Websense Content Gateway v7.5.2 Resolved and Known Issues

Topic 55144 / Updated: 14-September-2010

Applies To:	Websense Content Gateway v7.5.2

This list of known and resolved issues in Content Gateway version 7.5.2 is available to customers with a current MyWebsense account.

See the Release Notes for information about new features in this Content Gateway release.

See this topic for information about corrections in earlier releases of Websense Content Gateway.

Resolved issues

Configuration changes save properly

You are now able to save configuration changes made via Content Gateway Manager after viewing any log files in the management console. You no longer see these error messages at Restart: “Unable to read or write config file” or “Permission denied.”

Reset alarms now generate expected emails

You now receive the expected email message alert whenever a proxy reset occurs for an out-of-memory condition, malformed response, and other interruptions, if you have enabled reset alarms in the file **records.config**.

SSL Incident list shows correct URL

The SSL Incident List now shows the correct URL in the default tunnel rule for gotomeeting.com.

Tunneled ports can be cleared in management console

You can now use the Content Gateway Manager to remove all tunneled ports. Browse to **Configure > Protocols > HTTP > General**. Remove the Tunnel Ports that are listed and click **Apply**. This console option was not working correctly in the previous version.

FTP sites render completely with IE6

FTP sites accessed using Internet Explorer (IE) version 6 now render completely and no longer display the underlying HTML code.

Disabling NTLM credential caching

If you enable and configure NTLM with credential caching, and then later disable NTLM credential caching, credentials are no longer pulled from the cache.

Proxy authentication headers handled correctly

Websense Content Gateway was incorrectly treating proxy authentication headers as case-sensitive. This caused some clients, such as Windows Media Player, to occasionally fail to authenticate. Content Gateway is now case-insensitive when examining authentication headers, in compliance with the HTTP RFC.

Google AdWords client routes will SSL on

It is now possible to route traffic from the Google AdWords client successfully through Websense Content Gateway with SSL turned on.

Terminal server users accessing HTTPS sites identified correctly

Terminal server users are now identified correctly, and the correct filtering policy is applied to them, when the users access HTTPS sites with SSL Manager enabled.

iDisk file uploads successful

File transfers with the iDisk application at idisk.mac.com now upload successfully when proxied by Content Gateway.

ISO images and other large files download successfully

Large files such as ISO images can now be downloaded successfully.

HTTPS Post (URL) correct when ICAP in use

The correct URL is now sent from Websense Content Gateway to the Policy Engine when an HTTPS POST transaction is performed and ICAP Server is in use.

Known issues in this release

Manual authentication overrides SSL category bypass

Sites using transparent proxy mode with WCCP may see SSL Web sites decrypted, even when those sites belong to categories for which SSL Bypass has been configured.

When Manual Authentication is required for SSL sites, Websense software decrypts SSL sites (instead of bypassing them), because authentication is overriding the SSL Bypass.

A workaround is to remove the requirement for Manual Authentication.

Transparent Authentication with WCCP can fail in cookie mode

If your site has two or more Content Gateway instances pointing to the same WCCP router, do not use Cookie mode for credential caching. Instead, use IP mode.

If Cookie mode is in use, for most of the time the authentication works correctly. However, a user may receive 'Page cannot be displayed' instead of being forwarded to a block page.

To check this setting, navigate to **Configuration > Security > Access Control > Transparent Proxy Authentication**. Ensure that **Authentication Mode** is set to **IP mode** (the default). Click **Apply** if you made a change, and then restart the proxy to put the change into effect.

In IP mode, the client IP address is associated with a username when the session is authenticated. Requests made from that IP address are not authenticated again until the Session TTL expires (default = 15 minutes). Requests made from that IP address within the time-to-live are considered to be made by the user associated with that IP address.

WCCP proxy cluster with IP spoofing requires source-based distribution

When a site deploys multiple Content Gateway servers in a WCCP cluster, with IP spoofing enabled, the default configuration for WCCP does not distribute the cache appropriately.

The workaround is to modify the default hash assignment to select source-based distribution.

Advertise packets not matching value in records.config

For routers and switches that support both GRE and L2, after Websense Content Gateway has registered for WCCP with the router (or switch), the device caches the negotiated mode, until Websense Content Gateway is de-registered.

De-registration occurs only if 3 heartbeat messages fail, and there is no response from Websense Content Gateway.

If your site changes the negotiation mode on Websense Content Gateway after it has registered once, and then restarts Websense Content Gateway, note that Content Gateway does not get de-registered. This is because the restart completes before 3 heartbeat failures. Thus, the router (or switch) mode still has the last value negotiated prior to the restart.

Websense Content Gateway also advertises this same value, and thus the file records.config does not match the advertised capability.

The workaround in this case is to disable WCCP in Websense Gateway Manager and wait until it de-registers, and then enable WCCP again. At that point, the router will advertise both GRE and L2, and Websense Content Gateway will choose the one configured in records.config.

Preferred method for changing the mode:

1. Disable WCCP on the router (all service groups to proxies).
2. Wait for all service groups to expire on proxies (1 minute).
3. Make desired changes on all proxies.
4. Enable WCCP on the router.

Alternate method for changing mode: (no access to switch or router):

1. Disable WCCP on the proxies.
2. Wait for all service groups to expire on the router (1 minute after last proxy is disabled).
3. Make changes on all proxies.
4. Enable WCCP on all proxies.

Keep in mind:

The router can choose the mode it wants, regardless of what the proxy asks or advertises.

Changing forwarding/redirect methods is best done in a maintenance window. A change of this sort requires all proxies to be de-registered (otherwise the router attempts to preserve the existing methods, regardless of the proxies' capabilities).

Websense Content Gateway auto-negotiates successfully even when it has been misconfigured in Content Gateway Manager. This means that it will never advertise a mode that the router doesn't support.

Cache distribution incorrect with WCCP cluster and IP spoofing

When a site deploys multiple Content Gateway servers in a WCCP cluster with IP spoofing enabled, the default configuration for WCCP does not correctly distribute the cache to the cluster.

The workaround is to modify the default hash assignment to select source-based distribution.