v7.8.1 Release Notes for Websense® Content Gateway

Topic 60072 / Updated: 21-October-2013

Applies To:	Websense Content Gateway version 7.8.1 (a component of Web Security Gateway / Anywhere)

These Release Notes are an introduction to Websense Content Gateway version 7.8.1.

All sections of these notes include important information that helps ensure your successful installation, upgrade, and deployment of Content Gateway.

TRITON security solution upgrade instructions, including Web Security Gateway / Anywhere, start here.

Important

If your deployment uses Integrated Windows Authentication (IWA):

- After upgrade to v7.8.1 check and, if necessary, rejoin IWA domains.
- Version 7.8.1 does not support IWA with a load balancer. If your deployment requires this combination, after upgrade to v7.8.1 upgrade to v7.8.2. See the v7.8.2 Release Notes.

New in Websense Content Gateway v7.8.1

Topic 60073 / Updated: 21-October-2013

Applies To:	Websense Content Gateway version 7.8.1 (a component of Web Security Gateway / Anywhere)

- *ThreatScope™*
- *64-bit Content Gateway*
- *SSL*
- *User authentication*
- *Range-based IP spoofing*
- *Policy Broker resiliency*
- *Filtering Service resiliency*
- *Secured by RSA® authentication*
- *FIPS 140-2 mode*
- *Office 365*
- *WCCP*
- *Japanese language embedded Help*
- *Removed: Support for the Microsoft ISA plugin*

ThreatScope™

ThreatScope is a Websense-hosted sandbox that provides enhanced detection of 0-day threats.

Suspicious downloads that fit the Websense Security Labs profile are uploaded to a cloud-hosted sandbox for activation and analysis. ThreatScope observes the behavior of the payload and compiles an extensive report. If the file is found to be malicious, an alert message is sent to the Web Security administrator with information about the threat and links to the ThreatScope report and an Investigative Report generated from your log records. Websense updates the Master Database, ACE analytic databases, and other security components. The next time someone in the organization tries to access the site, they and the organization are protected.

ThreatScope is a premium option for Web Security Gateway Anywhere subscribers.

This feature is described in detail in the version 7.8.1 Web Security Release Notes.

64-bit Content Gateway

Content Gateway version 7.8.1 is now full 64-bit and is offered only as 64-bit.

Important

If you are planning to upgrade to version 7.8.1 and Content Gateway is currently hosted on any version of Red Hat Enterprise Linux 5-series, you must include an operating system upgrade to Red Hat Enterprise Linux 6-series to the Content Gateway upgrade process. Red Hat Enterprise Linux 6.3 or 6.4 is recommended. Web Security upgrade instructions start here.

Content Gateway is certified on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.4: 2.6.32-358
  - Kernel version for 6.3: 2.6.32-279
- V-Series appliances

Content Gateway is supported on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.2: 2.6.32-220
  - Kernel version for 6.1: 2.6.32-131
  - Kernel version for 6.0: 2.6.32-71
- The corresponding CentOS versions, including updates 3 and 4 (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

Only kernels listed above are certified or supported. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

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

Websense, Inc. provides “best effort” support for the version of Red Hat Enterprise Linux and CentOS listed above. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion until the issue is deemed a Red Hat Enterprise Linux- or CentOS-specific issue, at which point you must contact Red Hat directly for assistance.

Websense recommends that the Red Hat Enterprise Linux version that will host Content Gateway be updated to the latest patch before running the version 7.8.1 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*.

SSL

Support for SSL (HTTPS) decryption, analysis, and re-encryption has been re-engineered for version 7.8.1.

SSL support is now part of the core Content Gateway proxy.

Rearchitected support:

- Increases connection capacity, boosting concurrent end-to-end SSL connections to a minimum of 10,000 on a V-Series V10000 G2 (10,000 inbound client to proxy; 10,000 outbound proxy to origin server*).
- Improves real scaling, because connection capacity is limited only by memory capacity (and the Connection Management settings*).
- Improves performance and stability. Asynchronous event, multiple thread architecture and improved caching and memory management improves stability and reduces latency.

*The total proxy concurrent connection limit (HTTP + HTTPS) is determined by the value of **Throttling Net Connections** (default 45,000) set in the Content Gateway manager on the **Configure > Networking > Connection Management > Throttling** page.

In addition to the high-level enhancements, SSL support:

- Provides functional parity with past versions of SSL Manager, including the Certificate Verification Engine (CVE)

- Provides near-parity in the UI presentation in Content Gateway manager. Some configuration options are no longer needed and have been removed (see *Changes from past versions*, below)
- Participates in Content Gateway management clustering; the separate SSL clustering mechanism is removed
- Adds support for the TLS v1.1 and v1.2 protocols; support is enabled/disabled with **records.config** variables; details below
- Pre-installs the trusted Root CA tree used by Mozilla Firefox

What is SSL support?

