v7.7.3 Release Notes for Websense Content Gateway

Topic 55400 / Updated: 20-February-2013

Applies To:	Websense® Content Gateway, version 7.7.3 (a component of Web Security Gateway and Web Security Gateway Anywhere)

These Release Notes describe Content Gateway version 7.7.3.

Important

Users of Integrated Windows Authentication (IWA):

- If you are upgrading from 7.6.x or 7.7.0, note that the upgrade procedure does not preserve the domain join. Post-upgrade you must re-enable IWA and rejoin the Windows domain.
- When you join the domain, one entry is automatically added to your DNS server for every interface on your appliance or server. The entry for the primary interface is useful, the others must be removed. See IWA domain join in Content Gateway v7.7.3 can create DNS entries that cause problems.

It is highly recommended that you read all of these release notes and follow the upgrade instructions step-by-step.

Appliance upgrade instructions, which includes Content Gateway, start here.

Content Gateway software upgrade instructions start here.

© 2013 Websense, Inc.

New in Content Gateway v7.7.3

Topic 55401 / Updated: 20-February-2013

Applies To:	Websense Content Gateway Version 7.7.3 (a component of Web Security Gateway and Web Security Gateway Anywhere, version 7.7.3)

Support for Red Hat Enterprise Linux 6, Update 3

Content Gateway version 7.7.3 is supported on:

- **Red Hat Enterprise Linux 6, update 3, kernel version 2.6.32-279, 64-bit, Basic Server**

Content Gateway version 7.7.3 is also supported on:

  - Update 6.0, kernel version 2.6.32-71, 64-bit, Basic Server
  - Update 6.1, kernel version 2.6.32-131, 64-bit, Basic Server
  - Update 6.2, kernel version 2.6.32-220, 64-bit, Basic Server

In addition, Content Gateway is supported on:

- Red Hat Enterprise Linux 5 series, updates 3, 4, 5, 6, and 7, 32-bit, base and Advanced Server

- Corresponding CentOS versions (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 hosts Content Gateway be updated to the latest patch before running the version 7.7.3 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*.

User authentication enhancements

User-Agent specifier in Multiple Realm Authentication rules

In a multiple realm authentication rule, Request header User-Agent values can be used to determine if user authentication will be performed. This is useful when you want to authenticate users based on a known set of client applications, usually browsers. Such rules can also specify IP addresses and, if explicit proxy, inbound proxy port.

As with all multiple realm authentication rules, only the first matching rule applies.

When the User-Agent field is used, the critical element is the regular expression (regex) that performs the match.

- The regex must be POSIX-compliant.
    - The “^” operator is not supported.
- Predefined regexes are provided for the most common browsers.
- You can create a custom regex by directly editing the field.
- When the field is empty, all User-Agent values match.

- Multiple regexes are allowed. They must be separated by a "|" ('or' operator).

User-Agent use case:

An organization with a single domain wants to perform user authenticate on requests originating from 2 common Web browsers. They also want to bypass authentication for Web applications that do not support authentication.

An organization—let's call it Best Corp—uses Content Gateway. They have one domain (BCORP), and one domain controller. They use IWA to authenticate users.

Best Corp wants to ensure that:

- Requests from common Web browsers are authenticated. They control which Web browsers are allowed on their computers.
- Web applications that don't support authentication bypass authentication.

The Multiple Realm Authentication feature makes this possible.

To configure the solution, Best Corp:

1. Enables Multiple Realm Authentication.
2. Creates an IWA rule that:
   a. Optionally, specifies the supported client IP address ranges.
   b. Specifies, by User-Agent value, the Web browsers to authenticate.

      For example, in the **User-Agent** field, they use the **Predefined** drop down list to select and **Add** Internet Explorer and Firefox. The regex looks like:

      ```
      MSIE*|Firefox*
      ```

That's it. With this configuration, all requests from Internet Explorer and Firefox, the only 2 browsers that can be installed on their computers, are subject to user authentication. Other User-Agents bypass authentication because they do not match any rule (the same is true for IP addresses that do not match any rule). To further customize the approach, Best Corp could create other realm rules and/or add proxy filtering rules (filter.config) to deny or bypass specific applications by User-Agent value.

