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 and known 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.

Known issues

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

Reporting

- 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 different for different attributes, rather than the same string being used.
- When Privacy Protection is enabled for data loss incidents, selecting the Source IP attribute under the Privacy Protection settings does not anonymize the corresponding values in the Incident Manager report. To anonymize values in the Source IP column in the Incident Manager, you must select the Connection IP attribute on the Privacy Protection page.

Web 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

- 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.

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.