2014 Release 3 Notes for Websense® Cloud Security

Updated: 16-April-2014

Applies To:	Websense Cloud Security Solutions, 2014 Release 3

Use the Release Notes to learn about:

What's new in Websense Cloud Security Release 3?

Cloud Web Security features

Category-based bypass for single sign-on

If end users authenticate with either single sign-on or secure form-based authentication, web traffic is decrypted as part of the authentication process, regardless of whether SSL decryption is enabled in the policy. There may be some

categories with privacy implications where you do not want this decryption to occur, for example financial data sites.

To define a web category that is never decrypted during authentication, select the category in the **Available categories** list, and click the **>** button to move it to the **Selected categories** list.

Note the following for the selected categories:

- The selections apply only to end users browsing from proxied connections. They do not apply to roaming users.
- Users browsing these categories will be considered anonymous for both policy enforcement and reporting.

Override privacy protection for security events

You can now override privacy protection in the event of a security threat on the **Account Settings > Privacy Protection** page. To enable this feature, mark **Preserve end user information for security threats**.

Changing the end user password

End users can now change their password for basic authentication by clicking a link from the Welcome page, rather than needing to respond to an email message. As part of this update, 2 notification pages – Password Change and Password Change Complete – are available to edit under **Web Security > Block & Notification Pages**.

Using an existing policy as a template for new policies

When creating a new policy, you can now choose to use an existing policy as a template. To do this:

1. On the **Web Security > Policy Management > Policies** page, click **Add**.
2. Enter a policy name and administrator email address.
3. Select **Existing policy**, and choose one of your policies from the drop-down list. All of the current settings in that policy are copied into your new policy, except for the following:
   - Proxied connections
   - End user details

- Category and application control exceptions

> **Note**
> Selecting **Default** from the policy template drop-down is different than selecting the Default policy from the **Existing policy** drop-down. The first option applies only to web category blocking, while the second option uses the settings across all tabs in the Default policy for your new policy.

You can select a policy template only when creating a new policy. Once you have saved your settings for a new policy on the General tab, you cannot select a different template.

Cloud Email Security features

ThreatScope™ enforce option

ThreatScope sandboxing now includes the **Enforce** option in addition to **Monitor only**. **Enforce** holds any messages with attachments sent for analysis, and then quarantines those messages found to contain malicious attachments.

ThreatScope details in Message Center

Messages analyzed by ThreatScope are now visible in the Message Center as follows:

- To search for analyzed messages, select ThreatScope under the ThreatSeeker options. You can refine this further by selecting a ThreatScope status from the drop-down list: choose from All, Clean, Malicious attachment(s), Malicious and pending further analysis, and Pending analysis.
- The message details page now shows a details of the ThreatScope status and links to reports if a message has been found to be malicious.

Anti-spoofing checks for internal domains

On the Antispam tab in a policy, select **Filter spoofed messages of domains in this policy** to detect and act on messages sent from domains within the policy to recipient domains within the policy, where the sender address has been spoofed.

A sender address is considered to be spoofed if the following conditions are true:

- The IP address of the sending MTA does not match any of the outbound connections configured in the policy.
- Cloud Email Security additional message authenticity checks fail.

Select the action to perform when spoofed messages are detected:

- **Quarantine the message.** This is the default option. Spoofed messages are kept in quarantine for up to 30 days.
- **Discard the message.** Spoofed messages are discarded. Note that no notifications are sent for this disposition
- **Tag the message subject.** The subject headers of detected spoofed messages are tagged with “SPOOFED:” or a custom tag that you enter.

Resolved and known issues

Resolved issues

Cloud Web Security

- If a file size block was configured on the File Blocking tab, this behavior was not reflected in the policy filtering test –instead of showing Blocked where appropriate, the result displayed Allowed.
- The policy filtering test was not returning the correct results when quota time for a category was exceeded.
- The policy filtering test was not returning the correct results when a category exception applied only to a roaming user.
- When authentication bypass was configured for a specific user agent, the policy filtering test did not return results for that user agent consistent with the configuration – for example, for a category requiring authentication, the result showed as Authenticated.
- Category exceptions that applied only to roaming users did not work for end users browsing via Web Endpoint.
- File type detection has been updated to recognize a WISE installer as an executable rather than an archive.

Cloud Email Security

- The Message Center was showing messages as clean or accepted, but logs showed them as discarded. This was due to a spam override setting affecting logging details, and has been fixed.
- Adding a comma-separated list of email addresses to the per-user configuration section of the Antivirus tab did not warn when the character limit was reached.

Known issues

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

Cloud Web Security

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**.

  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.
- When changing an appliance password, the confirmation popup window appears briefly and then disappears before you can click **OK**.

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