For complete information, see Multiple Realm Authentication in Content Gateway Manager Help.

Cookie Mode specifier in Multiple Realm Authentication rules

Cookie mode credential caching is now an option that can be specified in IWA and Legacy NTLM Multiple Realm Authentication rules. When specified, cookie mode caching applies whether your deployment is explicit or transparent proxy.

With multi-user hosts such as Citrix servers, or when client IP addresses are NATed or are routed through a proxy chain resulting in multiple users with the same IP address, you can specify **Cookie Mode Caching** to identify unique users and cache their credentials.

✓ **Note**

IP address caching is recommended when users have unique IP addresses.

Several special requirements and limitations apply:

- With transparent proxy deployments, **Redirect Hostname** must be defined on the **Configure** > **Security** > **Access Control** > **Transparent Proxy Authentication** tab.

✓ **Note**

The Help system incorrectly states that Redirect Hostname must be defined for explicit proxy deployments, as well. It is required only for transparent proxy deployments.

- When the browser is **Internet Explorer**, the full proxy hostname in the form “http://host.domain.com” must be added to the **Local intranet zone**.
- When the browser is **Chrome**, it must be configured to allow third-party cookies, or configured for an exception to allow cookies from the proxy hostname in the form “host.domain.com”.
- When the IP address is set for Cookie Mode and the request method is CONNECT, no caching is performed.

When this option is **disabled**, the global setting is applied. For transparent proxy deployments, the global option is set on **Configure** > **Security** > **Access Control** > **Transparent Proxy Authentication**. For explicit proxy deployments, cookie mode caching is not offered. Instead you must define a set of **Multi-user IP Exceptions** on the **Configure** > **Security** > **Access Control** > **Global Authentication Options** tab.

✓ **Note**

Cookie mode caching does not work with applications that do not support cookies, or with browsers in which cookie support has been disabled.

For complete information see Multiple Realm Authentication in Content Gateway Manager Help.

NTLM Fail Open

The timing of Content Gateway releases 7.6.5 and 7.7.0 prevented a Fail Open feature that was added to 7.6.5 from being included in 7.7.0. That option is added in 7.7.3.

When IWA is the authentication method, when you configure the NTLM global settings (**Configure > Security > Access Control > Global Authentication Options**), there are three choices for **Fail Open**:

- **Disabled**
- **Enabled only for critical services failures** (default)
- **Enabled for all authentication failures, including incorrect password**

This setting applies when IWA negotiates NTLM or falls back to NTLM.

If **Legacy NTLM** is configured, the option is set on the **Configure > Security > Access Control > NTLM** tab.

When **Enabled only for critical services failures** is selected (default), requests proceed if authentication fails because there is no response from the domain controller or because the client is sending badly formed messages.

When **Enabled for all failures**, **including incorrect password** is selected, requests proceed for all authentication failures, even password failures.

When fail open occurs, if a Web Security XID agent is configured, Filtering Service attempts to identify the user and apply user-based policy, otherwise if a policy is assigned to the client's IP address, that policy is applied. Failing that, the Default policy is applied.

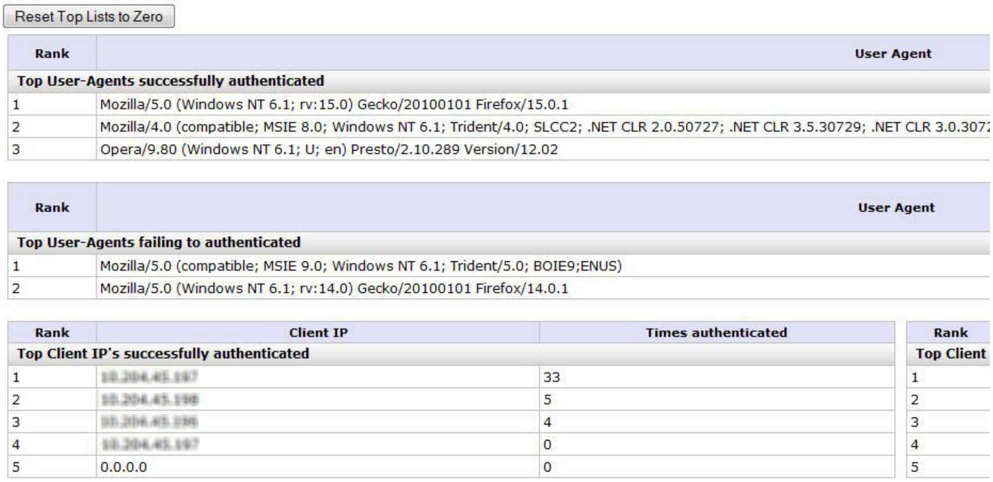
Set **Fail Open** to **Disable** if you want to stop requests from proceeding when authentication failures occur.

