeded.

You can specify a time, in seconds, after which Content Gateway begins returning a portion of buffered data to the client (default = 30 seconds). You can specify the exact percentage of buffered data to release to the client (default = 80 percent). This trickling of data to the client continues until the transaction is complete or the scan size limit is exceeded.

## Low Memory Mode

---

When Content Gateway load is especially heavy, or there is a problem that prevents proxy process memory from being recovered as designed, the proxy may enter a low memory condition. In some situations, such as client demand spikes (for example at lunchtime), the condition may be transient.

At your option, you can configure Content Gateway to suspend analysis of traffic for a specified period of time when a low memory condition occurs. In this state, **URL filtering is applied as usual**, and content analysis is suspended.

When the option is enabled, you specify the length of time, in minutes, that analysis is suspended (default = 120 minutes).

Should the memory condition trigger low memory mode:

- ◆ If the low memory condition subsides before the timer expires, analysis resumes and the trigger is reset.
- ◆ If the timer expires, analysis resumes and the trigger is **not** reset.

## Automatic registration with WebDLP and Data Security Management Server

---

To support the Web Security **Threats** dashboard, Content Gateway automatically registers with WebDLP components. For Web Security Gateway, this is the **Forensics repository**. For Websense Web Security Gateway Anywhere, this is the **Data Security Management Server**.

To register with Data Security Management Server, in Content Gateway Manager on the **Configure > My Proxy > Basic** page, you must enable **Data Security > Integrated on-box**. If this option is not enabled, registration is with the Forensics repository.

Auto-registration takes place at Content Gateway startup. Registration is checked every time the proxy restarts and auto-registration is attempted, if necessary.

To perform registration, Content Gateway queries Websense Web Security Policy Broker for needed information, including IP address and cluster ID.



#### Note

If after installation or upgrade registration fails, ensure that the subscription key is installed in TRITON Unified Security Center and restart Content Gateway.

The registration status can be viewed in Content Gateway Manager on the **Monitor > Summary** page by clicking **More Detail** and reviewing the list at the bottom of the **Subscription Details** section.

Once registered, Content Gateway uses the WebDLP Policy Engine for malware detection. WebDLP policies are configured in the **System Modules** section of TRITON – Data Security. After configuration, you must **deploy** the Data Security policies to put them into effect. See TRITON - Data Security Help for details.

If automatic registration fails, an alarm displays stating that an error occurred registering with the component at the IP address. In Websense Web Security Gateway deployments, a manual registration with Data Security Management Server can be attempted in Content Gateway Manager by going to **Configure > Security > Data Security**. Alternatively, restarting Content Gateway initiates a registration attempt.

Registration failure logs are located in: /opt/WCG/logs/dss\_registration.log

## Enhancements to Content Gateway clustering

Enhancements include:

- ◆ The ability to have multiple versions of Content Gateway in the same cluster. This is intended to simplify the process of upgrading a cluster. You should not run a cluster containing different version for a prolonged period of time (many days). Support for multiple versions in a cluster has these features and limits:
  - Configuration synchronization does **not** take place among nodes of different versions.
  - Condition alarms are passed among all nodes.
  - The VIP feature is supported.

## User authentication support for Apple devices

Websense Web Security and Content Gateway can authenticate or identify Mac and iPhone/iPad users for user- or group-based filtering. See the Websense knowledge base article: [How do I use Websense Web Security solutions to authenticate or identify Mac users for user- or group-based filtering?](#)

## Support for sites that use a custom header

---

A growing number of Web sites and Web-based services are using custom HTTP headers to control access to pages or services. Typically a site establishes a unique header/value pair that the client proxy inserts into the request that the destination site examines to validate access. Two examples are Google Apps for Business and YouTube for Schools.

Content Gateway supports this type of destination server access with **add\_hdr** rules defined in **filter.config**. These rules are easily created in Content Gateway Manager on the **Configure > Security > Access Control > Filtering Configuration** page.

*[Google Apps for Business](#)*

*[YouTube for Schools](#)*

### Google Apps for Business

Businesses are adopting Google Apps for Business, including Business Gmail, to provide high-value, low-cost services to the organization.

This can present a challenge to Web security administrators who need to provide access to the enterprise services while blocking the parallel personal services. For example, allowing Google Business Gmail, while blocking Google personal gmail.