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are the most common protocols for secure transmission of data on the Internet. They rely on data encryption and a system of trusted certificates issued by certificate authorities (CAs) that are recognized by clients and servers. SSL/TLS requests made in a browser are identified by the "https" string that leads the URL.

When the HTTPS protocol is enabled in the Content Gateway manager, HTTPS (SSL/TLS) traffic is decrypted, analyzed, and re-encrypted before it is sent to its destination. ACE real-time analytics are used to inspect content and protect against malicious and undesirable data flow, in the same way that ACE is applied to HTTP traffic.

SSL support:

- Can be used with explicit and transparent proxy deployments
- Can be configured to accept HTTPS traffic from multiple inbound ports (client to proxy)
- Provides certificate handling and management features
- Includes configurable certificate validation features
- Includes robust decryption bypass features to simplify the process of maintaining compliance with government and corporate laws and policies, and to whitelist trusted sites and blacklist untrusted sites
- Allows for customizable messages to users when there is a certificate verification failure or connection error

Support for TLSv1.1 and TLSv1.2

Version 7.8.1 supports TLSv1.1 and v1.2.

Enabling and disabling TLSv1.1 and/or v1.2 is done by changing the value of **records.config** variables.

Inbound support (client to proxy) is enabled by default.

Outbound support (proxy to origin server) is disabled by default.

To enable TLSv1.1 support on the proxy to origin server connection, set the following variable to 1. Set it to 0 to disable it (default). "client" in the variable name refers to Content Gateway's role in the connection (client to the origin server).

```
proxy.config.ssl.client.TLSv11 INT 1
```

To enable TLSv1.2 support on the proxy to origin server connection, set the following variable to 1. Set it to 0 to disable it (default). “client” in the variable name refers to Content Gateway’s role in the connection (client to the origin server).

```
proxy.config.ssl.client.TLSv12 INT 1
```

To enable TLSv1.1 support on the client to proxy connection (enabled by default), set the following variable to 1. Set it to 0 to disable support. “server” in the variable name refers to Content Gateway’s role in the connection (server to the client).

```
proxy.config.ssl.server.TLSv11 INT 1
```

To enable TLSv1.2 support on the client to proxy connection (enabled by default), set the following variable to 1. Set it to 0 to disable support. “server” in the variable name refers to Content Gateway’s role in the connection.

```
proxy.config.ssl.server.TLSv12 INT 1
```

To set the value of a variable:

- If Content Gateway is on a Websense appliance, use the **Administration > Toolbox > Command Line Utility**.
- If Content Gateway is installed on a standalone server, edit **/opt/WCG/config/records.config**. To apply the changes, run the following command from the Content Gateway bin directory (/opt/WCG/bin/):

  ```
  ./content_line -x
  ```

Changes from past versions

Although SSL support is functionally unchanged from prior versions, users of past releases will be interested in this summary of infrastructure changes. For a description of how version 7.7.x SSL Manager configuration is handled by the upgrade process to version 7.8.1, see *On upgrade*, below.

- The SSL Manager plug-in is removed.
- The **/opt/WCG/sxsuite** directory and its contents are removed. Notably, this includes **sxsuite/inbound*.log** and **outbound*.log**.
- Transaction logging is sent to **extended.log** or **squid.log** when the logging subsystem is configured for “Log Transactions and Errors” or “Log Transactions Only”. Otherwise, logging is sent to **content_gateway.out**.
- The SSL SQLite3 configuration database is renamed **new_scip3.db** and is located in **/opt/WCG/config**.
- The code for customized **Certificate Failure** and **Connect Error** pages has been changed to improve security by including the session ID. If those pages are customized in your deployment (**Configure > SSL > Customization**), you will have to reapply your customizations.
- The **Default** cipher setting uses all available ciphers except eNULL, the ADH suite, and the **EXP suite**. EXP suite is added to the exclusion set in version 7.8.1.

- On the Certificate Validation configuration page, “Run external program on incidents” is removed.
- Port 8071 is no longer used; there is no longer a separate server for SSL user interface configuration pages.
- On the **Configure > Protocols > HTTPS** page, **SSL Outbound Port** is no longer needed and has been removed.
- On the **Configure > SSL > Decryption / Encryption Inbound** and **Outbound** pages, **Credential Forwarding** and **VIA Header** are no longer needed and have been removed.

On upgrade

When you upgrade from version 7.7.x to 7.8.1, most of your SSL configuration settings are saved and applied to the upgraded version of Content Gateway.

It is very important that you read and follow the step-by-step upgrade instructions. Doing so helps ensure a smooth upgrade process and maximizes retention of data.

Please note the following details.

