2015 Release 1 Notes for Websense Cloud Web Protection Solutions

TRITON AP-WEB with Web Cloud Module |2-Feb-2015

To address the wide-scale adoption of cloud and mobile technologies, along with a rapid growth in distributed workforces, Websense, Inc., is excited to launch a new, industry-leading security suite – Websense® TRITON® APX 8.0. This new modular platform provides **advanced threat and data theft protection** for organizations that wish to embrace new technologies and working practices. TRITON APX provides protection across the entire kill-chain, reveals actionable intelligence, and enables real-time feedback to educate and motivate end users to avoid risky behavior. This product release is the culmination of eighteen months of business transformation and innovation. As a result, Websense customers are now able to maximize the unparalleled protection and ROI of Websense TRITON APX solutions well into the future.

The 2015 Release 1 product release adopts a new product naming and grouping of the familiar Websense TRITON product line.

Original Name	New Name
Websense Cloud Web Security Gateway	Websense TRITON AP-WEB with Web Cloud Module

Previous product functionality remains intact. The user interface has the same look and feel, and the core product continues to provide the strong protections you've come to rely on.

In addition to new names, our web protection solutions offer new features and includes product corrections. Refer to the information provided in these Release Notes for additional product information:

© 2015 Websense, Inc.

What's new in 2015 Release 1?

Endpoint end user control

> **Note**
> Endpoint end user control is a limited-availability feature, and may not be available in your account.

On the **Web > Endpoint** page, the End User Control feature offers the ability for end users to enable or disable the Web Endpoint on their machines. You may wish to do this if your users are working in a location that blocks web traffic to the cloud service. Note however that this option can introduce vulnerabilities: if enabled, it permits end users to circumvent the protections offered by the endpoint software.

To configure end user control:

1. Use the slider to enable or disable the feature.
2. For **Apply to**, select **Specified users or selections** to allow those you specify to enable or disable the endpoint on their machines. Select **Everyone except specified users or selections** to prevent those you specify from enabling or disabling the endpoint on their machines.
3. To add users to the end user control list, on the Users tab enter each user email address on a separate line in the **Users** field.
4. To select groups, policies, or connections to add to the end user control list, on the appropriate tab, click the item you want in the **Available** field, then click > to move it to the **Selected** field. Use the **Ctrl** key to select multiple items.
5. Click **Save** when done.

New appliance version

A new version of the i-Series appliance is available for this release. For more information, see the Appliance Release Notes.

Favorites in Report Catalog

The Report Catalog now includes a Favorites folder, enabling you to easily locate your most frequently-used reports. You can mark a report or report folder as a favorite in the following ways:

- Click the star to the left of the report or folder name in the Report Catalog. The star turns yellow when selected.
- Click the star to the right of the report name in the Report Builder or Transaction View. You do not need to save your changes.

To remove a report from Favorites, click the star again to turn it gray.

When viewing the Favorites folder, note that you are essentially viewing a list of shortcuts to the reports. Choose **View in folder** from a favorite report's drop-down menu to see the report in its original folder.

Security Labs News added to Threat Dashboard

The Websense Security Labs™ RSS news feed is now available on the Threat Dashboard.

Cloud Data Security updates

Important

Cloud Data Security is currently available to early adopters only. For additional information about this feature, please fill out the online registration form.

The following changes have been made for Cloud Data Security in this release:

- Drill-down to Transaction View has been added to the Data Security dashboards.
- Tooltips have been added to show a header name and content when a report column width is truncated.
- Tooltips have been added to matches in the Incident Report, detailing the transaction part where the match was found, the file name where the breach was found in an attachment, and the phrase weight (positive or negative) for dictionary breaches.

Tooltips added in Transaction View

Tooltips have been added to all columns in Transaction View reports, enabling you to hover over column headings to see the full metric name and, if applicable, measurement used.

Free text entry for autocomplete filters

Report filters that use autocompleted text (such as Category, Destination IP Country, Group, Parent Category, Policy, Source IP Country, User) now have a **Use free text entry** check box on the Filter popup window. Selecting this allows you to copy and paste multiple values into the text box rather then entering each one individually.

Any autocompleted values already added are converted to free text when the check box is selected, and if the check box is cleared, any free text values are converted to autocompleted values.