The usual way of controlling access is by URL. But that approach doesn't work in this case because the destination URL for work and personal services is the same (i.e. mail.google.com).

Google provides a solution via a custom header in the request with a list of domains that the administrator wants to allow. For example, using the custom header "X-GoogApps-Allowed-Domains", if the header has the value "domain1.com, domain2.com", then "user@domain1.com" and "user@domain2.com" are allowed, but "user@xyz.com" is blocked by Google.

When a user attempts to access Google services from an unauthorized account, Google displays a block page similar to this:



## This service is not available

Gmail is not available for bob@gmail.com within this network. Gmail is only available for accounts in the following domains:

- example1.com
- example2.com

Please talk to your network administrator for more information.

Did you use this product with a different Google Account? [Sign out](#) of your current Google Account and then sign in to the account you want.

©2011 Google - [Google Home](#) - [Terms of Service](#) - [Privacy Policy](#) - [Help](#)

Content Gateway, as an SSL intercepting proxy, provides a facility for creating and adding the custom header.

To implement the solution:

- ◆ In TRITON – Web Security allow the Web Security category **Internet Communication > General Email**.
- ◆ In Content Gateway Manager, enable **HTTPS** (SSL decryption).
- ◆ In Content Gateway Manager, on the **Configure > Security > Access Control** page, open **filter.config** and create an **add\_hdr** rule (see below).

Creating an **add\_hdr** rule:

1. Go to the **Configure > Security > Access Control > Filtering** tab and click **Edit File** to open **filter.config**.
2. For **Rule Type** select **add\_hdr**.
3. For **Primary Destination Type** select **dest\_domain**.
4. In **Primary Destination Value** specify “mail.google.com”.
5. In the **Custom Header** field specify “X-GoogApps-Allowed-Domains”.
6. In the **Header Value** field specify your domain. For example: www.example.com.
7. Click **Add** to add the rule.
8. Click **Apply** to save the changes and then click **Close** to close the edit window.
9. Restart Content Gateway to put the new rule into effect.

For Google’s description of this filtering solution, see the article [Block access to consumer accounts and services while allowing access to Google Apps for your organization](#).

## YouTube for Schools

YouTube for Schools is designed to provide access to educational videos from inside the school network, even when other YouTube content is blocked. Like Google Apps for Business, this YouTube service makes use of a custom header field in the HTTP header to identify YouTube for Schools requests. For Google's description of the service, see [How to Access YouTube in Schools](#).

For a detailed article with step-by-step instructions for creating a YouTube for Schools `add_hdr` rule, see the Websense knowledge base article [Allow content hosted by YouTube for Schools](#).

## Support for Skype

---

As in version 7.6, Skype traffic can be tunneled when SSL Manager is enabled and Content Gateway is an explicit proxy.

In version 7.7, it is no longer necessary to allow "Uncategorized" in the filtering policy that applies to users who are allowed to use Skype.

In version 7.7, to allow Skype traffic when SSL Manager is enabled:

1. In Content Gateway Manager, on the **Configure > Protocols > HTTPS** page, enable the **Tunnel Skype** option.  
The 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.
2. In **TRITON – Web Security**, ensure that filtering policies that apply to users of Skype allow "Internet telephony". This is required for users of Skype whether SSL Manager is enabled or not.
3. If Skype is not prevented, after the handshake Skype 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](#).

## Integrated SOCKS server on V-Series appliances

---

When Content Gateway is deployed on a V-Series appliance, Content Gateway includes an integrated SOCKS server.

SOCKS capabilities are enabled on the **Configure > My Proxy > Basic > General** page.

All SOCKS features are configured on the **Configure > Security > SOCKS** tabs.

You can configure Content Gateway to use more than one SOCKS server and specify which among the servers is the default server.



---

**Note**

Content Gateway does not perform user authentication with the client. However, the proxy can perform user name and password authentication with a SOCKS server running SOCKS version 5.

---

For complete details, see the section titled “Configuring SOCKS servers” in Content Gateway Help.

## Support for IPv6

---

Version 7.7 of TRITON Enterprise, including the Content Gateway proxy, provides incremental support for IPv6.



---

**Important**

**Support is provided for explicit proxy deployments only.**

**Also:** When HTTPS (SSL Manager) is enabled, IPv6 is **not** supported on Red Hat Enterprise Linux, update 6.0 and 6.1. This is due to a Red Hat Enterprise Linux kernel issue.