- You can upgrade directly from Content Gateway version 7.7.0 and 7.7.3. Earlier versions must upgrade to 7.7.x before upgrading to 7.8.1.
- The Certificate Authority Tree is retained (trusted Root CA tree).
- Static entries in the Incident List are retained and added to the new Incident List .
- CRL and OCSP revocation records are retained.
- The 7.7.x SSL SQLite3 database is converted to a new database file.
- Dynamic certificates are not retained. All other certificates are retained.
- Customized error message pages are lost. Record your customizations in advance and be prepared to reapply them after upgrade.
- If SSLv2 is enabled, the setting is retained on upgrade.
- SSL **inbound*.log** and **outbound*.log** files are deleted. After upgrade, transaction logging is sent to **extended.log** or **squid.log** when the logging subsystem is configured for “Log Transactions and Errors” or “Log Transactions Only”. Otherwise, logging is sent to **content_gateway.out**.

User authentication

Important

If you are upgrading from version 7.7.x and your user authentication configuration includes Multiple Realm Authentication rules, the Rule-Based Authentication enhancements may impact your configuration. Please read the following sections carefully. You will want to review and adjust your user authentication configuration after the software upgrade is complete.

Rule-based authentication

Proxy user authentication now includes a more flexible, expanded, and reorganized rule-based model that supports rules for:

- Multiple realms – A realm is a domain that doesn't share trust relationships with other domains and therefore its members must be authenticated by a domain controller within its domain.
- Authentication with an ordered list of domains. This is valuable when a user's domain membership is unknown. When a list of domains is specified in a rule, authentication is attempted against each domain, in order, until authentication succeeds or the list is exhausted, in which case no authentication is performed. When authentication succeeds, the domain is cached and the list is not traversed in subsequent authentications. The authentication method (IWA, NTLM, LDAP) can vary by domain and is specified when a domain is added to the Domains list.

Rule match is based on:

- Client IP address, and/or
- Inbound proxy port (explicit proxy only), and/or
- User-Agent value

Note

Support for use of a single authentication method for the entire deployment is unchanged. The proxy can be configured to perform Integrated Windows Authentication (IWA), Legacy NTLM, LDAP, or RADIUS authentication for all clients against a single domain or directory service. See Proxy user authentication.

Users of the pre-existing Multiple Realm Authentication feature should think of rule-based authentication as:

- A rename and expansion of the Multiple Realm Authentication feature
- The addition of support for ordered domain lists
- A reorganization and simplification of how domains are specified for use in rules
- A simplification of how credential caching is configured (see *Credential caching*)

Users of rule-based authentication should understand that the authentication method (IWA, Legacy NTLM, LDAP) has the same features, requirements, and limitations as the same method used standalone. Read the documentation for each authentication method in Content Gateway Help before specifying the method with a domain.

Rule-based authentication structure and logic

Structure:

- A list of domains is created and maintained.
  - When a domain is added to the list, the authentication method is specified.

    IWA, Legacy NTLM, and LDAP are supported. RADIUS is not supported.
  - Domains on the list can be specified in authentication rules.
  - The Domains list is created and maintained on the **Configure** > **Security** > **Access Control** > **Domains** tab.
  - The Domains list is stored in **auth_domains.config**.
- Authentication rules match users (clients) based on:
  - Client IP address
  - Inbound proxy port (explicit proxy only)
  - User-Agent value
- When a user matches a rule, authentication is performed against the specified domain or list of domains.

  Authentication rules are defined on the **Configure** > **Security** > **Access Control** > **Authentication Rules** tab. Rules are stored in **auth_rules.config**.

> ✓ **Note**
>
> *Credential caching* configuration is performed on the **Configure** > **Security** > **Access Control** > **Global Configuration Options** tab. On that page you specify IP address caching, cookie caching, or both. The setting applies to both transparent proxy and explicit proxy traffic. When both IP address caching and cookie caching are specified, the IP addresses that cookie caching is applied to must be specified.

Logic:

- One or more rules are defined for client/domain(s) pairs (**Configure > Security > Access Control > Authentication Rules**).
- When a request for web content is received:
    - A top-down traversal of the rule list begins
    - The first match is applied
    - If the rule includes a list of domains, authentication proceeds as follows:
        - The proxy attempts to authenticate with the first domain using the method configured for that domain. For example, if the first domain is IWA, Content Gateway transparently negotiates with the browser for credentials.
        - If authentication fails and Content Gateway hasn't already challenged (prompted) for basic credentials, it then prompts for credentials.

> **Important**
>
> When Content Gateway is an explicit proxy and the first and second domains are IWA, there is no prompt for basic credentials when authentication with the first domain fails. Instead, Content Gateway uses the issued Kerberos ticket to attempt to authenticate against the second domain.
>
> When Content Gateway is a transparent proxy and the user is not a member of the first domain, the request for a Kerberos ticket fails because the client does not trust the FQDN sent with the request. The fallback to NTLM authentication also fails and the user is prompted for credentials.