“Contains” options added to autocomplete filters

The following report filters that use autocompleted text now include “contains” and “does not contain” in the drop-down list:

- All autocomplete attributes in Web reports
- The User attribute in Authentication reports
- The Policy, Protocol, and User attributes in Protocol reports

This makes it easier to search for matches that contain the text that you specify.

Policy details in authentication reports

The Policy ID is now supported as part of the Authentication attribute reports, enabling you to report on authentication events and the policy they originated from.

Time zone settings updated

The time zone settings for quota and confirm actions have been updated to reflect changes in Russian Federation time zones.

Report limit extended in scheduled jobs

The maximum number of reports in a scheduled job has been raised from 5 to 6.

User Agent attributes added to Web reports

The following attributes have been added to Web reports, under the User Agent heading:

Name	Description	Filter Values
Browser	The specific browser used, including type and version (for example, Internet Explorer 11). When filtering, if the browser you wish to report on is not shown in the filter check boxes, you can enter it manually.	Check boxes/manual text
Browser Type	The type of browser used across all versions (for example Internet Explorer). When filtering, if the browser type you wish to report on is not shown in the filter check boxes, you can enter it manually.	Check boxes/manual text
Operating System	The specific operating system used, including type and version (for example, Windows 7). When filtering, if the operating system you wish to report on is not shown in the filter check boxes, you can enter it manually.	Check boxes/manual text
Operating System Type	The general type of operating system used across all versions (for example, Windows or Linux). When filtering, if the operating system type you wish to report on is not shown in the filter check boxes, you can enter it manually.	Check boxes/manual text

Name	Description	Filter Values
User Agent	The specific user agent used to access sites. This is a string sent from your browser or Internet application to the server hosting the site that you are visiting. The string indicates which browser or application you are using, its version number, and details about your system, such as the operating system and version. The destination server then uses this information to provide content suitable for your specific browser or application. For example, this is a user agent for Firefox: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.6) In this example, Windows NT 5.1 indicates that the operating system is Windows XP, and the language it uses is US English..	Autocompleted text
User Agent Type	The type of user agent used to access sites. Options are Browser, Email Client, Feed Reader, Library, Mobile Browser, Multimedia Player, Offline Browser, Robot, Validator, or Unknown.	Check boxes

Resolved issues

Resolved issues

Reporting and Dashboard

- In reporting and on the dashboard, the menu option for “Last 1 day” has been amended to “Last 24 hours”.
- The Bandwidth dashboard is now correctly sorted.
- The tooltips for report descriptions and buttons were truncated in Safari version 7.0.3.
- When setting a report or dashboard filter, if you select an option in the drop-down list (for example, “is not”) but then click OK without selecting any further options, no filters are applied and the popup window reverts to the defaults next time it is opened.
- The Update Report button behavior is now consistent, turning yellow only when there are changes to the report that can be generated.
- Policy names in Hebrew were not available in report filters.

- In Transaction View, the Sorted column is now clearly visible.
- Scheduled reports were not sending out the last report occurrence.
- The following attributes are now available in Transaction View only (under Metrics > Advanced): Client Write Time, Filtering Time, Request Filter Time, Response Filter Time, Server Response Time, Total Time.
- When searching in the Report Catalog, the folder name is now displayed in search results for standard reports, and right-clicking a result and selecting **View in Folder** takes you to the report's folder.
- The Scheduler page now displays the full list of scheduled jobs.
- There was a mismatch between the top-level event count on the Threat dashboard and the events listed in the Security Event Summary.

Cloud Data Security

- On the Data Security dashboard, unknown user events are now included.
- The Top Sources dashboard now shows incidents with Medium Severity.
- PCI rules now return both masked and unmasked content.
- After editing a content classifier's threshold value, the value is now initially shown in the table with correct spacing
- The Content Classifiers > Add Regular Expression page is now aligned correctly in Internet Explorer 8.
- In reports, the Content Subcategory attribute now displays the custom classifier type (Dictionary, Key Phrase, or RegEx) rather than the name of the specific rule.
- On the Data Security tab in a policy, the geographical regions list in the Regulations section now shows regions that do not have sub-regions (for example, USA and Canada).

