Release Notes

for Websense Web Filter, Web Security, and Web Security Gateway | v7.6.5

Topic 50206 / Updated: 08-May-2012

Applies To:	Web Filter 7.6.5 Web Security 7.6.5 Content Gateway 7.6.5 Web Security Gateway 7.6.5 Web Security Gateway Anywhere 7.6.5 V-Series Appliance v7.6.5

Version 7.6.5 is a stability and maintenance release for Websense Web security solutions. It rolls up many resolved issues and adds a small number of improvements requested by our customers for the v7.6.x series of Web security modules.

Use the Release Notes to find information about what's changed and improved in version 7.6.5.

- *New in version 7.6.5*
- *Installation and upgrade*
- *Resolved and known issues*

New in version 7.6.5

Topic 50207 / Updated: 01-May-2012

Applies To:	Content Gateway Version 7.6.5 (a component of Web Security Gateway and Web Security Gateway Anywhere Version 7.6.5)

- *SSL certificate verification engine (CVE) enhancements*
- *Support in Web Security Gateway for "Google Apps for Business," "YouTube for Schools," and other sites with a custom header*
- *New fallback option*

SSL certificate verification engine (CVE) enhancements

- The certificate authority (CA) store has been updated with several new CAs. The added CAs can reduce the number of new CAs added to the store when clients browse the Web. This, in turn, can reduce the number of “explicitly denied” errors that may result after a new CA is added to the store.

  The changes also help to prevent “local user not found” and “expired certificate” errors for certificates that have been renewed recently.
- The logic for “Block certificates with no CRL URI and no OCSP URI” has been improved, to be more consistent with administrator expectations. This will reduce the number of incorrect “Unknown revocation state” failures.
- SSL connection logic has been improved for sites that **do not** support SNI. If the SSL handshake with a server fails with SNI enabled, then another attempt is now made without SNI. In this way, Websense software is able to connect to servers that are not SNI-compliant. And, this prevents users from receiving “Common Name mismatch” errors when SNI is provided. Customers who had previously disabled SNI are encouraged to enable it with the new version.
- Clients using a Google Chrome browser (version 18.0.0 or higher) or a Safari browser to request SSL Web sites would receive a warning from the browser that said: “The site’s security certificate is signed using a weak signature algorithm.” Clients were unable to access an SSL Web site. Content Gateway now uses a more secure SHA-1 algorithm (instead of MD5) to sign SSL certificates, resulting in increased access.

Support in Web Security Gateway for “Google Apps for Business,” “YouTube for Schools,” and other sites with a custom header

Web Security Gateway (Anywhere) now supports YouTube for Schools and Google Apps for Business.

Special configuration of Content Gateway filtering rules makes this possible.

For example, you can now allow Google Business Gmail while simultaneously blocking Google *personal* gmail.

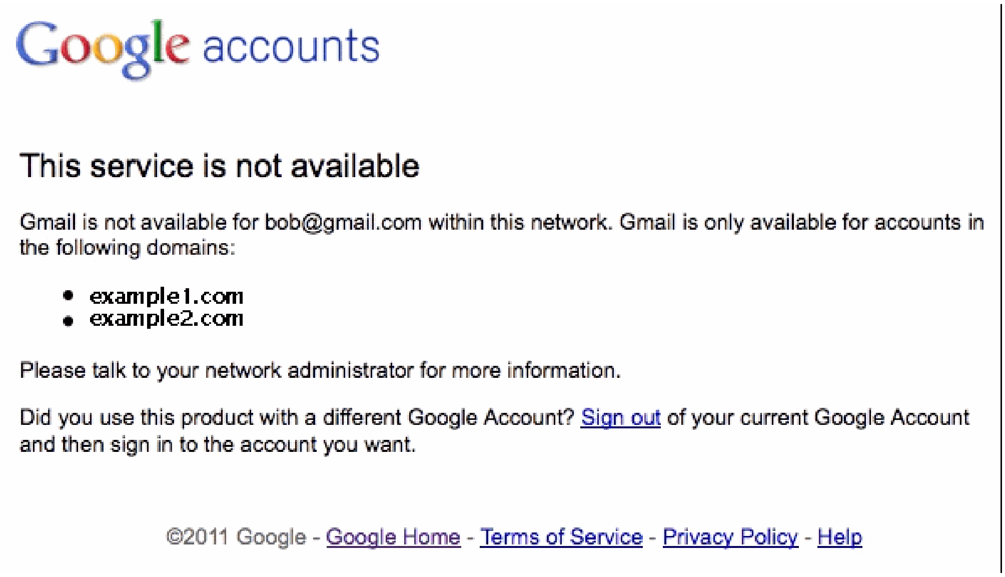
In Content Gateway, to allow YouTube for Schools or Google Apps for Business (or any host that supports filtering via custom headers), define the filtering rule type **add_hdr**. This causes a custom header-value pair to be inserted, providing support for destination hosts (such as YouTube for Schools) that require a specific header-value pair.