-
    -
        - Content Gateway then uses the basic credentials with each subsequent domain, starting with the second, proceeding sequentially until authentication succeeds or the list is exhausted.
        - Content Gateway then uses the basic credentials to attempt, again, to authenticate with the first domain.
        - If authentication fails with all domains, the proxy assumes that the user misentered their credentials, prompts again for basic credentials, and attempts to authenticate sequentially against the list.
    - If no rule matches, no authentication is attempted
- Transactions are logged with the user name used by Filtering Service.
- Proxy authentication statistics are collected and reported individually for each authentication method on the **Monitor > Security** pages.

Rule-based authentication configuration summary

1. If Content Gateway is an explicit proxy and you want to bring traffic in on multiple ports, specify the ports on the **Configure** > **Protocol** > **HTTP** tab.

> **Important**
>
> You must also configure your clients to use the correct port.

2. Configure **Global authentication options** (**Configure** > **Security** > **Access Control** > **Global Authentication Options**). See *Credential caching*.
3. Create a Domains list (**Configure** > **Security** > **Access Control** > **Domains**).
   - To specify a domain in a rule, it must be a member of the **Domains** list.
   - Active Directory domains used with IWA must be joined.
4. Create authentication rules (**Configure** > **Security** > **Access Control** > **Authentication Rules**).

5. Restart Content Gateway to make the new rules take effect.

For complete details, see Rule-Based Authentication in Content Gateway Help.

Rule-based authentication best practices

- If you know the domain membership of a set of users, create a rule just for that group; do not combine that group with another group and use a list of domains.
- Place the rule with the largest number of users authenticating with known domain membership at the top of the list.
- If you don't know what domain a set of users belongs to, specify the smallest number of domains needed to authenticate the users in the set.
- In a list of domains, if there is an IWA domain, make it first in the list.
- If there is more than one IWA domain in a list, place the largest domains at the top of the list.
- Note that users who are **not** joined to the first IWA domain in a list are prompted for credentials (basic authentication).
- Note that if the first domain in the list is LDAP, every user who matches that rule is prompted for credentials. The credentials provided by the user are offered to each successive domain in the list.

On upgrade

Multiple realm rules are converted to the new rule-based format. It's important to review and verify the configuration.

- The domain defined in each realm rule is added to the Domain list.

  If it is a joined IWA domain, it remains joined.

After upgrade, review the Domain list and for every IWA domain, select and edit the entry to assign a unique **Domain Identifier** (this is not the domain name but rather an internal identifier used by Content Gateway; a name is automatically assigned to other domain/directory service types).

- A functionally equivalent rule is created.

  After upgrade, review the Authentication Rules list and verify that the:

  - Rules are in the correct order
  - Every rule has the correct specifications

  If Cookie Mode Caching is specified in the multiple realm rule, the specified IP addresses are moved to the cookie caching list in the Caching Methods section of the **Global Authentication Option** page. **Cache using Cookies only** or **Cache using both IP Addresses and Cookies** should be enabled.

- If Content Gateway is a transparent proxy, the v7.7.x **Authentication Mode** setting (IP address or Cookie mode) is retained from **Transparent Proxy Authentication** tab.

Credential caching

User authentication credential caching has been simplified and enhanced.

There is now one credential cache for both explicit and transparent proxy mode and one, global configuration for setting the caching method and Time-To-Live.

The redesigned **Global Authentication Options** page hosts:

- The authentication **Fail Open** setting – This option is unchanged from previous releases.
- **Credential Caching** options – These settings are global and apply to explicit and transparent proxy traffic.

  Settings include:

  - **Caching Method**
  - **Cache Time-To-Live**, in minutes
  - **LDAP purge cache on authentication failure**

- **Redirect Hostname** (transparent proxy only) – This option is unchanged from prior versions.

Credential caching options apply to all clients whether Content Gateway is an explicit or transparent proxy. Settings support:

- **Caching using IP address only** – Recommended when all clients have a unique IP address.
- **Caching using Cookie mode only** – Recommended when all clients share IP addresses, as with multi-user hosts such as Citrix servers, or when traffic is NATed in a proxy chain or by a firewall.
- **Caching using both IP address and cookie mode** – Recommended when the network has a mix of clients, some with unique IP addresses and some not. In this

mode, cookie mode is used with specified IP addresses and ranges, the remainder are cached by IP address.

Note

The user interface setting to disable the NTLM cache for explicit proxy has been removed. Although not recommended, the cache can be disabled for explicit proxy traffic in **records.config** by setting the value of **proxy.config.ntlm.cache.enabled** to **0** (zero).

When upgrading from v7.7.x to 7.8.1, if NTLM caching is disabled, it remains disabled.

