

2016 Release 3 Notes for Forcepoint Cloud Web Protection Solutions

Cloud Web Protection Solutions | 27-Jul-2016

2016 Release 3 of our web protection products offers new features and product corrections:

- *What's new in 2016 Release 3?*
 - *Data Security (DLP) support for blocking, page 2*
 - *New Direct Connect web endpoint client, page 3*
 - *Enhanced management for i-Series appliances and edge devices, page 4*
 - *New and enhanced DLP classifiers, page 5*
 - *Features now generally available, page 5*
- *Resolved and known issues*
 - *Resolved issues*
 - *Known issues*

What's new in 2016 Release 3?

Cloud Web Protection Solutions | 27-Jul-2016

Data Security (DLP) support for blocking

Starting in this release, you can configure policies that block data security incidents.

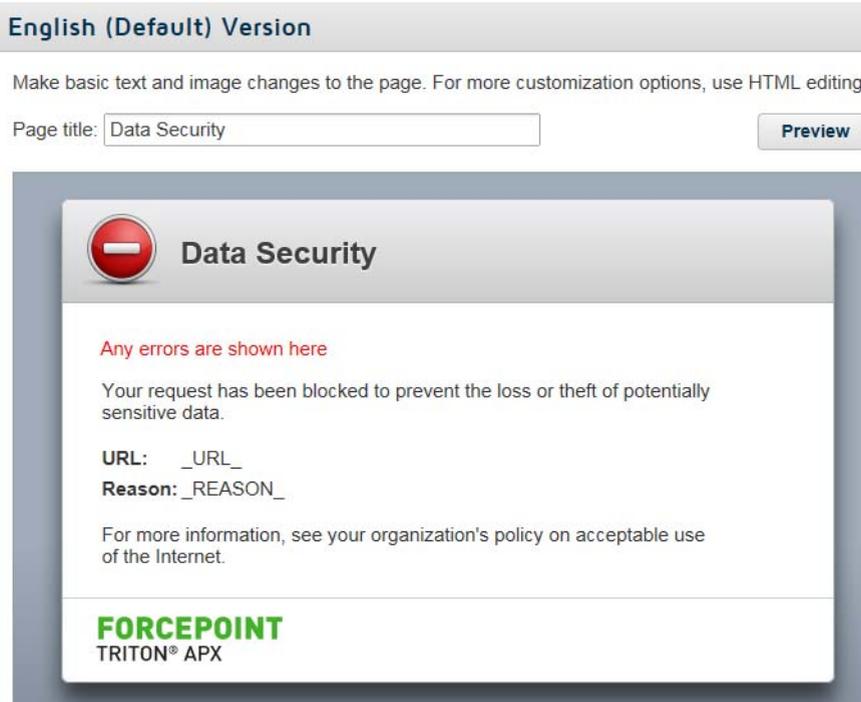
1. In the cloud portal, navigate to the **Web > Policies** page and select a policy.
2. Select the **Data Security** tab for the policy.
3. For each regulation or data theft type that you select, you can also specify an **Action**:
 - When you select the **Monitor** action (default), incidents are logged and appear in reports, but are not blocked.
 - When you select the **Block** action, any incident that violates the selected regulation is blocked, and the user receives a new Data Security block page.

Regulations

Select the geographical regions that you must regulate: [1 region selected](#)
Your selection determines which policies are used for the regulations below. It does not affect other w

<input type="checkbox"/>	Data Type	Action	Sensitivity
<input checked="" type="checkbox"/>	Personally Identifiable Information (PII)	Monitor	Default
<input checked="" type="checkbox"/>	Protected Health Information (PHI)	Monitor	Default
<input checked="" type="checkbox"/>	Payment Card Industry (PCI DSS)	Monitor	Default

Optionally customize the Data Security block page on the **Web > Block & Notification Pages** page, under **General**.



In the Incident Manager, a new column, **Action**, is displayed by default. For DLP regulations and data theft that are monitored, rather than blocked, the action shown is **Allow**.

Action is also available as an attribute for report filtering.

New Direct Connect web endpoint client

TRITON AP-ENDPOINT Web now includes 2 endpoint client options:

- A new endpoint client known as **Direct Connect** will route traffic directly to the Internet and contact a new endpoint cloud service to determine whether to block or permit a request, perform analysis of traffic content, and/or deliver endpoint configuration.