Endpoint

- The headings in the CSV export of the Endpoint Auditing Report now match the headings in the report.
- Users deleted from a policy no longer appear under End User Control on the **Web >Endpoint** page.

Logging and Auditing

- The category reporting and dispositions for full traffic logging have been updated: "Cannot connect" and "User disabled" events are now logged.
- The Audit Trail now includes entries for actions performed with content classifiers.

i-Series appliance

- An issue where SSL decryption was enabled and an element on the Facebook logon page was not displayed correctly has been fixed on the appliance and in the cloud service.

General

- Portal tables were missing dividing lines in Internet Explorer 8.
- The unique pass phrase answer can now be changed on the **My Account** page.

2015 Release 2 Notes for Websense Cloud Web Protection Solutions

Websense Cloud Web Protection Solutions |10-March-2015

2015 Release 2 of our web protection products offers new features and includes a number of product corrections:

What's new in 2015 Release 2?

Custom dashboards

In addition to the standard dashboards, you can now create custom dashboards enabling you to easily access the data you most frequently need. Each custom dashboard can contain up to 6 charts.

You can have a total of 10 visible dashboards per portal account. If you wish to hide one or more of the standard dashboards to allow additional custom dashboards, you can click the Settings icon in the top right corner and select **Hide Current Dashboard**. Click **Continue** to confirm. You can restore hidden dashboards at a later time by using the **Settings** > **Unhide Dashboard** option.

To create a custom dashboard:

1. From any dashboard, click the Settings icon () in the top right corner.
2. Select **Add Dashboard**.
3. Give your dashboard a name, and click **Add**.

Your new dashboard appears as a blank tab. You can rename or delete the dashboard from the Settings menu.

To add charts to a custom dashboard, click the Settings icon and select **Add Chart**. Then choose whether you want to create a new chart, or a chart from an existing report.

Once you have added charts to your dashboard, you can reorder them by dragging them around the screen. You can also change the date range for all charts from the drop-down at the top of the dashboard – by default the range is 24 hours.

To edit or delete a chart, click the arrow in the top right of any chart and select the option you want.

Dashboard updates

The following dashboard enhancements are in this release:

- You can now drill down to Transaction View from both standard and custom dashboards. Click a data point in any chart and select **View Transactions** from the context menu. Transaction View opens with the appropriate filters applied, including any filters active on the dashboard as a whole and within the selected chart. The date range for the query is the same as the range selected on the dashboard.
- You can also drill down on a standard or custom dashboard chart by an additional attribute to investigate further details. Click a data point in any chart, select **Drill Down By** from the context menu, and select the attribute you want. This runs a query in Report Builder with the appropriate grouping and filters applied: the report is grouped by the selected attribute, and includes any filters active on the dashboard as a whole and within the selected chart. The date range for the query is the same as the range selected on the dashboard.

Export from Transaction View

When you select rows in Transaction View and choose to export to PDF, you now have the option to export either Table View or Detail View for the transactions you select. Note that the detail view export is limited to 20 transactions.

Privacy protection updates

On the **Settings > Privacy Protection** page, you can now define the attributes that should be anonymized in web reports. By default, User name, Connection IP, Source

IP, and Workstation are all selected; you can select and clear the options most appropriate for your organization, but at least one check box must be selected.

> **Note**
> If you have selected **Preserve end user information for security threats,** the attributes that you select are not anonymized for any web traffic considered to be a security risk.

Account-wide non-proxied destinations

The **Non-Proxied Destinations** tab on the **Web > Bypass Settings** page enables you to add, and import in bulk, destinations that bypass the proxy for all policies.

To add a new non-proxied destination:

1. Click **Add**.
2. Enter a **Name** and optionally a **Description** for the destination.
3. Select the destination **Type**: Address, Subnet, or Domain.
4. Do one of the following:
   a. For an address, enter the destination's IP address.
   b. For a subnet, enter the destination's subnet address and define whether it uses CIDR notation or subnet mask.
   c. For a domain, enter the destination's domain name.
5. Click **Submit**.

To import non-proxied destinations in bulk:

1. Click **Import Destinations**.
2. Click the CSV template link, and save the template in a location of your choice.
3. Add the non-proxied destination information to the CSV template file.