Credential caching applies to:

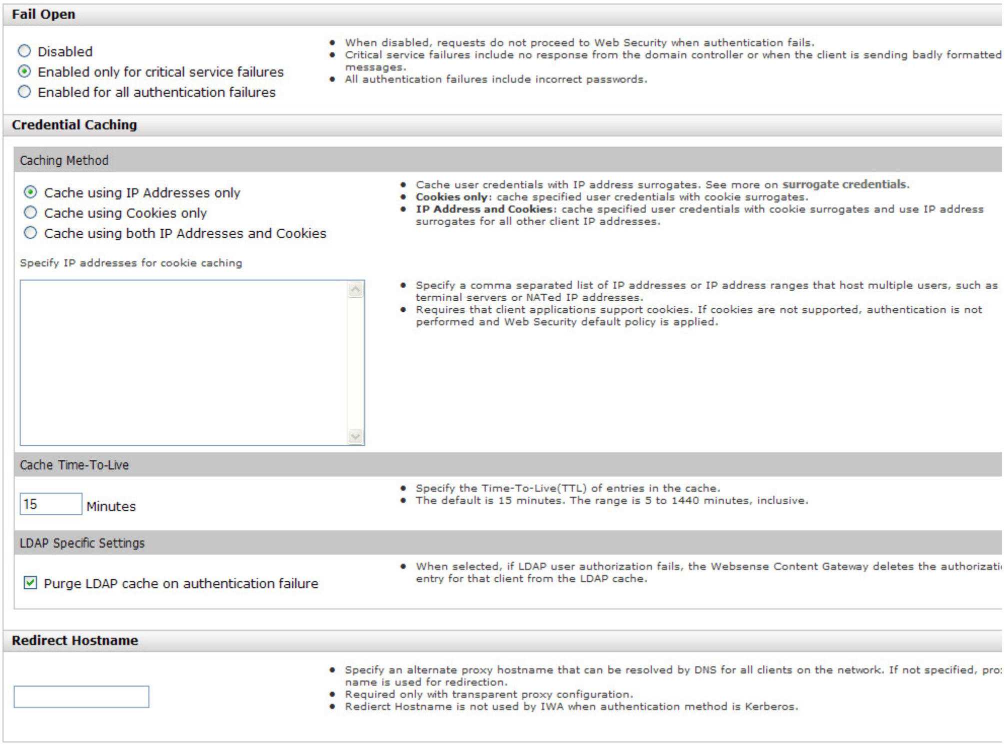
- NTLM authentication when Integrated Windows Authentication (IWA) falls back to NTLM
- Legacy NTLM

Note

When IWA authenticates with Kerberos, Kerberos handles ticket caching (equivalent of credential caching).

The **LDAP purge cache on authentication failure** causes the proxy to delete the authorization entry for the client from the LDAP cache if the LDAP user authorization fails.

The 7.8.1 Global Authentication Option screen:



Fail Open

○ Disabled
● Enabled only for critical service failures
○ Enabled for all authentication failures

- When disabled, requests do not proceed to Web Security when authentication fails.
- Critical service failures include no response from the domain controller or when the client is sending badly formatted messages.
- All authentication failures include incorrect passwords.

Credential Caching

Caching Method

● Cache using IP Addresses only
○ Cache using Cookies only
○ Cache using both IP Addresses and Cookies

- Cache user credentials with IP address surrogates. See more on **surrogate credentials**.
- **Cookies only**: cache specified user credentials with cookie surrogates.
- **IP Address and Cookies**: cache specified user credentials with cookie surrogates and use IP address surrogates for all other client IP addresses.

Specify IP addresses for cookie caching

- Specify a comma separated list of IP addresses or IP address ranges that host multiple users, such as terminal servers or NATed IP addresses.
- Requires that client applications support cookies. If cookies are not supported, authentication is not performed and Web Security default policy is applied.

Cache Time-To-Live

15 Minutes

- Specify the Time-To-Live(TTL) of entries in the cache.
- The default is 15 minutes. The range is 5 to 1440 minutes, inclusive.

LDAP Specific Settings

☑ Purge LDAP cache on authentication failure

- When selected, if LDAP user authorization fails, the Websense Content Gateway deletes the authorizati entry for that client from the LDAP cache.

Redirect Hostname

- Specify an alternate proxy hostname that can be resolved by DNS for all clients on the network. If not specified, pro name is used for redirection.
- Required only with transparent proxy configuration.
- Redierct Hostname is not used by IWA when authentication method is Kerberos.

Note

The Transparent Proxy Authentication page has been removed.

On upgrade

- The credential caching Enabled/Disabled setting for explicit proxy is retained from the v7.7.x Global Authentication Options tab. Caching for transparent proxy traffic is always enabled.
- The Authentication Mode setting (IP address or Cookie mode) is retained from the Transparent Proxy Authentication tab.
- The Cache TTL value is retained from Transparent Proxy Authentication tab unless the value on the Global Authentication Options tab is not the default, in which case the customized value is used. The cache TTL value is in minutes.
- IP addresses and ranges on the Global Authentication Options Multi-user IP Exclusions list are moved to the cookie cache IP address list.
- If Cookie Mode Caching is enabled in a multiple realm rule, the source IP addresses from that rule are copied to the cookie cache IP address list.