IPv6 **is supported** with HTTPS enabled, on Red Hat Enterprise Linux, update 6.2, and updates 5.3-5.7.

---

Content Gateway support for IPv6 includes:

- ◆ IPv6 on dual IP stack Ethernet interfaces
- ◆ Support for all protocols: HTTP, HTTPS, FTP, DNS
- ◆ IPv6 traffic to the Internet, clients, and PAC file servers
- ◆ IPv6 virtual IP addresses (vaddrs.config)
- ◆ Authentication rules by client IPv6 address ranges
- ◆ Client IPv6 addresses and address ranges to allow or restrict access to the proxy (ip\_allow.config)
- ◆ Client IPv6 addresses and address ranges to allow or restrict access to Content Gateway Manager (mgmt\_allow.config)
- ◆ IPv6 Primary Destination value and Source IP values in proxy filtering rules (filter.config) and cache rules (cache.config)
- ◆ IPv6 addresses in the SSL Manager Incident List

- ◆ SNMP traps and counters for IPv6 data

Limits and restrictions:

- ◆ IPv6-only internal networks are not supported
- ◆ IPv4 must be used to communicate among all TRITON components, including other members of a Content Gateway cluster



**Note**

Contrary to the embedded descriptive text in Content Gateway Manager, **Multicast Group Address** must be IPv4 (**Configure > My Proxy > Basic > Clustering**).

---

- ◆ With all user authentication, the Domain Controller(s) must be reachable on an IPv4 address
- ◆ The ARM does not support IPv6 addresses, including ipnat.config and bypass.config
- ◆ The parent proxy in a chain cannot be IPv6
- ◆ IP spoofing is not supported
- ◆ The SOCKS proxy is not supported



**Note**

The client operating system must support IPv6. Not all common operating systems support IPv6 by default, including Windows XP. For a comprehensive list, see this Wikipedia article: [Comparison of IPv6 support in operating systems](#).

---



# Updated user interface look and feel

Content Gateway Manager has been updated to have a look and feel that is more consistent with other members of TRITON Enterprise.

**Subscription Details**

Feature	Purchased Status	Expiration Date
Content Categorization	Purchased	Saturday, June 30, 2012
Threat Detection	Purchased	Saturday, June 30, 2012
Data Security	Purchased	Saturday, June 30, 2012
SSL Manager	Purchased	Saturday, June 30, 2012

**Scanning Data Files**

Engine Name	Engine Version	Data File Version	Last Update
Tunneled Protocol Detection	2.0	1028	Wednesday, February 29, 2012 14:39:14
Security Scanning	4	210071	Thursday, March 01, 2012 13:02:51
Advanced File Scanning	3	101344	Thursday, March 01, 2012 08:30:43
Integrated Anti-Virus	5.3.6	201203012103	Thursday, March 01, 2012 14:45:14
Advanced Detection	4	210071	Thursday, March 01, 2012 13:02:51
Content Categorization	3	100938	Monday, February 27, 2012 00:32:44
Malicious IFrame Detection	1	500030	Monday, February 27, 2012 00:32:41
Suspicious PDF Identity Engine	1.0	-	-
File Type Identification	-	7701269	Thursday, February 23, 2012 11:45:55
Content Classification Analytics	3.2.2034	1237	Friday, January 27, 2012 00:17:35
Last time Content Gateway loaded databases, settings, and policies			Thursday, March 01, 2012 14:45:44
Last time Content Gateway successfully checked with Websense for updates			Thursday, March 01, 2012 15:16:01

**Node Details**

Node	On/Off	Objects Served	Ops/Sec	Hit Rate	Throughput (Mbit/sec)	HTTP Hit (ms)	HTTP Miss (ms)
TL3-RH5u5-01	On	0000065168	0.00	0.00%	0.00	0	0

# Installation and upgrade

Topic 60052 / Updated: 2-July-2012

<b>Applies To:</b>	Websense Content Gateway, version 7.7 (a component of Web Security Gateway (Anywhere), version 7.7)
--------------------	---

The Websense [Deployment and Installation Center](#) is the complete resource for deployment, installation, and upgrade information for version 7.7 TRITON Enterprise solutions.

