# Websense Content Gateway Release Notes v7.5.2

Release Notes: Topic 55143 / Updated: 06-October-2010

| | |
|---|---|
| **Applies To:** | Websense Content Gateway v7.5.2 |

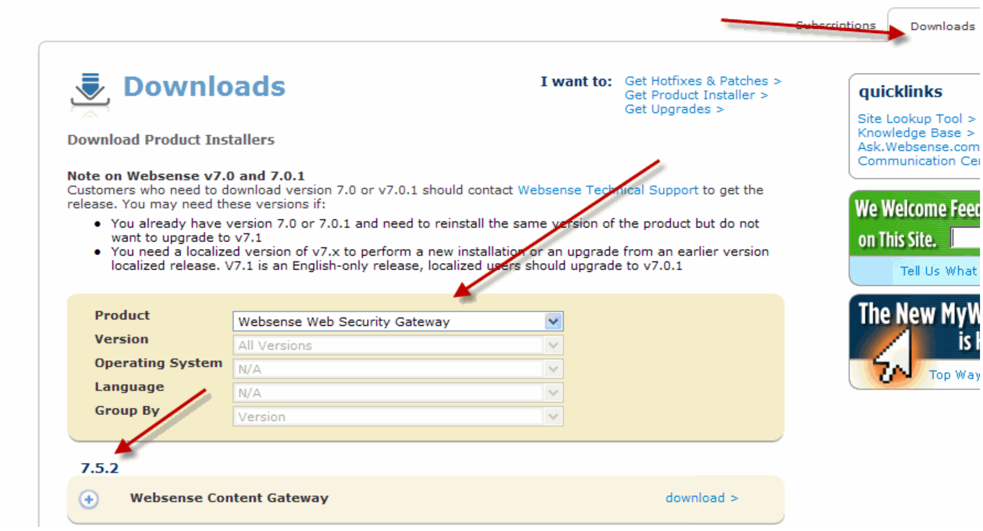
*New features in v7.5.2*

*Known and Resolved issues*

## How do I get the patch files?

Go to MyWebsense.com and log in.

Then choose the **Downloads** tab, and Websense Web Security Gateway, as shown in this screen:



Download Product Installers

**Note on Websense v7.0 and 7.0.1**
Customers who need to download version 7.0 or v7.0.1 should contact Websense Technical Support to get the release. You may need these versions if:

- You already have version 7.0 or 7.0.1 and need to reinstall the same version of the product but do not want to upgrade to v7.1
- You need a localized version of v7.x to perform a new installation or an upgrade from an earlier version localized release. V7.1 is an English-only release, localized users should upgrade to v7.0.1

| | |
|---|---|
| **Product** | Websense Web Security Gateway |
| **Version** | All Versions |
| **Operating System** | N/A |
| **Language** | N/A |
| **Group By** | Version |

**7.5.2**

**Websense Content Gateway** download >

# New features in v7.5.2

Version 7.5.2 contains important corrections for the Content Gateway module, as well as several new features.

## ARM module now certified for use with RHEL 5.5

The Adaptive Redirection Module (ARM) of Websense Content Gateway is now certified for use with Red Hat Enterprise Linux v5.5.

## Port range for tunneled ports

The tunnel ports option in the Content Gateway Manager at **Configure > Protocols > HTTP** now supports port ranges. This allows you to permit proxy tunneling to all ports (1-65535), or specific ranges of ports.

## Skype

The VOIP application Skype can now tunnel through the Content Gateway proxy when SSL decryption is *enabled*.

To enable Skype tunneling when SSL decryption is enabled, access Content Gateway Manager and navigate to **Configure > Protocols > HTTPS**. In the Tunnel Skype option at the bottom of the page, click Enabled. You may need to restart Content Gateway.

Note that Skype tunneling works only for clients who are accessing Content Gateway in explicit proxy deployments.

You don’t need to set the Tunnel Skype option if SSL decryption is not in use. Skype tunneling works properly when SSL decryption is *disabled*, regardless of the setting for the Tunnel Skype option.

## Compatible with Data Security Management Server v7.5.3

Websense Content Gateway v7.5.2 includes all new features and corrections included in the integrated policy engine from Data Security Suite v7.5.3.

Content Gateway v7.5.2 is compatible with all v7.5 versions of the Data Security Management Server, including v7.5.3 and later versions, but Websense recommends that customers upgrade to Data Security Suite v7.5.3 prior to upgrading to Content Gateway v7.5.2.

## ICAP server failover capability added

Content Gateway now has the ability to fail over to a backup ICAP server if the active ICAP server fails. Load balancing between multiple ICAP servers is also an option.

In previous releases, Content Gateway could reference only a single ICAP server, with the option to fail open if that server was unresponsive.

You can now configure a backup ICAP server in case the primary ICAP server fails. The proxy detects the failed machine and sends traffic to the secondary. If the secondary becomes unresponsive, the proxy uses the primary. If no ICAP servers are available, the proxy fails open.

## Time to fail over

Content Gateway may experience temporary request-processing latency between the time the real failure occurs and the time Content Gateway has marked the failed server as down. After the failed server is marked down, all new requests are sent to the second ICAP server. The time to failover is primarily limited by the connection timeout configuration.

## Failure conditions leading to failover

- ICAP request failed due to layer-3 failure (twice for the same request)
- Failure to connect to a port within a given timeout
- Failure to send request (server resetting connection, and the like)

## Excluded failure conditions

Content Gateway does not consider missing, invalid, or slow responses as a failure.

However, Content Gateway does verify that the ICAP server is valid at startup by verifying the response to the ICAP OPTIONS request.

## Recovery Conditions

After the failed server is marked down, new requests are sent to the second server. No new ICAP requests are sent to the failed server until that server is detected to be alive again, based on the recovery conditions below.

Content Gateway tests for recovery conditions for each down ICAP server at a specified interval. If load balancing is disabled, requests continue to be sent to a secondary ICAP server until the primary comes back online. If load balancing is enabled, Content Gateway starts sending requests to a server (round-robin) as soon as it is marked up.

- TCP connection success
- Successfully sent OPTIONS request
- Successfully received valid response to OPTIONS request

### Recovery actions

Upon server recovery (server comes back online and is marked as up)

- Load balancing ON: Requests start being distributed to the newly up server (round-robin)
- Load balancing OFF: If the primary server recovers, all requests start being sent to the primary. If the secondary server recovers, traffic continues to be sent to the primary, until the primary goes down.

### Fail open

If all ICAP servers are down, a configuration option allows fail open or fail closed behavior. When all ICAP servers are down, the background thread continuously attempts to reestablish a new connection with each.

### Configuration settings

These ICAP failover parameters are set in the file **records.config** (defaults shown):

- CONFIG proxy.config.icap.ActiveTimeout INT 5

  (read/response timeout in seconds, considered a failure if timeout exceeded)
- CONFIG proxy.config.icap.RetryTime INT 5

  (recovery interval in seconds; interval to test whether a down server is back up)
- CONFIG proxy.config.icap.ICAPUri STRING icap://1.2.3.4:1344/reqmod,icap://4.3.2.1:1344/reqmod

  (comma-separated list of ICAP URIs)
- CONFIG proxy.config.icap.LoadBalance INT 1

  (distribute ICAP requests across available icap servers. 1=yes, 0=no)
- CONFIG proxy.config.icap.FailOpen INT 1

  (if no ICAP servers are online. 1= fail open, 0=fail closed with block page)

## Known and Resolved issues

A list of known and resolved issues in this release is available to customers with a current MyWebsense account. If you are not currently logged in to MyWebsense, the link above takes you to a login prompt. Log in to view the list.