2015 Release 3 Notes for Websense Cloud Web Protection Solutions

Websense Cloud Web Protection Solutions | 29-June-2015

2015 Release 3 of our web protection products offers new features and includes a number of product corrections:

- *What's new in 2015 Release 3?*
  - *Google redirect*
  - *Privacy protection updates*
  - *Global authentication page for single sign-on users*
  - *New error pages for connection issues*
  - *Reporting updates*
  - *OpenSSL version updated*
- *Resolved and known issues*

What's new in 2015 Release 3?

Google redirect

> **Note**
> This is a limited-availability feature that may not be available in your account.

If you wish to control the Google domain that your end users see, you can now choose to override Google's standard redirect behavior. By default, Google redirects browsers to the appropriate site for the country it detects (for example, google.fr for France). However, sometimes this is not accurate, for example if your end users are browsing through a cloud service proxy that is in a different country.

To use this feature, you should enable SSL decryption for the Search Engines and Portals category on the **SSL Decryption** tab, and install the Websense root certificate on end user machines.

To define Google redirect behavior for the policy, go to a policy's **General** tab, then:

1. Select **Override Google redirect behavior**.

   If you have not already enabled SSL decryption for the Search Engines and Portals category, a warning message appears at this point. You can enable SSL decryption directly from this dialog box.

2. Select one of the following options:

   - **Ensure requests for google.com are not redirected** – This option prevents Google from redirecting to a local country site when the end user enters "google.com".
   - **Redirect requests for google.com to** – This option ensures all google.com requests are redirected to a local country site of your choice. Enter the country code in the text field (for example, **fr** for google.fr, or **co.uk** for google.co.uk).

3. Click **Save** when you are done.

You can also configure Google redirect behavior for specific connections within your policy, when you add or edit a proxied connection on the **Connections** tab. If you configure Google redirect behavior for both the policy and a connection, the settings for the connection take precedence over the policy settings. If you do not configure Google settings specifically for the connection, it uses the behavior configured at policy level, if any.

Note

For i-Series appliance traffic, note the following:

- Google redirect does not apply to traffic coming from clients defined as session-based. This traffic is first directed to Google for termination before being redirected to the cloud service, and in such cases Google redirects to the local country site.
- This feature does not work correctly if a user browses to http://www.google.com and Google does not automatically change this to https://www.google.com. In this case, traffic is not redirected to the cloud service and Google applies its own redirect to the appropriate site for the country it detects, rather than the options set in the cloud portal. If the country site selected by Google conflicts with your cloud settings, add "google.com" to the **Always analyze** list on the Web Content & Security tab to ensure traffic redirection to the cloud.

Privacy protection updates

If you are a TRITON AP-MOBILE user, the IMEI number can now be anonymized in web reports. To enable this option, go to the **Account** > **Privacy Protection** page, and

select **Anonymize end user information**. Then select the IMEI number attribute for anonymization.

Note that if you also select **Preserve end user information for security threats,** any attributes that you select are not anonymized for web traffic considered to be a security risk.

Global authentication page for single sign-on users

A new authentication page has been added for roaming single sign-on end users who need to authenticate with the cloud service. This enables the service to identify the single sign-on identity provider of the roaming user's account, and then execute the single sign-on process.

The authentication page asks the end user to provide their email address. The page is not visible or editable in the cloud portal.

New error pages for connection issues

Additional error pages have been added for cases where the cloud service proxy cannot connect to an HTTPS site. These pages cover the following cases:

- SSL connection errors
- Network or system error (for example, the site is currently unavailable)
- DNS error

Reporting updates

The following updates have been made in web reporting:

- The Date range popup window now includes the option to select a custom time zone for a report. By default the time zone is automatically detected and reports are generated in the user's local time zone. Selecting a custom time zone means the report is always generated for that time zone, regardless of the user's location.
- Scheduled reports now include the option to password-protect the report. If you select this on the **Delivery Options** tab, you must enter and confirm a password that the report recipient must use to view the report contents. Ensure the password is distributed securely to all report recipients.
- When adding or editing a scheduled report job, manually entering one or more email addresses in the **Other recipients** field triggers a warning message on clicking **Next** or **Save**. This is to ensure the recipients are authorized to receive the reports.

OpenSSL version updated

The version of OpenSSL used in the cloud service has been upgraded to protect against newly-published vulnerabilities.

Resolved and known issues

Resolved issues

Reporting and Dashboard

- When Privacy Protection is enabled, the attributes you select to be anonymized in reports map to columns in the Transaction Viewer. The string used to replace data to be anonymized is now the same for each attribute ("Not available").
- When Privacy Protection is enabled for data loss incidents, selecting the Source IP attribute under the Privacy Protection settings now anonymizes the corresponding values in the Incident Manager report.

Endpoint

- The **Web > Endpoint** page now displays correctly after setting the anti-tampering password.

Directory synchronization

- Directory synchronization was failing when a new group was synchronized with a duplicated DN, but different CN and GUID.

Known issues

The following are known issues in this version of the cloud web protection products:

Endpoint

- The Endpoint Auditing report has the following known issues:
  - All times in the report are based on the time zone of the machine used to view the report, rather than the end-user machine on which the endpoint is installed.
  - If communication to the endpoint client machine is lost or the machine enters suspend or hibernate mode, this change of state is not reflected in the report.
  - If an end-user machine is shut down, the endpoint is automatically enabled on restart regardless of its previous state, and this is not reflected in the report.

- If the endpoint is automatically installed from the cloud and then immediately disabled, end user details are not associated with a policy, and the disable action is not reflected in the report until the endpoint is re-enabled and the end user starts browsing.
- When an endpoint version is upgraded, either manually or via GPO, the endpoint is enabled even if it was previously disabled. This is not reflected in the report.

- 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.

Data Security

- When an end user composes an email message using Gmail, as soon as any sensitive information is entered, an incident is generated every time Gmail auto-saves the message.

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.

Trademarks