   The template file contains the following columns: Name, Type, Destination, and Description. Only Description is optional; all other columns must be filled in. Ensure the Type column contains either Address, Domain, or Subnet, and any destinations with the Subnet type use CIDR notation. For example:

   ```
   Name    Type     Destination      Description
   Dest1   Domain   destination1.com Here is a description
   Dest2   Address  154.10.2.36      Another description
   Dest3   Subnet   154.10.2.38/19   Yet another description
   ```

   Save the CSV file when done.
4. On the Import Destinations page, browse to your CSV file, then click **Import**.

Once the destinations are successfully imported, the Import Destinations page closes and the imported destinations are listed on the Non-Proxied Destinations tab. If the

import fails, any errors are listed on the Import Destinations page. Each error states which line of the CSV file is affected, and explains the problem; fix any issues before trying the import process again.

Changes to Bypass Settings page

The **Web > Bypass Settings** page has been divided into 3 tabs:

- The **Authentication Bypass** tab contains the custom settings for Internet applications and websites that cannot authenticate with the cloud service. If you have an i-Series appliance or an edge device, this tab also includes authentication bypass rules for internal networks behind the device.
- The **Non-Proxied Destinations** tab contains the new options to add, and import in bulk, destinations that bypass the proxy for all policies. See *Account-wide non-proxied destinations*.
- The **SSL** tab contains the bypass certificate verification and bypass authentication decryption settings.

The Endpoint Bypass options have been moved to the **Web > Endpoint** page (see *Changes to Endpoint page* below).

All existing settings have been maintained.

Changes to Endpoint page

The **Web > Endpoint** page has been divided into 3 tabs:

- The **General** tab contains the endpoint client download links, as well as the facility to set the anti-tampering password and select a default policy for roaming users.
- The **End User Control** tab contains the options for end users, groups, policies, or connections to enable or disable the endpoint on their machines.

Note
End User Control is a limited-availability feature and may not be available in your account.

- The **Endpoint Bypass** tab contains the bypass options moved from the W**eb > Bypass Settings** page.

All existing settings have been maintained.

Changes to Welcome page

The cloud service displays the Welcome page when it is unable to identify end users (for example, roaming users or those required to use manual authentication). The text and layout on this page have been updated for clarity.

Note that for endpoint users who reach this page in error, a link is provided to further instructions on workarounds, such as checking their endpoint status and enabling or disabling it as necessary, or restarting their browser.

Data Security updates

Important

Data Security for TRITON AP-WEB Cloud is a limited-availability feature and may not be available in your account. To request the feature is enabled in your account, please complete the online registration form.

The following changes have been made for Data Security in this release:

- The option to export Detail View to PDF also applies to Incident Manager.

Resolved issues

Resolved issues

Reporting and Dashboard

- If you started a second portal session while the first was still active, the first session took you to blank Report Catalog and Report Builder pages rather than expiring and returning you to the logon page.
- A scheduled report due to end on a specific date was not running the report on the last day.
- In Report Builder, running a report grouped by Hour and selecting one of the trend charts caused a “Failed to run report” error.
- Empty user values were displayed as “System” in the Web and Protocol schemas.

Data Security

- After adding phrases to a new dictionary classifier, the table headers and columns were misaligned.

- Clicking **OK** after adding a phrase to a dictionary opened a “Choose file to upload” window as if the **Import** button had been clicked.

Policies

- When adding an end user to a policy, if the entered email address already existed in the account, the email address field became non-editable after the error message appeared.
- On the Web Categories tab, if a category’s action was changed by repeatedly clicking on its icon (for example, from Quota to Block), the notification page was not updated.
- Monitor Only policies had certain categories blocked by default when they should be permitted.

Endpoint

- With User Access Control, giving access rights to one end user could affect the rights of other users in the same policy browsing on different machines.

2015 Release 3 Notes for Websense Cloud Web Protection Solutions

Websense Cloud Web Protection Solutions | 29-June-2015

2015 Release 3 of our web protection products offers new features and includes a number of product corrections:

What's new in 2015 Release 3?

