

2016 Release 4 Notes for Forcepoint Cloud Web Protection Solutions

Cloud Web Protection Solutions | 2016 Release 4 | 21-Sep-2016

2016 Release 4 of our web protection products offers new features and product corrections:

- *What's new in 2016 Release 4?*
 - *First logon wizard for new accounts, page 2*
 - *Define trusted categories for Data Security, page 2*
 - *Enhanced proxy bypass definitions, page 3*
- *Resolved and known issues*
 - *Resolved issues*
 - *Known issues*

What's new in 2016 Release 4?

Cloud Web Protection Solutions | 2016 Release 4 | 21-Sep-2016

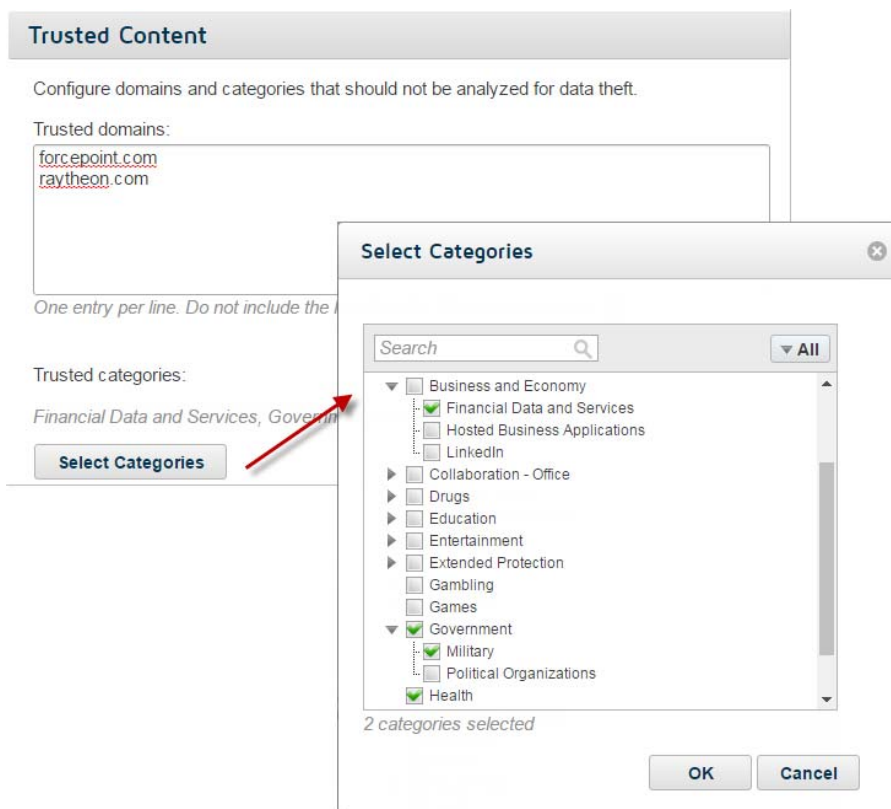
First logon wizard for new accounts

When administrators connect to the Cloud TRITON Manager for the first time to activate their account, a new wizard takes them through the initial steps of:

- Accepting the license agreement for each Forcepoint cloud product that they have purchased
- Selecting a primary and backup cloud data center for storing their reporting data
- Providing an administrator email address and password recovery question for use in recovering a lost administrator password

Define trusted categories for Data Security

Within each policy, the Data Security tab allows administrators to identify trusted content, which now includes both domains and **categories** for which data security analysis is not performed.



To select trusted categories, the administrator can either browse through a category tree or use search to find a category.