Content Gateway is the proxy component of the Web Security Gateway and Web Security Gateway Anywhere solutions. Installation and upgrade must be performed in the context of installation or upgrade of Web Security Gateway (Anywhere).



## Important

If you are using Content Gateway on a V-Series appliance, Content Gateway is installed and updated when the appliance is factory imaged and upgraded with the appliance patch facility.

TRITON solution **installation information** starts [here](#).

TRITON solution **upgrade information** starts [here](#).

Below are summaries of Content Gateway:

- ◆ [Hardware requirements](#)
- ◆ [Operating system and software requirements](#)
- ◆ [Instructions for downloading the installer](#)

## Hardware requirements

CPU	Quad-core running at 2.8 GHz or faster
Memory	
◆ If RHEL 6, 64-bit	6 GB
◆ If RHEL 5, 32-bit	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	<p>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.</p>
—or—	
Layer 4 switch	<p>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). To support L2 forward or return, 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).</p>

## Operating system and software requirements

---

Websense Content Gateway version 7.7 is certified on:

- ◆ Red Hat Enterprise Linux, 6 series, updates 0, 1, and 2, 64-bit, Basic Server
  - Kernel version for 6.0: 2.6.32.71
  - Kernel version for 6.1: 2.6.32.131
  - Kernel version for 6.2: 2.6.32-220
- ◆ Red Hat Enterprise Linux, 5 series, updates 3, 4 and 5, base or Advanced Platform, 32-bit only

- ◆ Corresponding CentOS versions (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.

Only kernels shipped with the above Linux versions are supported. Visit [www.redhat.com](http://www.redhat.com) for kernel information. To display the kernel version installed on your system, enter the command:

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



#### Important

If you are installing Content Gateway on Red Hat Enterprise Linux 6, you must see [Requirements for Red Hat Enterprise Linux](#) for a list of library requirements, critical ethernet interface naming requirements, and other considerations.

---

## Websense Web Security Gateway (Anywhere)

- ◆ Version 7.7 required



#### Important

Web Security Gateway (Anywhere) must be installed prior to Content Gateway.

---

## Websense Data Security

- ◆ Version 7.7
- ◆ Any version can be used via the ICAP interface. See Content Gateway Manager Help for configuration instructions.

## Web browsers:

- ◆ Websense Content Gateway is configured and maintained with a Web-based user interface called Content Gateway Manager. Content Gateway Manager supports the following Web browsers:
  - Microsoft Internet Explorer 8 and 9
  - Mozilla Firefox versions 5 and later

- Google Chrome 13 and later



#### Note

Browser restrictions apply only to the use of Content Gateway Manager and not to client browsers proxied by Content Gateway.

## Instructions for downloading the installer



#### Note

If Content Gateway is running on a V-Series appliance, it is installed during factory imaging and upgraded when the v7.7 patch is applied. You do not need to download the installer.

To download the Content Gateway v7.7 installer:

1. Go to [mywebsense.com](http://mywebsense.com) and log in to your account.  
You are taken to the My Products and Subscriptions page.
2. Click the **Downloads** tab.
3. Under Download Product Installers, select your **Product and Version (7.7)**.  
The available installers are listed under the form.
4. Click the plus sign (“+”) next to an installer entry for more information about the installer.
5. Click the **download** link to download the installer.

## Operating tips

Topic 60053 / Updated: 2-July-2012

Applies To:
-------------

Websense Content Gateway, version 7.7 (a component of Web Security Gateway (Anywhere), version 7.7)
---

- ◆ [Installation](#)
- ◆ [Configuration](#)
- ◆ [Proxy user authentication](#)
- ◆ [SSL Manager](#)
- ◆ [Post upgrade](#)

# Installation

---

## Software installation location and file ownerships

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 script.

Content Gateway files are installed with root ownership. Content Gateway processes are run as root.

## 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 analytic databases cannot be downloaded from the Websense Database Download Server until Internet connectivity is available.

## Ports

A full deployment of Content Gateway requires that several ports be open. See [Installing Content Gateway](#) in the Deployment and Installation Center for information about open ports and the reassignment of ports, if necessary.

## ‘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)

## 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.

## Configuration

---

### In explicit proxy deployments, send HTTPS traffic to port 8080

In explicit proxy deployments, when HTTPS (SSL Manager) 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 was removed in version 7.6.

### 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.example.com
```

For external Web sites:

```
nslookup www.example.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”.

