2015 Release 4 Notes for Websense Cloud Web Protection Solutions

Websense Cloud Web Protection Solutions | 6-August-2015

2015 Release 4 of our web protection products offers new features and includes a number of product corrections:

What's new in 2015 Release 4?

Password policy for end users

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

If available in your account, you can also use the password policy on the **Account** > **Contacts** > **Edit** page for your end users. Select **Apply password policy to end users authenticating with the service** to impose the same password requirements for any end users who are registered for the service and using manual authentication, including the minimum and maximum length and restrictions on using previous passwords. If you have also defined a password expiration limit, you can select

Remind end users when passwords are about to expire to send an email reminder to end users when they need to change their passwords.

As part of this feature, you can now search for end users who are overdue to change their passwords on the **Account** > **End Users** page.

Microsoft AD FS supported for single sign-on

Microsoft Active Directory Federation Services (AD FS) is now a supported option on the **Web** > **Single Sign On** page.

> ✓ **Note**
> Single sign-on is a limited-availability feature that may not be available in your account.

Updates to Endpoint Auditing Report

> ✓ **Note**
> The Endpoint Auditing Report is a limited-availability feature, and may not be available in your account.

The following options are now available from the **Endpoint status** drop-down:

- **Enabled** – all endpoints that are currently enabled
- **Enabled (manually)** – endpoints that have been manually enabled by the end user
- **Enabled (auto-override)** – enabled endpoints that have an automatic temporary override due to lack of connection with the cloud service
- **Enabled (system restart)** – endpoints that have been automatically re-enabled on machine restart
- **Disabled (manually)** – endpoints that have been manually disabled by the end user
- **Standby mode** – disabled endpoints that have an automatic temporary override due to lack of connection with the cloud service

You can now see further details for a particular workstation by clicking the workstation name. The Workstation Details pages show the following additional information:

- When the endpoint status was last updated
- The endpoint version
- The operating system on which the endpoint is installed
- The endpoint status change history for that workstation

Note also the following:

- The columns in the endpoint status table are now in the order Workstation, User Name, Endpoint Status.
- In the Log activity table, Enabled (system restart) events show the User as “System”. The “System” user is also displayed when there is no user associated with an event.

New block page for non-certificate errors

A new block page has been added for cases when the cloud service proxy cannot access a requested URL and the error is not related to certificate issues.

SSL decryption updates

The following updates have been made to SSL decryption in this release:

- The RC4 cipher has been removed from the list of ciphers used in SSL decryption.
- When an SSL tunnel is decrypted for authentication but not for analysis, a log record is created which is the same as the CONNECT transaction for non-decrypted tunnels.

i-Series appliance updates

The following updates have been made in the cloud service as part of the i-Series appliance v1.5 release. For more information, see the Release Notes for Websense i-Series Appliances.

Use of Active Directory for authentication

You can now connect an appliance to a local Active Directory server to enable transparent NTLM password authentication. This function offers enhanced authentication over the simple identification method available in previous versions.

If you are connecting your appliance to a local Active Directory for NTLM authentication, you do not need to enter the domain that forms part of your users’ NTLM identity on the **Authentication** tab when configuring an appliance in the portal.

Endpoint interoperability

In previous versions, all traffic from TRITON AP-ENDPOINT Web was redirected immediately to the cloud service, bypassing appliance processing. In this version, if some of your end users have the endpoint installed, perhaps because they often work remotely, you can set up your appliance to handle endpoint traffic in one of the following ways when those end users are at a site served by an appliance:

- Ignore all traffic generated by an endpoint client. This means that endpoint users are effectively treated as roaming users even when on-site.
- Manipulate PAC file requests from endpoint clients and ensure that endpoint traffic goes direct through the appliance rather than via the cloud service proxy. This means that end users have less latency and get a better user experience.

Both of these configurations must be enabled by Websense Technical Support; please contact Support for further information.

Integration of Cyren antivirus engine

An updated version of the Cyren antivirus engine has been integrated into cloud service categorization and deployed as part of this release.

Stricter password checking

When creating or updating portal passwords, note that passwords can no longer contain common words or keyboard sequences.

Resolved and known issues

Resolved issues

Policies

- Full traffic logging was not logging data for users in policies after the first policy.

Reporting and Dashboard

- After adding more columns to a report, the column order in the exported report was not the same as in the user interface.

Authentication

- Requests to HTTPS sites from roaming single sign-on users are now logged and reported accurately.

Data Security

- Compressed uploads were causing a DLP exception.

i-Series appliance

- Appliance end-of-life email messages were being generated multiple times and with incorrect information.

Categorization

- A POST form was being mis-categorized as an executable.

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

- The proxy does not recognize NTLM IDs sent from Microsoft AD FS as an attribute. This can result in the proxy creating auto-provisioned users with incorrect NTLM IDs.
- If an end user is browsing with Internet Explorer and their system clock is set to a future time or date, session-based authentication fails and is repeatedly requested because IE considers the session cookie to be expired. To avoid this, ensure the system clock is set correctly.
- 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

- Google redirect 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.

- 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.