Range-based IP spoofing

IP Spoofing is extended to support groupings of clients (IP addresses and IP address ranges) that are mapped to specified IP addresses for spoofing. This is called range-based IP spoofing.

Among other scenarios, range-based IP spoofing supports:

- Website service differentiation by IP address. For example, to receive a web-hosted service, an organization might identify membership to the service via a shared IP address.
- IP address-based authentication with an external service when a unique IP address represents a group of users.
- A way to configure traditional IP spoofing for some clients (source IP addresses that don't match any group are spoofed with their own IP address), range-based IP spoofing for some clients, and standard proxy IP address substitution for some clients. The latter is done by creating a group that specifies the proxy IP address.

About IP Spoofing

IP Spoofing is supported with transparent proxy deployments only.

IP spoofing configures the proxy to use either the IP address of the client or a specified IP address (range-based IP spoofing) instead of the proxy IP address when communicating with the origin server. As a result, requests appear to come from the client or the specified IP address instead of the proxy.

IP spoofing is supported for HTTP and HTTPS traffic. When IP spoofing is enabled, it is applied to both protocols. It cannot be configured to apply to only one.

IP spoofing requires special return traffic routing configuration for all HTTP/S traffic (80 and 443) to deliver spoofed traffic back to the proxy for processing.

IP Spoofing does not support IPv6.

Range-based IP Spoofing is not supported on many older versions of Cisco IOS firmware. Update your Cisco device to the latest firmware.

\

Warning

Deploying IP spoofing requires precise control of the routing paths on your network, overriding the normal routing process for traffic running on TCP ports 80 and 443.

With IP spoofing enabled, traditional debugging tools such as traceroute and ping have limited utility.

For complete information, see IP Spoofing in Content Gateway Help.

Policy Broker resiliency

Content Gateway receives several sets of important data from Web Security Policy Broker. One set of data includes the **Web Security Scanning Options** settings, including analytics settings, scanning exceptions, and SSL decryption bypass settings. In past releases, Content Gateway stored this information in memory only. If Policy Broker was unavailable when Content Gateway started or restarted, the Scanning Options settings could not be loaded or applied.

Content Gateway has been enhanced to keep a configuration file of Policy Broker data, including the Scanning Options settings. If Policy Broker becomes unavailable, Content Gateway continues to apply the most recent settings. If Content Gateway restarts and Policy Broker is unavailable, Content Gateway loads the locally stored settings until the connection with Policy Broker is restored and updates can be received. Whenever Policy Broker becomes unavailable after Content Gateway has started, an alarm is generated to inform the administrator.

If after Content Gateway is installed and started for the first time Policy Broker is not available, there are no pre-existing settings to load. An Alarm is generated to alert the administrator of the condition.

Filtering Service resiliency

Content Gateway works with Web Security Filtering Service to perform policy enforcement. If Filtering Service becomes unavailable, there can be substantial latency in traffic handling.

Content Gateway has been tuned to provide better performance when requests to Web Security Filtering Service timeout and when Filtering Service becomes unavailable.

Every request that Content Gateway sends to Filtering Service must be completed within the communication timeout period. If it is not, the request is either permitted or blocked based on the **Action for Communication Errors** setting on the **Configure > My Proxy > Subscription > Scanning** page. When a communication timeout occurs, a dedicated monitor process continues to test the connection. If it fails 5 consecutive times, Filtering Service is marked down and the communication errors setting is applied until the monitor process detects that Filtering Service is responding.

Secured by RSA® authentication

TRITON Unified Security Center has been extended to support Secured by RSA authentication for TRITON administrators. See the v7.8.1 Release Notes for TRITON Unified Security Center.

Secured by RSA is a form of two-factor authentication that:

- Is configured for and applies to the TRITON Unified Security Center logon.

- **Can be made to apply to Content Gateway Manager** by forcing administrators to log on to the TRITON console before accessing the Content Gateway manager through the Web Security manager.
- Requires single sign-on (direct access) to be configured in Web Security manager for administrators allowed access to the Content Gateway manager.
- Requires that the Content Gateway manager password logon capability be disabled to prevent administrators not configured for single sign-on from accessing the Content Gateway manager directly via its IP address. See Configuring Content Gateway for two-factor authentication in Content Gateway Manager Help. If Content Gateway is deployed on an appliance, password access is disabled with an appliance manager command. See Configuring two-factor authentication in V-Series Appliance Manager Help.

For information about configuring two-factor authentication in the TRITON console, see Logging on with RSA SecurID authentication in TRITON console Help.

FIPS 140-2 mode

The **openssl** library used in FIPS 140-2 mode has been updated to 1.0.1e from 0.9.8r.