Authentication statistics for top User-Agents and IP addresses

When IWA or Multiple Realm Authentication is configured, the **Monitor > Security > Integrated Windows Authentication** page includes statistics for the top 20 User-Agents and top 20 IP addresses that are passing or failing authentication.

A **Reset Top Lists to Zero** button allows you to reset the counters to zero.

This information can help administrators rapidly identify clients and User-Agents that may need special configuration or handling.



Rank	User Agent
Top User-Agents successfully authenticated	
1	Mozilla/5.0 (Windows NT 6.1; rv:15.0) Gecko/20100101 Firefox/15.0.1
2	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.307
3	Opera/9.80 (Windows NT 6.1; U; en) Presto/2.10.289 Version/12.02

Rank	User Agent
Top User-Agents failing to authenticated	
1	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; BOIE9;ENUS)
2	Mozilla/5.0 (Windows NT 6.1; rv:14.0) Gecko/20100101 Firefox/14.0.1

Rank	Client IP	Times authenticated
Top Client IP's successfully authenticated		
1	[redacted]	33
2	[redacted]	5
3	[redacted]	4
4	[redacted]	0
5	0.0.0.0	0

Rank
Top Client
1
2
3
4
5

IWA domain controller information

When IWA is configured, the **Configure > Security > Access Control > Integrated Windows Authentication** tab or, with Multiple Realm Authentication, the **Configure > Security > Access Control > Domains** tab includes:

- The Active Directory site that includes Content Gateway. For information about AD sites, see the Microsoft Technet article Sites overview.

- A list of active domain controller connections showing the current number of domain controller connections and their location.

> **Important**
>
> Users of Integrated Windows Authentication (IWA):
>
> - If you are upgrading from 7.6.x or 7.7.0, note that the upgrade procedure does not preserve the domain join. Post-upgrade you must re-enable IWA and rejoin the Windows domain.
> - When you join the domain, one entry is automatically added to your DNS server for every interface on your appliance or server. The entry for the primary interface is useful, the others must be removed. See IWA domain join in Content Gateway v7.7.3 can create DNS entries that cause problems.
>
> It is highly recommended that you read all of these release notes and follow the upgrade instructions step-by-step.
>
> Appliance upgrade instructions, which includes Content Gateway, start here.
>
> Content Gateway software upgrade instructions start here.

SAMBA engine update and optimization

The SAMBA engine that supports Integrated Windows Authentication has been updated to a newer version (3.6.7) and Content Gateway has been tuned in several ways to provide better performance with the new engine.

SSL Enhancements

SSL certificate verification engine (CVE)

- The **Certificate Authority Tree** (trusted certificate store**)** has been updated. The updated trusted CA tree should reduce the number of new CAs added when clients browse the Web, which should reduce the number of errors that can result after a new CA is added to the tree.
- **Performance optimized CRL revocation checks**. The CRL data tables have been optimized to improve performance and reduce latency when “Check certificate revocation by CRL” is enabled.

See the updated SSL Manager Certificate Verification Engine guide for best practices when using the CVE.

Tunnel Unknown Protocol

The Tunnel Unknown Protocol option directs Content Gateway to tunnel (bypass) SSL connection requests that fail the SSL handshake with an “Unknown protocol” error. Bypassed SSL connections are not decrypted and inspected. This behavior introduces a significant vulnerability. Even so, the behavior is desired by some organizations.

