2015 Release 6 Notes for Websense Cloud Web Protection Solutions

Websense Cloud Web Protection Solutions | 10-Nov-2015

2015 Release 6 of our web protection products offers new features and includes a number of product corrections:

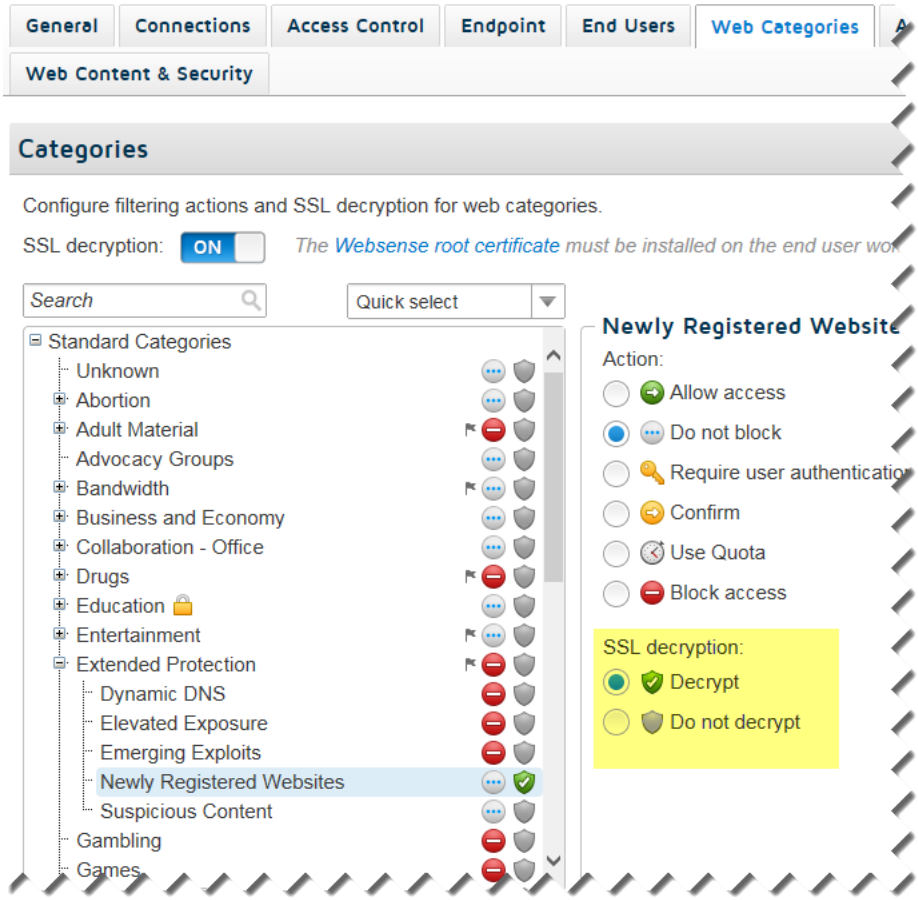
What’s new in 2015 Release 6?

Websense Cloud Web Protection Solutions | 10-Nov-2015

Manage SSL decryption on the Web Categories tab

SSL decryption is now enabled and configured on the **Web > Policies > Web Categories** tab in the Cloud TRITON Manager.

For TRITON AP-WEB customers, this includes the ability to specify whether or not to decrypt traffic via the same interface used to apply filtering actions to categories.



Configure filtering actions and SSL decryption for web categories.

SSL decryption: ON

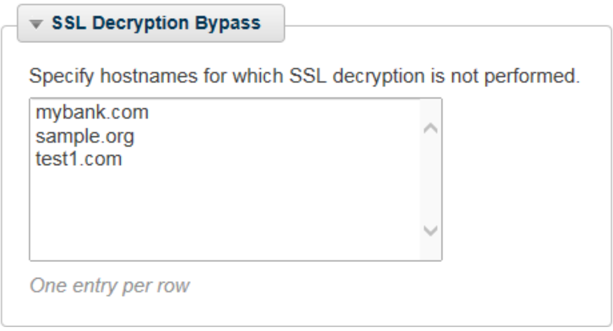
The Websense root certificate must be installed on the end user wo

Newly Registered Website

Action: ● Do not block

SSL decryption: ● Decrypt

SSL decryption bypass settings are also configured on the Web Categories tab, in a simplified interface that makes it easy to add, edit, and remove sites from the list.

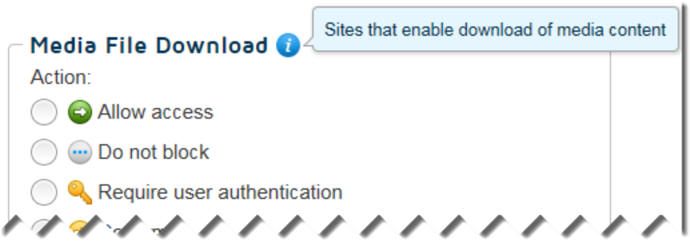


Specify hostnames for which SSL decryption is not performed.

mybank.com
sample.org
test1.com

One entry per row

In order to make room for the new options, the Category Info box is no longer displayed under the Action list. To see a description for the selected category, mouse over the "i" icon next to the category name at the top of the list of actions.



Media File Download
Sites that enable download of media content
Action:
○ Allow access
○ Do not block
○ Require user authentication

Reporting enhancements

- When you are creating custom reports with the Report Builder, the advanced attribute options now include the **Filtering Source**.

  Use this attribute to report on the method used to direct client traffic for filtering:

  - Cloud connection
  - Endpoint Web (Proxy)
  - Endpoint Web (Direct)
  - IPSec VPN
  - Appliance (Cloud traffic)
  - Appliance (Local traffic)
  - Secured mobile traffic
  - Aerohive integration
- When exporting a report to a file, a progress indicator provides visual feedback that the export process is underway. A Cancel button, adjacent to the progress indicator, allows you to terminate the export process prior to its completion.

Changes to mobile integration page

When integrating TRITON AP-MOBILE with AirWatch Mobile Device Management (MDM), in the Cloud TRITON Manager, now go to **Account** > **Mobile Integration > MDM Connection Setup** to connect the cloud service with AirWatch MDM (Step 5 in the Getting Started Guide).

Administration enhancements

- An alert is now issued when a license is added or changed and must be accepted to place the provisions of the license into service. The alert is accessed on the banner of the Cloud TRITON Manager. If the Alert window is not already open, click on the message icon and then click View Pending Licenses.
- When one or more alerts are created since the last administrator logon, the next time the administrator logs on the Alert window is automatically opened to give the alert high visibility. The alert list is sorted by severity with the highest severity alerts at the top.

Resolved and known issues

Websense Cloud Web Protection Solutions | 10-Nov-2015

Resolved issues

Policies

- When an exception was applied to a group, and then the group was deleted, an internal error occurred.
- Attachments to Gmail messages are now analyzed. Incidents can now be created for attachments that contain data that violates data security policies.

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

- 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 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.