Google redirect

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

If you wish to control the Google domain that your end users see, you can now choose to override Google's standard redirect behavior. By default, Google redirects browsers to the appropriate site for the country it detects (for example, google.fr for France). However, sometimes this is not accurate, for example if your end users are browsing through a cloud service proxy that is in a different country.

To use this feature, you should enable SSL decryption for the Search Engines and Portals category on the **SSL Decryption** tab, and install the Websense root certificate on end user machines.

To define Google redirect behavior for the policy, go to a policy's **General** tab, then:

1. Select **Override Google redirect behavior**.

   If you have not already enabled SSL decryption for the Search Engines and Portals category, a warning message appears at this point. You can enable SSL decryption directly from this dialog box.

2. Select one of the following options:
   - **Ensure requests for google.com are not redirected** – This option prevents Google from redirecting to a local country site when the end user enters "google.com".
   - **Redirect requests for google.com to** – This option ensures all google.com requests are redirected to a local country site of your choice. Enter the country code in the text field (for example, **fr** for google.fr, or **co.uk** for google.co.uk).
3. Click **Save** when you are done.

You can also configure Google redirect behavior for specific connections within your policy, when you add or edit a proxied connection on the **Connections** tab. If you configure Google redirect behavior for both the policy and a connection, the settings for the connection take precedence over the policy settings. If you do not configure Google settings specifically for the connection, it uses the behavior configured at policy level, if any.

Note

For i-Series appliance traffic, note the following:

- Google redirect does not apply to traffic coming from clients defined as session-based. This traffic is first directed to Google for termination before being redirected to the cloud service, and in such cases Google redirects to the local country site.
- This feature 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.

Privacy protection updates

If you are a TRITON AP-MOBILE user, the IMEI number can now be anonymized in web reports. To enable this option, go to the **Account > Privacy Protection** page, and select **Anonymize end user information**. Then select the IMEI number attribute for anonymization.

Note that if you also select **Preserve end user information for security threats,** any attributes that you select are not anonymized for web traffic considered to be a security risk.

Global authentication page for single sign-on users

A new authentication page has been added for roaming single sign-on end users who need to authenticate with the cloud service. This enables the service to identify the single sign-on identity provider of the roaming user's account, and then execute the single sign-on process.

The authentication page asks the end user to provide their email address. The page is not visible or editable in the cloud portal.

New error pages for connection issues

Additional error pages have been added for cases where the cloud service proxy cannot connect to an HTTPS site. These pages cover the following cases:

- SSL connection errors
- Network or system error (for example, the site is currently unavailable)
- DNS error

Reporting updates

The following updates have been made in web reporting:

- The Date range popup window now includes the option to select a custom time zone for a report. By default the time zone is automatically detected and reports are generated in the user's local time zone. Selecting a custom time zone means the report is always generated for that time zone, regardless of the user's location.
- Scheduled reports now include the option to password-protect the report. If you select this on the **Delivery Options** tab, you must enter and confirm a password that the report recipient must use to view the report contents. Ensure the password is distributed securely to all report recipients.
- When adding or editing a scheduled report job, manually entering one or more email addresses in the **Other recipients** field triggers a warning message on clicking **Next** or **Save**. This is to ensure the recipients are authorized to receive the reports.

OpenSSL version updated

The version of OpenSSL used in the cloud service has been upgraded to protect against newly-published vulnerabilities.

Resolved issues

Resolved issues

Reporting and Dashboard

- When Privacy Protection is enabled, the attributes you select to be anonymized in reports map to columns in the Transaction Viewer. The string used to replace data to be anonymized is now the same for each attribute (“Not available”).
- When Privacy Protection is enabled for data loss incidents, selecting the Source IP attribute under the Privacy Protection settings now anonymizes the corresponding values in the Incident Manager report.

Endpoint

- The **Web** > **Endpoint** page now displays correctly after setting the anti-tampering password.

Directory synchronization

- Directory synchronization was failing when a new group was synchronized with a duplicated DN, but different CN and GUID.

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 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.

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 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.