The option is set on **Configure** > **Protocols** > **HTTPS**.

How this option affects proxy handling of SSL requests depends on how Content Gateway is deployed.

- When Content Gateway is an **explicit proxy**, before the SSL connection request is made to the origin server the proxy decrypts the request header to get the URL, a URL database lookup is performed, and policy is applied. If the request is allowed and the subsequent SSL handshake with the origin server fails, the request is tunneled. Transactions are logged as usual.
- When Content Gateway is a **transparent proxy** it immediately attempts to connect to the origin server to get the Common Name from its SSL certificate. The Common Name is used for the URL lookup. If this initial handshake fails, the connection is tunneled without the proxy being aware of it. In this case, transactions are not logged.

Warning

Tunneled connections are not decrypted or inspected.

When the proxy is transparent, tunneled connections are not logged.

SSL resource conservation

- **Improved handling of client requests.** When an incomplete client request is received, 10 retries are attempted before the connection is closed. This tuning of client request handling reduces CPU resource consumption and improves performance.
- **CRL Updates.** CRL updates are enabled by default and can be disabled to conserve Content Gateway resources.

  Disabling CRL updates is recommended if:

  - HTTPS is enabled and the CVE disabled; or
  - HTTPS is disabled

  To disable CRL updates when HTTPS is enabled with the CVE disabled:

  1. Go to **Configure** > **SSL** > **Validation** > **Revocation Settings** > **CRL Settings**.
  2. To disable the scheduled CRL update, remove the check mark next to **Download the CRL**.
  3. Click Apply.

4. Restart Content Gateway.

If HTTPS is disabled, complete the following:

1. Enable HTTPS (**Configure > My Proxy > Basic > General**).
2. Disable CRL updates using the steps listed above.
3. Disable HTTPS (**Configure > My Proxy > Basic > General**).
4. Restart Content Gateway.

SSL Manager pages available when HTTPS is not enabled

Beginning with version 7.7.3, SSL Manager configuration pages are accessible even when HTTPS is disabled. The change is made as an aid in troubleshooting. It is sometimes helpful to be able to change the SSL Manager log level and verify SSL configuration settings that may have persisted from an earlier configuration.

Proxy Health Check URLs to Assist Load Balancers

Content Gateway includes 3 URLs that return proxy health and performance information in the HTTP response. These URLs are designed to help load balancers optimize performance by providing the load balancer with current state information.

The default port for health check URLs is 8083.

The load balancer should consider the service down if the URL request fails for any of the following reasons:

- No TCP connection -- proxy down
- Response too slow -- proxy deadlocked or not responsive
- Invalid response

Health check URLs:

http://[Content Gateway IP address]:8083/health.basic

This URL checks connectivity with Content Gateway and responds with WSUP or WSDOWN.

http://[Content Gateway IP address]:8083/health.app.filtering

This URL checks the health of Filtering Service responses to Content Gateway requests and reports WSUP or WSDOWN.

http://[Content Gateway IP address]:8083/health.load

If the health.basic URL reports WSDOWN, this URL also reports WSDOWN.

Otherwise, health.load returns:

- CPU usage (operating system load average)
- Connection usage (number of open connections)
- Bandwidth usage

The default response looks similar to:

```
HTTP/1.0 200 OK
Server: Content Gateway Manager 7.7.0
Date: Thu, 26 Jul 2012 20:26:14 GMT
Cache-Control: no-store
Pragma: no-cache
Content-type: text/plain
Content-length: xx

Load=2253
Conns=5150
Mbps=6.42
```

There is also an option to force the URLs to report the node down:

Force Health Checks to Report Proxy Down

When enabled on a node, all health check URLs report WSDOWN.

The URL response is similar to:

```
HTTP/1.0 503 Service Unavailable
Server: Content Gateway Manager 7.7.0
Date: Thu, 26 Jul 2012 20:26:14 GMT
Cache-Control: no-store
Pragma: no-cache
Content-type: text/plain
Content-length: 6

WSDOWN
```

The option is set on the **Configure > Networking > Health Check URLs** page.