The Direct Connect endpoint may be beneficial for roaming users where proxy-type connections are problematic. This includes, for example, websites that do not work well with a proxy, areas where geographic firewalls prohibit the use of proxies, situations where localized content is required regardless of user location, and in complex/changing network environments.

Please see the TRITON AP-ENDPOINT Web Direct Connect release notes (available soon) for further details.

- The existing web endpoint client is now called the **Proxy Connect** endpoint. It redirects traffic to the cloud proxy for analysis.

Select which endpoint client to use on the **Web > Settings > Endpoint** page in the cloud portal. You can deploy a combination of Direct Connect and Proxy Connect endpoint clients in your organization.

Endpoint Client Download

Endpoint type: Direct Connect (i)
 Proxy Connect (i)

Platform: Windows 64-bit ▼

Available version: 1.5.8.1.3255 [Release notes](#) Supported on Windows XP, 7, 8, 8.1, 10

Automatic initial deployment is not supported for Direct Connect web endpoints. Both the Direct Connect and Proxy Connect web endpoints, however, can optionally receive automatic updates.

Enhanced management for i-Series appliances and edge devices

A new, limited-availability interface makes it easier and more efficient to manage and configure i-Series appliances and edge devices. It includes the ability to:

- Organize devices into folders for streamlined management
- Find devices via search
- Access device details from within the Device Management page, without opening a sub-page or pop-up

Edge Devices			
<input type="checkbox"/>	Name	Authentication	Default Policy
<input type="checkbox"/>	Devices		
<input type="checkbox"/>	All		
<input type="checkbox"/>	PSK devices		
<input type="checkbox"/>	Certificate devices		
<input type="checkbox"/>	Specific policy		
<input type="checkbox"/>	2122	Certificate	DEFAULT
<input type="checkbox"/>	Test1	PSK	DEFAULT
<input type="checkbox"/>	Test2	PSK	P1YE

Test1

Name: Test1

Description: Tes1

MAC address: 00:11:22:33:44:A1

Default policy: DEFAULT

Other policies: • P1YE
• P2YE

Authentication: PSK

Egress IP: 1.1.1.1

Pre-shared key: *****

When the feature is enabled for your account, you are prompted to try the new interface on the **Web > Settings > Network Devices** page. In case you aren't sure you're ready to make the change, a link at the bottom of the page can be used to toggle back to the original interface.

New and enhanced DLP classifiers

There are several new and improved DLP classifiers in TRITON AP-WEB Cloud. For details, refer to [Data Security Content Classifiers](#).

New

- Added new rules for the detection of Individual Numbers and Corporate Numbers in “Japan PII.”

Improved

- Raised the threshold for various classifiers
- Raised the threshold for “NHS number” default and narrow rules to 2.
- Raised the threshold for the various default and narrow “Common Medical Condition,” “Sensitive Disease or Drug,” and “Health Information” rules to 3.
- Raised the threshold for the “Greece PII: AFM number (Default)” rule to 2.
- Raised the threshold for various default and narrow “Name and driver license” rules to 3 in the policies “UK PII” and “Japan PII.”
- Raised the threshold of “South Korea PII: Korea Phones” and “Japan PII: Telephone Numbers” rules to 10.
- Changed the sensitivity of various classifiers
- Moved the rule “Malaysia PII: ID formal form with BP” to the wide sensitivity and the rule “Malaysia PII: ID formal form with BP with proximity” to the default/narrow sensitivity.
- Moved the rule “France PII: INSEE numbers” to the wide sensitivity.
- Moved the various default and narrow “Name and driver license” rules to the wide sensitivity in the policies “Australia PII,” “Canada PII,” “Ireland PII,” and “US PII.”
- Updated the Alexa database file for the Malware policy.

Features now generally available

After a period of time as limited-availability features, the features described in this section are now available to all TRITON AP-WEB Cloud administrators.

Using an existing policy as a template for new policies

When creating a new policy on the **Web > Policy Management > Policies** page, you can use an existing policy as a template. To do this, select the **Existing policy** option next to **Policy template**, then select a policy from the drop-down list. The current settings in that policy are copied into your new policy, except for the following:

- Proxied connections
- End user details
- Category and application control exceptions

Policy upload

You can automatically assign end users to policies by uploading a CSV file to the cloud service. Every line of the file must contain 2 fields, separated by commas:

- An email address belonging to an existing user in your account
- An existing policy in your account

To upload the file, navigate to the **Policy Assignment** section of the **Web > Policy Management > Policies** page, then browse to the CSV file and click **Upload**.