### 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 in the network.

### 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.

## 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.

## Reverse proxy

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

## Proxy user authentication

---

### Client browser limitations

**Not all Web browsers fully support transparent user authentication.**

The following table indicates how a browser responds to an authentication request when Integrated Windows Authentication (IWA) is configured.

Browser/  Operating System	Internet Explorer (v8 & 9 tested)	Firefox (v11 tested)	Chrome (v17 & 18 tested)	Opera (v10 tested on Windows, v11 tested on Red Hat)	Safari (v5 tested)
Windows	Performs transparent authentication	Performs transparent authentication	Performs transparent authentication	Falls back to NTLM and prompts for credentials	Falls back to NTLM and prompts for credentials
Mac OS X	Not applicable	Performs transparent authentication	Browser issue prevents IWA from working	Not tested.	Performs transparent authentication
Red Hat Enterprise Linux, update 6	Not applicable	Performs transparent authentication	Browser issue prevents IWA from working	Does not support any form of proxy authentication	Not applicable



#### Note

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.



## LDAP support for passwords with special characters

LDAP user authentication can support passwords containing special characters.

Configuration is made directly in the **records.config** file.

The following parameter must be enabled, and the correct encoding name to which the special characters belong must be configured.

Add these entries to **records.config**. Note that the default setting is 0 (feature disabled).

```
// To enable the feature specify 1.
CONFIG proxy.config.ldap.proc.encode_convert INT <1 or 0>
// Specify an encoding name here. For example,
// for German specify "ISO-8859-1".
CONFIG proxy.config.ldap.proc.encode_name STRING <encoding
name>
```

## SSL Manager

---

### SSL Manager and the Root CA

In v7.7 (and beginning with v7.6.5), the SSL Manager default Root CA (presented to clients) is signed with SHA-1. In prior versions, the Root CA was signed with MD5.

It is strongly recommended that all instances of Content Gateway use the same Root CA, and that for best security the signature algorithm be SHA-1.

The best practice is to replace the Websense default Root CA with your organization's Root CA signed by SHA-1 or stronger. See [Internal Root CA](#) in Content Gateway Help.

The Root CA should be imported into all affected clients.



#### Note

Client connections may fail (depending on specific browser behavior) if the client sees a certificate generated by an unknown Root CA.

### Accessing SSL Manager

Accessing SSL Manager with Firefox for the first time causes a certificate warning to display. To eliminate the warning, manually add the certificate to the browser.

1. In the upper left of the browser window, click on the **Firefox** pull down menu and select **Options**.

2. Click on **Advanced** and then **View Certificates**.
3. Click **Add Exception** and enter “https://<Content\_Gateway\_IP\_address>:8071.
4. Click **Get Certificate**, then **Confirm Security Exception**, and then **OK**.

The **Chrome** browser does not get the warning and needs no special configuration.

## Post upgrade

---

### Web Security Gateway and Data Security

If Web Security Gateway (Anywhere) and Data Security are deployed together and upgraded to version 7.7, you must remove stale entries of Content Gateway instances registered in Data Security system modules:

1. Log onto the TRITON Console.
2. Select the **Data Security** tab.
3. Select **Settings > Deployment > System Modules**.
4. Listed are 2 instances of each Web Content Gateway module that is registered with the system. Delete the older instances. You can identify these by looking at the version number that is displayed.
5. Click **Deploy**.

### Not included from version 7.6.5

Due to the timing of Content Gateway releases v7.6.5 and v7.7.0, one feature in 7.6.5 is not included in 7.7.0:

A new option in 7.6.5 supports fall back to the Web security default policy when Integrated Windows Authentication is configured and Fail Open is configured. For more information, see [New in version 7.6.5](#).

Because the feature is not supported in 7.7.0, on upgrade from 7.6.5:

- 7.6.5 “Disabled” is set to 7.7 “Disabled”
- 7.6.5 “Enabled only for critical services failures” is set to 7.7 “Enabled”
- 7.6.5 “Enabled for all authentication failures, including incorrect password” is set to 7.7 “Enabled”

## Resolved and known issues

<b>Applies To:</b>	Websense Content Gateway, version 7.7 (a component of Web Security Gateway (Anywhere), version 7.7)
--------------------	---

A [list of resolved and known issues](#) in this release is available to customers with a current MyWebsense account.

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