For complete information, including an explanation of how load values are calculated, see Health Check URLs in Content Gateway Manager Help.

WCCP service group configuration

Special Device Profile designation for Cisco ASA

A **Special Device Profile** has been added to simplify WCCP service group configuration when traffic is routed to Content Gateway by a **Cisco ASA** firewall.

When configuring the service group, if the forwarding device is an ASA Firewall, select **ASA Firewall** from the **Special Device Profile** drop down box instead of individually selecting the GRE forward and return methods. This automatically selects the Packet Forward Method and Packet Return Method and sets some proxy internals.

Important

With Cisco ASA firewalls, select the Special Device Profile; do not individually select the GRE forward and return methods.

WCCP Routers table

For each service group, up to 10 WCCP routers can be specified in the **WCCP Routers** table.

Each specified router must be configured with a corresponding service group.

The **Router IP Address** is the address that Cisco calls the Router ID, which is the physical interface on the router with the highest numeric IP address.

If **GRE Packet Forward Method** or **Packet Return Method** is configured, a **Local GRE Tunnel Endpoint IP address** must be specified for each router, including ASA firewall.

The **Local GRE Tunnel Endpoint IP address** is the Content Gateway tunnel endpoint for the associated **Router IP Address**. The **Local GRE Tunnel Endpoint IP Address**:

- Must be IPv4
- Must be unique and not assigned to any device
- Must be a routable IP address
- Should reside on the same subnet as the proxy. If it is not, you must define a route for it.
- Is not intended to be a client-facing proxy IP address
- Is bound to the physical interface specified for the service group (on a V-Series appliance, eth0 = P1; eth1 = P2)

When **GRE Packet Return Method** is configured and Content Gateway does not have a route back to the WCCP router, specify a **GRE Tunnel Next Hop Router IP Address**.

You can use “ping” to test connectivity to the router.

- From Content Gateway, ping each router defined in the service group (in the Router IP Address field).
- If ping doesn’t return a response, you need to define a **GRE Tunnel Next Hop** to that router. Intervening routers must have a route to the WCCP router, or a next hop.

WCCP configuration settings propagate around the cluster

DOCUMENTATION CORRECTION: Content Gateway Manager Help states that 3 configuration settings **do not** propagate around a management cluster when, in version 7.7.0 and 7.7.3, they do. These settings include:

- Service group **Status** enabled/disabled
- Service group **Network Interface** value (eth#)
- Service group **Weight** (Advanced setting)

Because the value of service group **Status** propagates, 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 the value of **Network Interface** propagates, all nodes in the cluster must use the same network interface for the service group.

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

Japanese language documentation

Japanese language documentation is available for several components of TRITON Enterprise.

Version 7.7.0 Japanese language PDF files are available for:

- TRITON Unified Security Center (console) Help
- TRITON – Web Security Help
- TRITON – Web Security New User Quick Start
- TRITON – Web Security Upgrading User Quick Start
- Content Gateway Manager Help
- V-Series Quick Start poster
- V-Series Getting Started Guide
- V-Series Appliance Manager Help

Japanese language **embedded Help** is available for:

- TRITON console Help

- TRITON – Web Security Help, including the New User Quick Start and Upgrading User Quick Start tutorials
- V-Series Appliance Manager Help

To select Japanese language embedded Help for TRITON console and TRITON – Web Security, log onto the TRITON console and navigate to **TRITON Settings**. From the **Help Language Preference** drop down box select Japanese. All Japanese language Help is enabled.

Installation and upgrade

Topic 55402 / Updated: 20-February-2013

Applies To:	Websense Content Gateway, version 7.7.3 (a component of Web Security Gateway and Web Security Gateway Anywhere)

The Websense Deployment and Installation Center is the complete resource for deployment, installation, and upgrade information for all v7.7.x 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 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.

Content Gateway step-by-step upgrade instructions start here.

