2015 Release 5 Notes for Websense Cloud Web Protection Solutions

Websense Cloud Web Protection Solutions | 12-Oct-2015

2015 Release 5 of our web protection products offers new features and includes a number of product corrections:

What's new in 2015 Release 5?

Websense Cloud Web Protection Solutions | 12-Nov-2015

Data Security (DLP)

Data security features provide visibility into the loss of sensitive data via the Web. When SSL decryption is enabled, this includes data transfered via both HTTP and HTTPS transactions. Monitor the types of data loss most useful to your organization, and use data security reporting to help you assess your risk exposure.

> **Important**
> Data security features are not compatible with the i500 appliance.

When data security features are enabled, you can monitor:

- Data that is protected by national legislation or industry regulations, specifically:
  - Personally Identifiable Information (PII)
  - Protected Health Information (PHI)
  - Payment Card Industry (PCI DSS)
- Information related to data theft by malware or malicious activities
- Loss of intellectual property via custom classifiers that you define

To enable data loss detection:

1. Navigate to the **Web > Policies** page and open an existing policy.
2. Select the **Data Security** tab.
3. Mark **Enable data security (monitor only)**.
4. Under **Regulation** and **Data Theft**, select the types of information to monitor.
5. Under **Custom**, enable any custom classifiers appropriate for this policy.

   Custom classifiers use custom phrases, dictionaries, or regular expressions containing business-specific terms or data to classify your data. They are defined on the **Web > Policy Management > Content Classifiers** page.
6. (*Optional*) Under **Trusted Domains**, first mark **Enable trusted domains**, then identify any domains to which data may be sent without data security analysis. No incidents will be created for sensitive data sent to these domains.

Additional steps are required to enable reporting on data loss incidents:

- The **Account > Settings > Privacy Protection** page now includes a Data Security Incident Settings section. Select **Store and display incident data** to capture the values that triggered data security incidents, store them in the incident database, and include them in reports.

- You can control which administrators can view data security reports (and potentially sensitive information) and the data security dashboard. This setting is assigned at the account level, under **Account > Settings > Contacts**.

For administrators with the appropriate permissions, there are a number of reporting features that can be used to monitor data loss and data theft activity.

- In the Report Catalog, select **Standard Reports > Data Security** to build reports about data loss and regulatory compliance over the web channel.
- For a high-level view of activity in your organization, click **Dashboard**, and then click the **Data Security** tab. Charts include:
  - **Incident Count Timeline** shows a daily incident count for the designated period. With it, you can quickly identify trends and make policy changes as required.
  - **Total Incidents by Content Type** shows the number of regulatory incidents, data theft incidents, and custom classifier incidents in the designated period.
  - **Top Sources** shows the users, machines, or IP addresses most frequently instigating data security violations as well as the severity of their incidents.
  - **Top Destination Domains** shows the Internet domains most frequently targeted with sensitive data.
  - **Top Web Categories** shows the website categories most frequently targeted with sensitive data. These can be custom categories or the categories classified by the Websense URL category database.

For more information about using data security features, see the Getting Started Guide and the Help.

Office 365 bypass

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

To ensure that Microsoft Office 365 applications function properly, the cloud service now offers the option to bypass authentication or bypass the proxy entirely for Office 365. Enable the feature on the **Web > Bypass Settings** page. Select the **Authentication Bypass** or **Proxy Bypass** tab, then mark the **Office 365** box.

Reporting updates

The following updates have been made to Web reporting in this release:

- The Connection Name attribute has been added to the Report Builder and Transaction Viewer, enabling you to report on traffic based on entire connections rather than only IP addresses.
- A new standard report, Top Connection Names, has been added to the Web Activity folder in the Report Catalog. This report provides the top 20 connections with the most web activity in the last 7 days.

Administrator password expiration limit warning

A warning that a password expiration limit of 90 days or fewer is recommended now appears in the following cases:

- When you go to **Account** > **Contacts**, and click **Edit** under Account Management
- When you edit a contact's login details, and select a value greater than 90 days from the **Expire password** drop-down list.

This recommendation is for both security best practice and PCI compliance purposes.

Links to data security and privacy information

A new Privacy & Security option has been added to the Help menu in the Cloud TRITON Manager. The documents accessible from this menu item include:

- a Data Privacy FAQ
- the Websense Privacy Policy
- an Information Security statement for Websense cloud services
- information about ISO27001 certification

TRITON AP-ENDPOINT Web installation page updates

The installation pages that appear to end users when installing TRITON AP-ENDPOINT Web directly from the cloud service have been updated to be consistent in style with other Websense notification pages.

New block page for endpoint end users

A new block page is displayed to end users when the request is known to come from a system with TRITON AP-ENDPOINT Web installed, but the user cannot be determined and authenticated.

This page cannot be edited by administrators.

Resolved and known issues

Websense Cloud Web Protection Solutions | 12-Oct-2015

Resolved issues

Authentication

- Unrecognized authentication methods are no longer logged by the proxy for inclusion in reports.
- The proxy now recognizes NTLM IDs sent from Microsoft AD FS as an attribute.

Reporting and Dashboards

- Filtering by the Policy attribute now works correctly for all operators, not just “is” and “is not”.
- Transaction Viewer now displays the correct timestamps for all time zones, including custom time zones.
- There were discrepancies between group information shown in reports and the equivalent shown in a downloaded CSV file. This has been fixed.
- Blocked HTTPS transactions were being reported twice, with an incorrect action.
- It is now possible to create a new chart in a custom dashboard using Chrome 43 without the menu collapsing.

Policies

- The validation of non-proxied destinations settings is now consistent at policy level (on the **Connections** tab) and account level (under **Web** > **Bypass Settings**).

i-Series appliance

- An error no longer appears when returning to the Protocols tab in a policy after creating a protocol exception.

Known issues

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

Data Security

- Attachments to Gmail messages are not analyzed. As a result, incidents cannot be created for attachments that contain data that violates data security policies.

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 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.