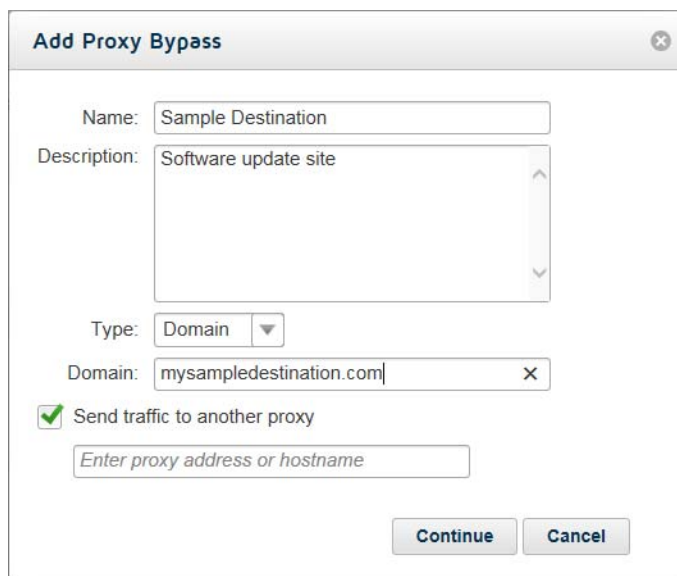
As with trusted domains, trusted category definitions are:

- Specific to a Web policy, applying only to content sent by users assigned that policy
- Enforced for all Data Security policies (both regulations and data theft, including all content classifiers) within the Web policy

Enhanced proxy bypass definitions

The **Connections** tab in web policies has been updated.

When defining a destination that bypasses the proxy administrators can define an alternate, third-party proxy to use for traffic to that destination. The alternate proxy **must not** be another Forcepoint proxy (like Content Gateway).



The screenshot shows a dialog box titled "Add Proxy Bypass" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Name:** A text input field containing "Sample Destination".
- Description:** A text area containing "Software update site".
- Type:** A dropdown menu currently set to "Domain".
- Domain:** A text input field containing "mysampledestination.com" with a clear button (X) on the right.
- Send traffic to another proxy:** A checkbox that is checked, with the label "Send traffic to another proxy".
- Proxy Address:** A text input field with the placeholder text "Enter proxy address or hostname".
- Buttons:** "Continue" and "Cancel" buttons at the bottom right.

In addition, the term “non-proxied destinations” has been replaced with **proxy bypass** on this screen for consistency with other areas of the cloud portal.

Resolved and known issues

Cloud Web Protection Solutions | 2016 Release 4 | 21-Sep-2016

Resolved issues

Data Security

- Data Security incidents are created as expected when users attempt to save sensitive data (that is, data that matches a Data Security rule) to Google Drive. This results from enhanced MIME parsing capabilities for Data Security.
- In Data Security reports, the Action attribute now has the values **Monitored** and **Blocked**, for improved clarity.

Reporting

- The Threat dashboard no longer includes transactions with a severity level of “None.”

Endpoint

- End users with Internet Explorer 11 are now prompted to deploy web endpoint software when administrators enabled automatic deployment of the endpoint client.

i-Series appliances

- A connectivity error message is no longer displayed in the cloud portal when an appliance is re-registered with the same software version.

Single sign-on

- Users are now properly redirected to the website they requested after they accept the compliance page in environments that use single sign-on.

Known issues

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

IPsec tunneling

- For SSL decryption to work with IPsec tunneling, SSLv3 must be disabled in Internet Explorer.
- Basic authentication does not work for iTunes with IPsec tunneling.
- Using authentication bypass settings to force NTLM, basic authentication, or the welcome page does not work with IPsec tunneling if a URL condition is present.
- Cisco ASA firewalls earlier than version 9.1 with multiple security contexts enabled cannot use IPsec tunneling.
- NTLM for non-domain users is not supported.
- Some web pages do not load properly in Safari after successful user authentication. The workaround for this is to ensure the Block cookies option is set to Never in Safari's privacy preferences.

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 the browser considers the session cookie to be expired. To avoid this, ensure the system clock is set correctly.
- If a roaming user authenticates using single sign-on with Oracle Identity Federation, the secure authentication form is intermittently displayed if the session times out.
- Firefox sometimes fails to load the page correctly when an end user re-authenticates after session timeout. This occurs only if the session timeout is set to a very short time period.
- 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.
- If a roaming user authenticates using single sign-on with a supported provider, and their policy also mandates an Acceptable Use Policy (AUP), the compliance page appears only on the second site they browse to, and not on the first site which triggered their authentication.
- 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 appliances

- 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 connections 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.
- 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.

Endpoint reporting

- 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.

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 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.
- End users may have to clear their cache for the Google redirect feature to work correctly.
- When administrators add a connection to a policy, field-level validation on IP addresses and IP address ranges may result in up to 8 overlapping error messages displayed on the screen.