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:

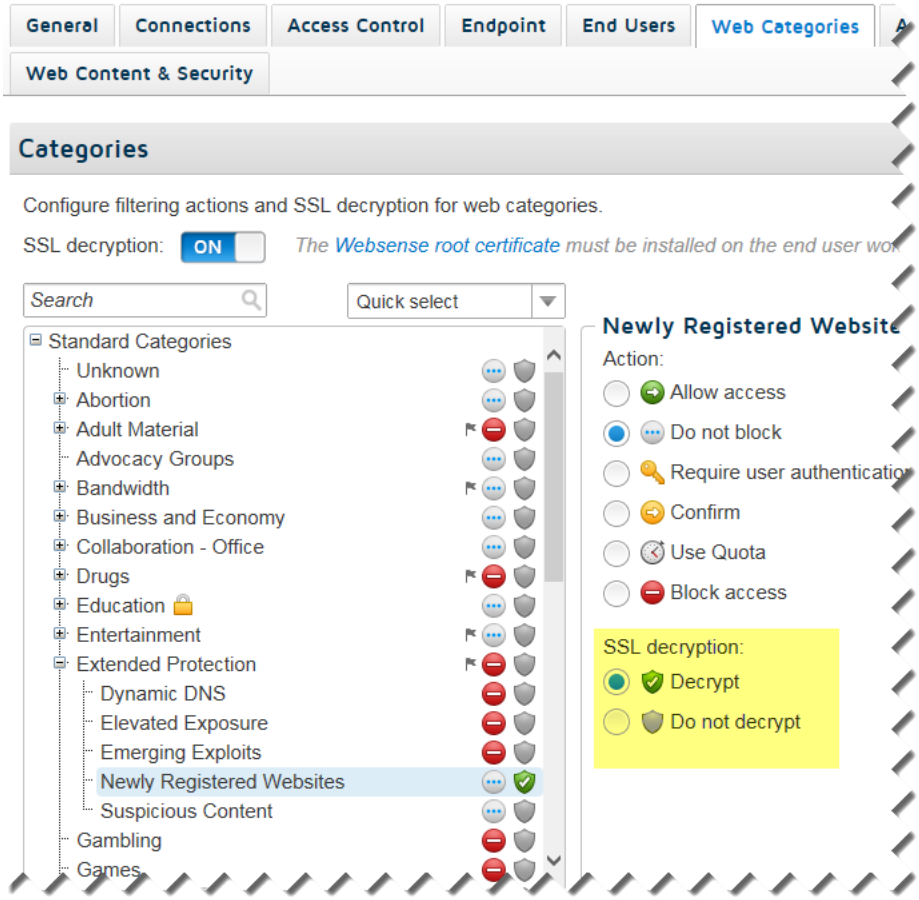
What's new in 2015 Release 6?

Websense Cloud Web Protection Solutions | 10-Nov-2015

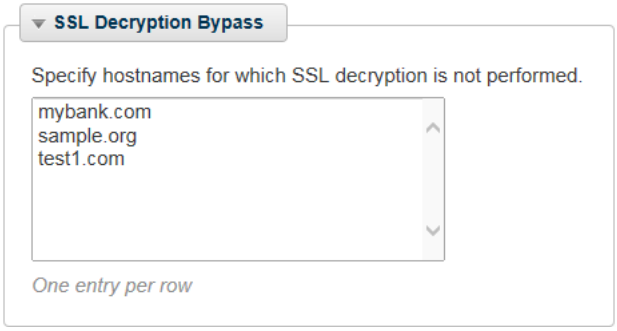
Manage SSL decryption on the Web Categories tab

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

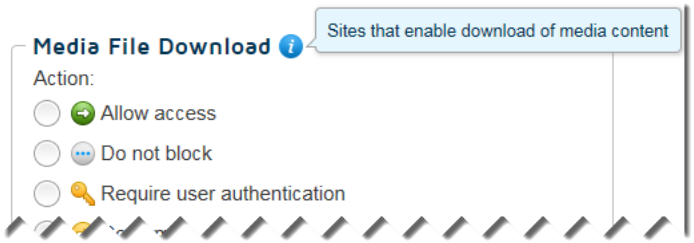
For TRITON AP-WEB customers, this includes the ability to specify whether or not to decrypt traffic via the same interface used to apply filtering actions to categories.



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.



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.



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.

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.

©1996–2015, Websense, Inc. All rights reserved.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.