2014 Release 4 Notes for Websense® Cloud Security

Updated: 14-July-2014

Applies To:	Websense Cloud Security Solutions, 2014 Release 4

Use the Release Notes to learn about:

What's new in Websense Cloud Security Release 4?

Cloud Web Security features

Endpoint auto-updates by operating system

You can now configure automatic updates for endpoint installations separately for Windows and Mac operating systems. This is done on the **Endpoint** tab in a policy.

Uploading policy assignments

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

You can now automatically assign end users to policies by uploading a file of policy and user information to the cloud service.

The file must be in comma-separated value (CSV) format, and every line must contain 2 fields separated by commas:

- An email address belonging to an existing user in your account
- A policy name in your account.

For example:

```
address1@domain1.com, Default
address2@domain1.com, Sales Policy
```

If a field contains a comma, it must be quoted. Note that you do not have to include all of your existing users in the file, only those whose policy assignment you wish to change.

To upload the file:

1. Go to **Web Security** > **Policy Management** > **Policies**.
2. Under Policy Assignment, browse to the file that you wish to use.
3. Click **Upload**.

The email addresses in the file are checked against the existing users in the account, and a confirmation message is displayed once the file has uploaded successfully. If there are errors in the file – for example, incorrect formatting, a non-existent policy

name, or an invalid, unknown, or duplicate email address – the upload is canceled and an error message is displayed to explain the problem.

You can also download a CSV file containing the current list of end users assigned to policies by clicking **Download existing policy assignments**.

Session-based authentication

> **Note**
> This applies to version 1.3 of the i-Series appliance, available from September 2014. For more information about this version, see the i-Series Appliance Release Notes.

When adding or editing details for an i-Series appliance, the Authentication tab now includes a section for **Session-Based Authentication**.

If you have users on a thin-client environment, the mapping of end user to source IP address is no longer 1-to-1. To overcome this issue and authenticate end users correctly, session-based authentication takes place at configurable intervals by using cookies injected into the web traffic that force the web client to authenticate.

Once a cookie is injected, it is analyzed by the appliance and serves as a replacement for the user-to-source IP address mapping to associate a specific transaction to a specific user.

Click **Add** under Session-Based Authentication to define network addresses and IP address ranges that should use session-based authentication. The defined addresses are then authenticated based on a cookie sent to the browser on the local machine. This authentication is valid for the length of time defined in the **Session timeout** drop-down list on the same tab.

> **Note**
> When session-based authentication is enabled, the **Allow end users to bypass all certificate errors** option on the portal Bypass Settings page is not currently supported.

Authentication bypass for internal networks

> **Note**
> This applies to version 1.3 of the i-Series appliance, available from September 2014. For more information about this version, see the i-Series Appliance Release Notes.

If you have an i-Series appliance, you can override policy authentication settings based on the IP addresses in your internal networks, so that specific nodes in a network (for example, guest networks) are forced to authenticate using an alternative method, or will not be authenticated at all.

If there is a conflict between the settings in this section and authentication bypass settings for user agents or websites, the IP address settings for the internal network take precedence.

To add a setting for an internal network:

1. Navigate to **Web Security > Bypass Settings**.
2. Click **Add** under the internal networks table in the **Authentication Bypass** section.
3. Enter a **Name** for the rule. This name appears in the internal networks list on the Bypass Settings page, and you can click on it at a later date to edit your settings.
4. Select the authentication method for the rule. Note that you can only select a fallback option for the authentication type configured in the policy – for example, if the policy specifies NTLM authentication, you can select Basic or No authentication, but not Form login.
   - **Use defaults:** Uses your default authentication method.
   - **NTLM:** Uses NTLM identification for the specified internal network(s). If an application is not NTLM-capable, basic authentication will be used instead.

     

     Note
     You must have NTLM identification enabled for your account to use this option.

   - **Form login:** Displays the secure login form to users before they use their cloud service credentials to proceed over a secure connection.
   - **Basic:** Uses the basic authentication mechanism supported by many web browsers. No welcome page is displayed.
   - **No authentication:** Bypasses all authentication and identification methods in the cloud service. Select this option for internal networks that should never use authentication credentials.
5. Content analysis is enabled by default. Optionally, you can bypass all filtering for the specified internal network(s) by selecting **Disabled**.

   

   Important
   We strongly recommend you do not disable content analysis, as this could allow viruses and other malware into your network.

6. To specify the internal network details, click **Add**.
   a. Enter a name for the network (for example, “Guest Network”).

b. Select the network type. This can be an individual IP address, an IP address range, or a subnet.

c. Enter the IP address, range, or subnet details.

d. Click **OK** when you are done.

7. Click **Save**.

Authentication decryption bypass for appliances

Authentication decryption bypass is now supported for traffic going through i-Series appliances that is subject to any type of authentication.

ACE integration update

This release integrates the latest version of the Advanced Classification Engine (ACE) for the most up-to-date real-time security analysis and content classification.

Cloud Email Security features

Releasing a distribution list message

When releasing a message from the end-user message report, and that message was originally sent to a distribution list address, you are given the option to release the message to the whole list or a specific email address.

New supported file types

The following new file types are supported for attachment blocking and parking:

File format	File type
Compressed and Encoded Formats	Microsoft Outlook for Macintosh (OLM)
	Web ARChive (WARC)
Executables	Java Class format (CLASS)
Videos	MPEG-PS container with CDXA stream (MPG)
Other Formats	MATLAB file format (MAT, FIG)
	SEG-Y Seismic Data format (SGY, SEGY)
	Microsoft Windows NT Event Log (EVT)
	Microsoft Windows Vista Event Log (EVTX)

Virus report time range extended

The Top Sources of Viruses report now has a maximum time range of 30 days.

Resolved and known issues

Resolved issues

Cloud Web Security

- Basic authentication could not be enforced when single sign-on was in use.
- There was an inconsistency in authentication, where the endpoint used the hostname from the URL but the proxy used the host header. In rare cases where these were not the same, further authentication was requested. This has been fixed.
- When an authentication bypass rule was set up for a specific user agent and URL with content bypass enabled, the Filtering Test on the **Policies** page did not display the correct result for that user agent and URL.
- All sites that require an intermediate certificate to operate correctly with SSL decryption are now supported.
- When changing an appliance password, the confirmation popup window now stays on screen until you click **OK**.

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**. 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.