Group and policy assignment for synchronized users

You can select how synchronized users are assigned to web policies if they appear in more than one group in the directory. On the **Account > Groups** page, click the **Policy assignment method** link, and select one of the following:

- **Directory hierarchy** means that a user in multiple groups is assigned the policy for the group with the fewest intermediate group memberships. For example, if a user is a member of GroupA, and is also a member of GroupB which itself is a member of GroupC, the policy for GroupA takes precedence.
- **Group ordering** means that a user in multiple groups is assigned the policy associated with the group highest in the list on the **Groups** page. If you change the order of the groups by dragging and dropping the group names in the list, the user's policy assignment also changes.

Google redirect controls

Use Google redirect options to control the Google domain that your end users see. By default, Google redirects browsers to the appropriate site for the country it detects (for example, google.fr for France). This may not be accurate, however, for end users browsing through a cloud service proxy that is in a different country.

To use this feature, first enable SSL decryption for the Search Engines and Portals category on the **SSL Decryption** tab, and install the root certificate on end user machines. Next, define Google redirect behavior on each policy's **General** tab.

Office 365 bypass

To ensure that Microsoft Office 365 applications function properly, the cloud service 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** option.

Certificate error bypass

The cloud service verifies certificates for HTTPS sites that it has decrypted and analyzed. If certificate verification fails, by default, the end user sees an error page and cannot access the website. Optionally, use the **SSL** tab of the **Web > Settings > Bypass Settings** page to **Allow end users to bypass all certificate errors**.

When this feature is enabled, end users see a notification page informing them that there is a certificate error, and can either proceed to the site or go back. This notification page is not available with i-Series appliances.

Endpoint Auditing report

Use the **Reporting > Account Reports > Endpoint Auditing** page to see the current status of all users with web endpoint client software installed.

By default, the report displays the status of all endpoint users updated in the last 7 days, listing user names, workstation names, and whether the endpoint software is enabled or disabled. You can change the report to list only enabled or disabled endpoints, and edit the time period. You can also export the results to a CSV file.

End user controls for endpoint software

Optionally, give some or all users the ability to enable or disable web endpoint client software on their machines. This may be useful, for example, for users 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 enable end user controls, select the **End User Control** tab of the **Web > Settings > Endpoint** page. You can then specify whether to allow all users or specified users, groups, policies, or connections to enable and disable the endpoint client software.

Secure form-based authentication

For users who are using neither single sign-on nor the web endpoint to connect to the cloud service, you can enable **Secure form-based authentication** to display a login form to the end user. When users enter their cloud credentials, their request is sent over a secure connection for authentication.

Enable secure form-based authentication on the **Access Control** tab of your web policies.

Extended session timeout period

Users' credentials for single sign-on and secure form-based authentication must be revalidated periodically for security reasons. The time period is defined on the **Access Control** tab of your web policies under **Session timeout**. There are now options to extend the period beyond 30 days, to 3 months, 6 months, or 12 months.

Resolved and known issues

Cloud Web Protection Solutions | 27-Jul-2016

Resolved issues

Reporting

- For HTTP requests that reach the cloud service via firewall redirect, the Filtering Source attribute now correctly shows **Firewall redirect** in reports. Previously, “Cloud connection” was displayed.
- The correct Help page is now displayed for the **Reporting > Endpoint Auditing** page in the cloud portal when an administrator clicks Help > Explain this Page.
- The expected results are shown when the report filter “Threat Name not equal to None” is selected. Previously, the report returned values including “None.”

Data Security

- An incident is recorded when a user uploads content that violates Data Security policies to Google Drive. If Data Security blocking is enabled, the upload is blocked.

Blocking

- To resolve an issue that caused certain websites to always be blocked when the “block files of unknown type” option was selected, empty files are now classified as type “empty,” rather than type “unknown.”
- The correct icon is now displayed in the title bar for “Use Quota Time” block pages.

Query page

- When a user accesses the cloud portal query page to find out if a client is connecting to the cloud service via firewall redirect, the query page now correctly reports that “Yes: you are using the TRITON AP-WEB Filtering Proxy Server.”

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 IE 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

- 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 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.