You can create an **add_hdr** rule for any host that supports filtering via custom headers. Following are two setup examples.

Example One: Google Apps for Business

Google supports a custom header in the request, containing a comma-separated list of domains that the administrator wants to allow. For example, with the custom header “X-GoogApps-Allowed-Domains”, if the header has the value “domain1.com, domain2.com”, then “user@domain1.com” and “user@domain2.com” are allowed, but “user@xyz.com” is blocked by Google.

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



Google accounts

This service is not available

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

- example1.com
- example2.com

Please talk to your network administrator for more information.

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

©2011 Google - Google Home - Terms of Service - Privacy Policy - Help

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

To implement the solution for Google Apps for Business:

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

Creating an **add_hdr** rule:

1. Go to the **Configure > Security > Access Control > Filtering** tab and click **Edit File** to open **filter.config**.
2. For **Rule Type** select **add_hdr**.
3. For **Primary Destination Type** select **dest_domain**.
4. In **Primary Destination Value** specify “mail.google.com”.
5. In the **Custom Header** field specify “X-GoogApps-Allowed-Domains”.
6. In the **Header Value** field specify your domain. For example: www.example.com.
7. Click **Add** to add the rule.

8. Click **Apply** to save all the changes, and then click **Close** to close the edit window.
9. To put the new rules into effect, select the Content Gateway Manager window and restart Content Gateway.

For Google's description of this filtering solution, see the article Block access to consumer accounts and services while allowing access to Google Apps for your organization.

Example Two: YouTube for Schools

To create an **add_hdr** rule to allow YouTube for Schools, do the following:

1. In Content Gateway Manager, go to the **Configure** > **Security** > **Access Control** > **Filtering** tab and click **Edit File** to open **filter.config** in the file editor.
2. For **Rule Type** select **add_hdr**.
3. For **Primary Destination Type** select **dest_domain**.
4. In **Primary Destination Value** specify "youtube.com".
5. In the **Custom Header** field, specify "X-YouTube-Edu-Filter".
6. In the **Header Value** field, specify your unique edufilter value.
   For example: 1234abcd
7. Click **Add** to add the rule.
8. Click **Apply** to save all the changes, and then click **Close** to close the edit window.
9. To put the new rule into effect, select the Content Gateway Manager window and restart Content Gateway.

You can create an **add_hdr** rule for any host that supports filtering via a custom header.

New fallback option

A new selection has been added to enable your site to fall back to your default policy when **Fail Open** is desired.

In Content Gateway Manager, when you configure the NTLM global settings (**Configure** > **Security** > **Access Control** > **Global Authentication Options** tab), you now have three choices for **Fail Open**:

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

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

When this setting is **enabled only for critical services failures**, requests proceed if authentication fails because there is no response from the domain controller or because the client is sending badly formatted messages.

When **enabled for all failures**, requests proceed for all authentication failures, even password failures.

In all of these situations, if a policy has been assigned to the client's IP address, that policy is applied. Otherwise, the Default policy is applied.

By default, **Fail Open** is set to **Enabled only for critical services failures**.

