2014 Release 6 Notes for Websense® Cloud Data Security

Updated: 8-Dec-2014

Applies To:	Websense Cloud Security Solutions, 2014 Release 6 Early Adopters Program

The Data Security feature in Websense® Cloud Web Security Gateway provides visibility into the loss of sensitive data via the web channel, and enables you to assess your risk exposure to data loss in this manner. This includes intellectual property, data that is protected by national legislation or industry regulation, and data suspected to be stolen by malware or malicious activities.

Important

The system monitors and reports on potential data leaks. It does not block them.

Use the Release Notes to learn about Data Security's various features:

- *Content classifiers*
- *Policy settings*
- *Privacy protection*
- *Reporting permissions*
- *Privacy protection*
- *Dashboard*
- *Known issues*

For more information on these features, see the Getting Started Guide for Data Security in the cloud, supplied as part of this release.

Content classifiers

Use content classifiers to classify your data using custom phrases, dictionaries, or regular expressions containing business-specific terms or data. You then select the classifiers that you want to enable for a policy using the Data Security tab in the policy.

You can use more than one classifier in your policies. The following classifier types are available:

- **Regular expression** - used to describe a set of search criteria based on syntax rules. For example: (abc{21,40}){1,30})
- **Key phrase** - a keyword or phrase that indicates sensitive or proprietary data (such as product code names or patents).
- **Dictionary** - a container for words and expressions relating to your business.

Select **Web > Policy Management > Content Classifiers**.

Policy settings

To enable the data loss detection feature, you need to open a web security policy, such as the default policy, and configure settings on the **Data Security** tab.

On this tab, you can configure the following:

- **Regulations** - Most countries and certain industries have laws and regulations that protect customers, patients, or staff from the loss of personal information such as credit card numbers, social security numbers, and health information. You need to set up rules for the regulations that pertain to you
- **Data Theft** - detect when data is being leaked due to malware or malicious transactions. When you select these options, Cloud Web Security Gateway searches for and reports on outbound passwords, encrypted files, network data, and other types of information that could be indicative of a malicious act.
- **Custom** - Use this section if you want to detect intellectual property or sensitive data using custom phrases, dictionaries, or regular expressions containing business-specific terms or data.
- **Trusted Domains** - Select **Enable trusted domains** if you do not want certain domains to be monitored, then enter URLs for the trusted domains separated by commas. The system does not analyze trusted domains. This means users can send them any type of sensitive information via HTTP, HTTPS, or other web channels from your network.

Privacy protection

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.

By default, incident data is *not* captured, stored, or displayed. Administrators with permission to view incident data are able to see the number of matches in the report, but not the match values or context.

Reporting permissions

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.

To give administrators these permissions:

1. Navigate to **Account > Settings > Contacts**.
2. Click the user name of the contact to edit.
3. On the Login Details screen, click **Edit**.
4. Under Account Permissions, select **View All Reports** and **Data Security Reports**.
5. Click **Save**.

This enables users to view data security reports, which may or may not contain incident forensics and trigger data, depending on your privacy protection settings.

Note that this option does not affect permissions to manage data security configuration settings.

Reporting

In the Report Catalog, select **Data Security** to build reports about data loss and regulatory compliance over the web channel.

Report	Description
Content Type	
Compliance Summary	Find out which compliance rules are most often violated in your organization and view a breakdown of the incident count for each policy or rule.
Custom Classifier Summary	See which custom classifiers triggered the most incidents during the designated period.
Data Theft Summary	View a list of all data theft incidents that were detected during the designated period, along with incident details.
Incidents	
Incident List	View list or chart of all data loss incidents that were detected during the designated period, along with incident details such as the destination, severity, and transaction size.
Sources & Destinations	

Report	Description
Destination Summary	Learn the destination URLs or IP addresses involved with the most violations, broken down by severity.
Users Summary	See the users, machines, or IP addresses most frequently violating data security policies and the severity of their breaches.

Dashboard

For a high-level view of activity in your organization, click **Dashboard**, and then click the **Data Security** tab. Data Security 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.

Known issues

The following known issues in this release will be fixed in the next release:

- On the **Account > Privacy Protection** page, “DLP Incident Settings” should be “Data Security Incident Settings”.
- Dashboard charts displaying metrics that can only be whole numbers should have axis labels in whole numbers rather than decimal.
- The Top Sources dashboard currently shows only incidents with High Severity; Medium Severity incidents are missing.
- After editing a content classifier’s threshold value, the value is initially shown in the table with incorrect spacing,
- Data Security dashboards should display Incidents instead of Hits.
- In reports, the Content Subcategory attribute currently displays specific classifier rule names rather than the classifier type (Dictionary, Key Phrase, or RegEx).
- On the Add Regular Expression page, the phrase “Regular expression pattern” should be “RegEx pattern”.
- The Add Regular Expression page has mis-aligned fields in Internet Explorer 8.

- On the Data Security tab in a policy, the geographical regions list in the Regulations section does not currently show regions that do not have sub-regions (for example, USA and Canada).
- In Incident Manager, switching Detail View from Off to On produces an error message.

The following known issues in this release will be fixed in a later release, or are not currently scheduled to be fixed:

- The PII classifier with Wide sensitivity for the Canada region can return false positives.
- In password dissemination rules, the word “password” is masked when it should not be.
- The Names classifier with Wide sensitivity can create incidents on generic text.
- When all regions are selected for regulation and all rules have Wide sensitivity enabled, a password post on Facebook can result in false positives.
- Under Data Theft on the Data Security tab, the “Malware communication” option should be “Suspected malware communication”.
- On the Add Dictionary page, the table headers are misaligned with the table body.
- When adding an end user to a policy, if you submit an email address that already exists in the account, an error is displayed but the email address field is not editable. Return to the previous page in the browser to be able to edit the email address.