All of the cryptographic libraries used in Content Gateway version 7.8.1 have been submitted to the Cryptographic Module Validation Program (CMVP) for FIPS 140-2 certification. Visit the CMVP validation page for more information.

When Content Gateway is in FIPS 140-2 mode, cryptography within Content Gateway and on the HTTPS channel from the client to the proxy and from the proxy to the origin server, is performed with algorithms that conform to the FIPS 140-2 standard. However, where Content Gateway interfaces with some other Websense components there can be a FIPS 140-2 boundary.

- In Web Security Gateway Anywhere, traffic that flows through the cloud does not use FIPS 140-2.
- ThreatScope traffic does not use FIPS 140-2.
- Websense Data Security does not use FIPS 140-2.
- TRITON Mobile Security does not use FIPS 140-2.
- When RSA SecurID is configured for the TRITON console logon, the connection to RSA SecurID is not FIPS 140-2.

Important

Due to a system limitation, FIPS 140-2 mode cannot be used with NTLM user authentication (IWA fallback to NTLM or Legacy NTLM).

For more information about FIPS 140-2 mode in Content Gateway, see FIPS 140-2 Mode.

Office 365

Support for cloud-hosted and on-premises Microsoft Office 365.

When there is access to the Microsoft cloud, documents are synchronized with Microsoft Office 365 in the cloud. When there is no access to the cloud, Microsoft Office 365 applications are available locally.

On-premises support includes:

- Access in explicit and transparent SSL proxy deployments
- SSL decryption bypass
- Integrated Windows Authentication (IWA) and Legacy NTLM user authentication
- Integration with WebDLP and outbound Data Security (with Web Security Gateway Anywhere)

On-premises Office 365 application support includes:

- SkyDrive and Sharepoint:
  - Open file from Word/Excel/PowerPoint/OneNote/Publisher/Access
  - Save file from Word/Excel/PowerPoint/OneNote/Publisher/Access
- Outlook:Share document through email
- SkyDrive Pro: Verify synchronization from cloud to local host
- Upload files through Office Upload Center
- Lync Online

Cloud-hosted support includes:

- Access in explicit and transparent SSL proxy deployments
- SSL decryption bypass
- Integrated Windows Authentication (IWA) and Legacy NTLM user authentication
- Integration with WebDLP and outbound Data Security (with Web Security Gateway Anywhere)

Cloud hosted Office 365 application support includes:

- Create directory
- Create, Open, Edit, Save: Word/Excel/PowerPoint/OneNote

WCCP

Synchronize in the Cluster

When several instances of Content Gateway are deployed in a cluster, use the **Synchronize in the Cluster** option to control whether the WCCP configuration is propagated around the cluster. (The value of **Synchronize in the Cluster** is always synchronized in the cluster.)

When this option is enabled, the WCCP configuration (stored in **wccp.config**) is synchronized in the cluster and configuration changes can be made on any node.

When this option is disabled, the WCCP configuration is not synchronized in the cluster and changes to the WCCP configuration must be made individually on each node. A common use case for this is to control which service groups are enabled/ disabled on each node, and to use proportional load distribution with **weight**. An efficient way to set up WCCP in this scenario might be to enable **Synchronize in the Cluster** while establishing the basic WCCP configuration, and then disable it when you're ready to control service group enable/disable (or other WCCP configuration values) on each node.

If after being disabled this option is enabled, the configuration of the node on which it is enabled is used to synchronize all members of the cluster.

Use this option with caution: When **Synchronize in the Cluster** is disabled, you must visit each node in the cluster to examine and maintain your WCCP configuration. In addition to the added maintenance burden, it can make WCCP troubleshooting more difficult.

Lifts 7.7.x limits

When **Synchronize in the Cluster** is set to **Disabled** it effectively eliminates a limitation in which you cannot configure the following service group attributes separately for each node in the cluster:

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

Japanese language embedded Help

Japanese language embedded Help is included in version 7.8.1. To select Japanese, go to **Configure > My Proxy > UI Setup > General**, locate the **Default Help Language** drop down list and select Japanese (the selection is presented in Japanese). The setting does not apply to all nodes in a cluster. Each node must be configured separately.

The setting does not apply to any TRITON manager embedded Help language options.

Performance graphs

Two new Content Gateway performance graphs that monitor DNS activity. In the Content Gateway manager go to **Monitor > Performance > Overview**.

- **DNS Lookup Latency** shows the average time in milliseconds to fulfill a DNS request.
- **DNS Cache Usage** shows the number of DNS requests handled by Content Gateway, including those served by the DNS cache.

Removed: Support for the Microsoft ISA plugin

With the transition to 64-bit Content Gateway, support for 32-bit Microsoft ISA server in a proxy chain is deprecated.

Content Gateway continues to support 64-bit Microsoft Forefront TMG.