Set **Fail Open** to **Disable** if you want to stop requests from proceeding to the Internet when authentication failure occurs.

Installation and upgrade

Topic 50208 / Updated: 08-May-2012

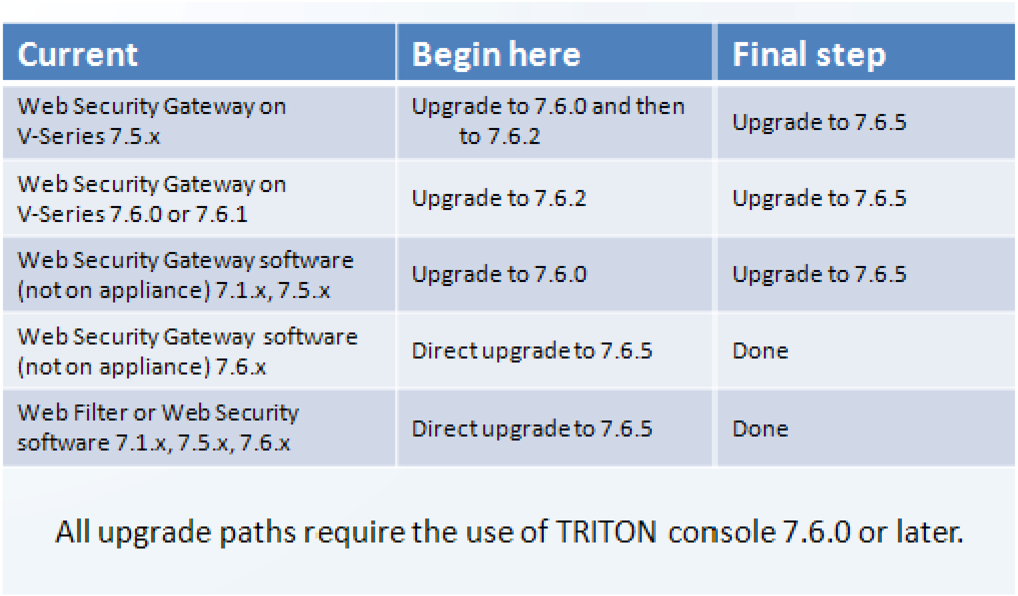
Applies To:	Web Filter 7.6.5 Web Security 7.6.5 Content Gateway 7.6.5 Web Security Gateway 7.6.5 Web Security Gateway Anywhere 7.6.5

Always perform a full backup of all servers and save the backup files to a secure location, before upgrading to a newer version of Websense solutions.

Sites upgrading software-only versions of Websense Content Gateway need to see the first Known Issue about a certificate authority that is known to be compromised.

Please see the online Deployment and Installation Center for instructions on installing and deploying Websense Web security products at v7.6.5.

Refer to the Upgrade Center for instructions about upgrading to v7.6.5 from a previous version. The upgrade follows standard Websense upgrade processes.



Current	Begin here	Final step
Web Security Gateway on V-Series 7.5.x	Upgrade to 7.6.0 and then to 7.6.2	Upgrade to 7.6.5
Web Security Gateway on V-Series 7.6.0 or 7.6.1	Upgrade to 7.6.2	Upgrade to 7.6.5
Web Security Gateway software (not on appliance) 7.1.x, 7.5.x	Upgrade to 7.6.0	Upgrade to 7.6.5
Web Security Gateway software (not on appliance) 7.6.x	Direct upgrade to 7.6.5	Done
Web Filter or Web Security software 7.1.x, 7.5.x, 7.6.x	Direct upgrade to 7.6.5	Done

All upgrade paths require the use of TRITON console 7.6.0 or later.

Resolved and known issues

Topic 50204 / Updated: 08-May-2012

Applies To:	Web Filter 7.6.5 Web Security 7.6.5 Content Gateway 7.6.5 Web Security Gateway 7.6.5 Web Security Gateway Anywhere 7.6.5

A separate list of Resolved and Known issues for this release is available to customers with a current MyWebsense account.

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

- Web Filter / Web Security
- Websense Content Gateway
- V-Series Appliances