2014 Release 5 Notes for Websense® Cloud Web Security

Updated: 14-October-2014

Applies To:	Websense Cloud Web Security, 2014 Release 5

2014 Release 5 updates the portal look-and-feel and introduces new reporting for Cloud Web Security. These features are available from mid-September and are covered by separate release notes. This document covers stage 2 of the release, available from mid-October 2014, which provides a small number of features and important corrections for Cloud Web Security customers.

Use the Release Notes to learn about:

What's new in Cloud Web Security Release 5?

Defining group and policy assignment for synchronized users

> **Note**
> This is a limited-availability feature that is not enabled in all accounts. For more information, contact cloudpm@websense.com.

If available in your account, you can select how synchronized users are assigned to web policies if they appear in more than one group in the directory. Go to **Account > Groups**, click the **Policy assignment method** link, and select one of the following:

- **Directory hierarchy** means that a user in multiple groups is assigned to the policy associated with the group that has the fewest intermediate group memberships. For example, if a user is a member of GroupA, and is also a member of GroupB which itself is a member of GroupC, the policy for GroupA takes precedence.
- **Group ordering** means that a user in multiple groups is assigned to the policy associated with the group highest in the list on the **Groups** page. If you change the order of the groups by dragging and dropping the group names in the list, the user's policy assignment also changes.

Data loss detection

Data loss detection is a limited-availability feature for Cloud Web Security Gateway early adopters only. For additional information about this feature, please fill out the online registration form.

Category updates

A number of new web categories are available for management and reporting. For more information, please refer to the Category Updates 2014, Quarter 3 knowledge article.

Resolved and known issues

Resolved issues

- A web form was being mis-categorized as an executable. Improvements have been made to reduce the likelihood of false positives.
- Basic authentication can now be enforced if single sign-on is used.

Known issues

The following issues either cannot be fixed, or are not currently scheduled to be fixed:

Web Endpoint

- When users install an up-to-date version of Windows endpoint, the endpoint summary report shows the Windows endpoint version as outdated, because the Mac endpoint version has a higher number than the Windows version.
- On machines where the Mac endpoint is installed, for certain types of users (e.g., root), it looks like they can edit the network proxies page. However, any changes made here are not saved. The endpoint's resistance to tampering continues to work.
- It is possible to delete the Mac endpoint in the System Preferences pane. This will not affect the operation of the endpoint. If this occurs, use the command line tools instead of the user interface to get the debug logs and to uninstall the endpoint.

  To have the endpoint re-appear in System Preferences, copy "/Library/PreferencePanes/WebsenseEndpoint.prefPane" to the same directory from another machine on which the Mac endpoint is installed.

Policies

- For users whose organizations choose to display the acceptable use policy compliance page, this page appears for each different browser they use within the frequency period selected (1, 7, or 30 days). For example, if they browse using Internet Explorer and Chrome within the same time period, the page appears twice, and they must agree to accept the page twice. Note that when using the endpoint auto-install feature, this same issue occurs.
- The acceptable use policy compliance page appears the first time an end user browses to an HTTP site and does not appear if the user browses to HTTPS or FTP sites. Note that when using the endpoint auto-install feature, this same issue occurs.
- In the File Blocking tab, file extensions for HTTPS remain blocked even if they are set to Allow.

Authentication

- When an authentication session times out and the end user re-authenticates in the same browser session, there is an intermittent issue that redirects the user to the URL requested after the initial authentication. This can occur if the user has

opened several tabs: they are redirected to the URL opened after authentication in the first tab.

- The New Tab page in Chrome displays “Internal Server Error” when a user authenticates using a cookie-based method (secure form authentication or single sign-on). To work around this, open a new tab in the browser and re-authenticate to browse successfully.
- This issue relates to the cloud and hybrid proxy. When using Internet Explorer, users may receive the welcome page for basic authentication instead of the welcome page for secure form-based authentication after the secure form-based authentication session expires. They can either restart the browser or browse to a different site.

i-Series appliance

- In cases where the appliance self-signed certificate is used or when the CA certificate is not loaded on clients, Chrome blocks the connection and displays an error page.

  To proceed past this error page, ensure the browser page is the active window, and then type **proceed**. For Chrome versions 33 and 34, type **danger**.

  To prevent this issue occurring, end users should not use the appliance self-signed certificate and should load the CA on their clients.
- The YouTube for Schools feature does not work for HTTPS sites. To work around this, you can redirect this traffic to the cloud: ensure you enable SSL decryption in your policy and under SSL Decryption Categories, set the YouTube category to Decrypt.
- The appliance does not currently support authentication decryption bypass for custom categories.
- When using a Windows XP machine with Internet Explorer 8 (or below), HTTPS connection are not supported on i-Series appliances.
- If you add a custom protocol with a name containing non-ASCII characters, an error occurs on the appliance and the new protocol is not added.
- The appliance does not support browsing directly to full URLs (i.e. those including a full path to a specific page) in custom categories for SSL traffic. Using the host name only is supported.

Technical Support

Websense provides technical information about Websense products online 24 hours a day, including:

- latest release information
- searchable Knowledge Base
- show-me tutorials
- product documents
- tips
- in-depth technical papers

Access support on the website at:

www.websense.com/content/support.aspx

If you need additional help, please fill out the online support form at:

www.websense.com/content/contactSupport.aspx

Note your case number.

Third-Party Software Notice

Websense, Inc., provides software solutions that integrate with your existing environment. In the complex environments that are common in today's marketplace, this involves interacting with a variety of third-party software products. In some cases, Websense, Inc. makes an effort to simplify the acquisition of this third-party software. However, you must obtain any upgrades and enhancements to those products directly from the third-party vendor.

If you have questions, contact Websense Technical Support for additional information.