For more information, see Chaining Content Gateway with other proxies.

Installation and upgrade

Topic 60074 / Updated: 21-October-2013

Applies To:	Websense Content Gateway, version 7.8.1 (a component of Web Security Gateway / Anywhere)

The Websense Deployment and Installation Center is the complete resource for deployment, installation, and upgrade information for version 7.8.1 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 installation instructions start 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*

Hardware requirements

CPU	Quad-core running at 2.8 GHz or faster
Memory	6 GB minimum; 8 GB recommended
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

Red Hat Enterprise Linux

Content Gateway is certified on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.4: 2.6.32-358
  - Kernel version for 6.3: 2.6.32-279
- V-Series appliances

Content Gateway is supported on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.2: 2.6.32-220
  - Kernel version for 6.1: 2.6.32-131
  - Kernel version for 6.0: 2.6.32-71
- The corresponding CentOS versions, including updates 3 and 4 (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

Only kernels listed above are certified or supported. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

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

Websense, Inc. provides “best effort” support for the version of Red Hat Enterprise Linux and CentOS listed above. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion until the issue is deemed a Red Hat Enterprise Linux- or CentOS-specific issue, at which point you must contact Red Hat directly for assistance.

Websense recommends that the Red Hat Enterprise Linux version that will host Content Gateway be updated to the latest patch before running the version 7.8.1 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.

Websense Web Security Gateway / Anywhere

- Version 7.8.1 required

> **Important**
> Web Security Policy Server and Filtering Service must be installed before Content Gateway.

Websense Data Security

- Version 7.8.1
- Any version can be used via the ICAP interface. See Content Gateway Manager Help for configuration information.

Web browsers:

- Content Gateway is configured and maintained with a Web-based user interface called the Content Gateway manager. The Content Gateway manager supports the following Web browsers:
    - Microsoft Internet Explorer 8, 9, and 10

- Mozilla Firefox versions 5 and later, except version 11 (due to an error in the way version 11 handles importing certificates)
- Google Chrome 13 and later

✓ **Note**

Browser restrictions apply only to the use of the 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 v7.8.1 patch is applied. You do not need to download the installer.

To download the Content Gateway v7.8.1 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** (7.8.1).

   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 60075 / Updated: 23-December-2013

Applies To:	Websense Content Gateway, version 7.8 (a component of Web Security Gateway / Anywhere)

- *Installation*
- *Configuration*
- *Proxy user authentication*
- *SSL Internal Root CA*

Installation

Software installation location and file ownerships

Content Gateway is installed in **/opt/WCG**.

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.

Cluster handling during upgrades

Content Gateway tolerates different software versions in the same cluster. This is intended to simplify the process of upgrading a cluster. You should not run a cluster containing different versions 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.

‘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 support) is enabled, client browsers should be configured to send HTTPS traffic to proxy port 8080.

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”.

DNS proxy caching

The DNS proxy caching option allows Content Gateway to resolve DNS requests on behalf of clients. This option off-loads remote DNS servers and reduces response times for DNS lookups. You can use the DNS proxy caching option only with a layer 4 switch or a Cisco router running WCCP v2.

DNS proxy caching can only answer requests for A and CNAME DNS entries. Other types of request (e.g., MX) will not be answered.

Limitation: If the host name to IP address mapping is not in the DNS cache, Content Gateway contacts the DNS server specified in the **/etc/resolv.conf** file. **Only the first entry in resolv.conf is used.** This might not be the same DNS server for which the DNS request was originally intended.

See “DNS Proxy Caching” in Content Gateway Manager Help.

If your environment is configured such that you have DNS servers that resolve internal sites only and others that resolve external sites only, see Using the Split DNS option in Content Gateway Manager Help.

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 (prompt-less).

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

Browser/ Operating System	Internet Explorer (v9, 10 tested)	Firefox	Chrome	Opera (v12.02 tested)	Safari (v6.02 tested)
Windows	Performs transparent authentication	Performs transparent authentication (v21 tested)	Performs transparent authentication (v26, 27 tested)	Falls back to NTLM and prompts for credentials	Falls back to NTLM and prompts for credentials
Mac OS X	Not applicable	Performs transparent authentication (v21 tested)	Browser issue prevents IWA from working (v23 tested)	Not tested	Performs transparent authentication
Red Hat Enterprise Linux, update 6	Not applicable	Performs transparent authentication (v11 tested)	Browser issue prevents IWA from working (v27 tested)	Not tested	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 Internal Root CA

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 default Root CA (presented to clients) is signed with 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: Data Security

If Web Security Gateway Anywhere and Data Security are deployed together and upgraded from v7.7.x to version 7.8.x, 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 60076 / Updated: 21-October-2013

Applies To:	Websense Content Gateway, version 7.8 (a component of 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 in to MyWebsense, the link takes you to a login prompt. Log in to view the list.