Below are summaries of Content Gateway:

- *Hardware requirements*
- *Operating system and software requirements*
- *Instructions for downloading the installer*

> **Note**
>
> Data Security Policy Engine with Content Gateway:
>
> Content Gateway includes an on-board Data Security policy engine. The v7.7.3 policy engine is compatible with Content Gateway v7.7.0 - v7.7.3; however, to take advantage of v7.7.3 policy engine improvements, Content Gateway must be v7.7.3.

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 – 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). 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).

Operating system and software requirements

Websense Content Gateway version 7.7.3 is certified on:

- Red Hat Enterprise Linux, 6 series, updates 0, 1, 2, and 3, 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
  - Kernel version for 6.3: 2.6.32-279
- Red Hat Enterprise Linux, 5 series, updates 3, 4, 5, 6, and 7, 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 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 7.7.3 required

Important

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

Websense Data Security

- Version 7.7.3

- 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 v7.7.3 patch is applied. You do not need to download the installer.

! **Important**

Users of Integrated Windows Authentication (IWA):

- If you are upgrading from 7.6.x or 7.7.0, note that the upgrade procedure does not preserve the domain join. Post-upgrade you must re-enable IWA and rejoin the Windows domain.
- When you join the domain, one entry is automatically added to your DNS server for every interface on your appliance or server. The entry for the primary interface is useful, the others must be removed. See IWA domain join in Content Gateway v7.7.3 can create DNS entries that cause problems.

It is highly recommended that you read all of these release notes and follow the upgrade instructions step-by-step.

Appliance upgrade instructions, which includes Content Gateway, start here.

Content Gateway software upgrade instructions start here.

To download the Content Gateway v7.7.3 installer:

1. Go to 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** (7.7.3).

   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 55403 / Updated: 22-December-2013

Applies To:	Websense Content Gateway, version 7.7.3 (a component of Web Security Gateway and Web Security Gateway Anywhere)

- ◆ *Installation*
- ◆ *Configuration*
- ◆ *Proxy user authentication*
- ◆ *SSL Manager*
- ◆ *Post upgrade*

Installation

Software installation location and file ownerships

Content Gateway is installed in **/opt/WCG**. 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 address 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**), restart the proxy to cause 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. If possible, do 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 & 10 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

Browser/ Operating System	Internet Explorer (v8, 9 & 10 tested)	Firefox (v11 tested)	Chrome (v17 & 18 tested)	Opera (v10 tested on Windows, v11 tested on Red Hat)	Safari (v5 tested)
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

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>
```

User authentication with SOCKS

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

SSL Manager

SSL Manager and the Root CA

In v7.7.0 (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 is 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.

Post upgrade

Integrated Windows Authentication (IWA)

The upgrade procedure does not preserve the IWA join to the Windows Domain.

Post upgrade, re-enable IWA and rejoin IWA to the Windows Domain. See **Configuring Integrated Windows Authentication** in Content Gateway Manager Help.

! **Important**

When you join the domain, one entry is automatically added to your DNS server for every interface on your appliance or server. The entry for the primary interface is useful, the others must be removed. See IWA domain join in Content Gateway v7.7.3 can create DNS entries that cause problems.

Web Security Gateway and Data Security

If Web Security Gateway Anywhere and Data Security are deployed together and upgraded from v7.6.x to version 7.7.3, 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 Content Gateway module registered with the system. Delete the older instances. You can identify these by looking at the version number.
5. Click **Deploy**.

If Web Security Gateway Anywhere and Data Security are deployed together and configured to use the on-box policy engine, and then reconfigured during upgrade or later to use the ICAP interface, the Content Gateway instance must be deleted from the list of Data Security system modules or the deployment will fail.

1. Log on to the TRITON console.
2. Select the **Data Security** tab.
3. Select **Settings** > **Deployment** > **System Modules**.
4. Locate the entry for the Content Gateway instance, click on it to open its **Details** page and then click **Delete**.
5. Click **Deploy**.

Resolved and known issues

Topic 55404 / Updated: 20-February-2013

Applies To:	Websense Content Gateway, version 7.7.3 (a component of Web Security Gateway and Web Security Gateway Anywhere)

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 on to MyWebsense, the link takes you to a logon prompt. Log on to view the list.