2016 Release 1 Notes for Forcepoint Cloud Web Protection Solutions

Cloud Web Protection Solutions | 26-Feb-2016

2016 Release 1 of our web protection products offers new features and includes a number of product corrections:

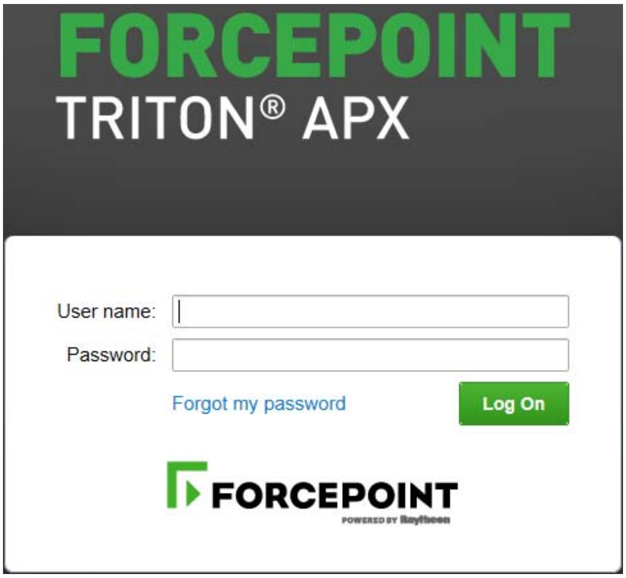
- *What's new in 2016 Release 1?*
  - *Look and feel enhancements*, page 1
  - *Support for multiple policies per network device*, page 2
  - *Configurable SSO redirection page*, page 3
  - *Access controls for Google Apps for Work*, page 4
  - *Reporting enhancement*, page 4
- *Resolved and known issues*
  - *Resolved issues*

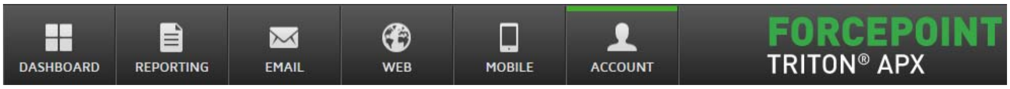
What's new in 2016 Release 1?

Cloud Web Protection Solutions | 26-Feb-2016

Look and feel enhancements

To support the transition from Raytheon | Websense to Forcepoint LLC, the cloud portal has a new look and feel. The colors and logos throughout the portal, including the logon screen and the portal toolbar, have been updated to reflect the Forcepoint brand.





In addition, if you are using the default block and notification pages, end users will see that the Websense logo has been replaced by the Forcepoint logo. If you have previously changed the default logo or customized your notification pages, however, your changes remain in effect and end users will not see any change.

These changes do not affect product functionality.

Over time, you may notice the branding extended to other areas of the portal, like the Help system, as well as to external content, like the Knowledge Base.

Support for multiple policies per network device

In the past, only one policy could be assigned to an i-Series appliance or supported edge device.

Starting in this release, you can define each internal network managed by an appliance or edge device, and assign a different policy to each.

Note

This feature is not available for devices older than v1.6.0. If you are using an older appliance that does not support this feature, the corresponding controls in the user interface are disabled and an explanation is displayed.

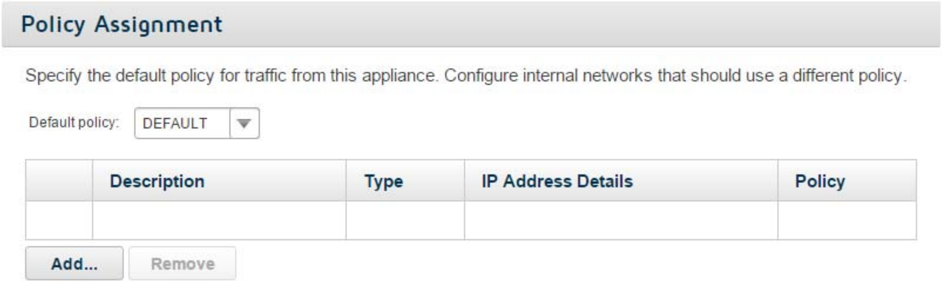
Warning

Currently, when you assign multiple policies to a device, all users must have a policy that has been mapped to the device. When a user has a policy that is not mapped to the device, user authentication fails.

Define the internal networks managed by each appliance or edge device on the **Web** > **Settings** > **Network Devices** page in the Cloud TRITON Manager.

- Click the name of an existing device to edit its properties.
- Click **Add** to configure a new device.

You can then configure both the default policy for the device and the internal networks with separate policies.



Policy Assignment

Specify the default policy for traffic from this appliance. Configure internal networks that should use a different policy.

Default policy: DEFAULT

	Description	Type	IP Address Details	Policy

Once you have configured policies for your devices, the assignments are reflected in the Connections tab for each policy, under Proxied Connections.

Configurable SSO redirection page

The page displayed when users are redirected to your organization’s single sign-on (SSO) service is now configurable.

To edit the page, navigate to **Web** > **Block & Notification Pages** in the Cloud TRITON Manager and expand the **Authentication** list.

When you click the **SSO Redirection Page** entry, you are given the option to edit the:

- Languages in which the page will be displayed
- Page title
- Page content
- Logo
- Page footer

Access controls for Google Apps for Work

A new feature makes it possible to allow end users to access the Google Apps for Work service using only specified credentials. Users attempting to log on to Google services using personal credentials instead of corporate credentials, for example, could be blocked from accessing those services.

Your organization must have a subscription to Google Apps for Work before you can activate this feature.

To request that this feature be enabled for your account, contact Forcepoint Technical Support.

Reporting enhancement

The Report Builder now includes a new Advanced attribute: **Data Center**. The values of this attribute reflect which cloud service data center handled a given request.

Resolved and known issues

Cloud Web Protection Solutions | 26-Feb-2016

Resolved issues

Policies

- When an administrator enabled the Personally Identifiable Information (PII) policy for the USA region on the Data Security tab of a given Web policy, no DLP incidents were triggered. This issue has been corrected. (EI-8016)
- In some circumstances, the General Email category was allowed, even though it was supposed to be blocked. This issue has been corrected. (EI-7479)
- URLs with newer top-level domains (like xyz) could not be added to the Non-Proxied Destinations list on the Connections tab for a policy. This issue has been corrected.
- When an exception was applied to a group, and the group was deleted, administrators could no longer edit the exception. This issue has been corrected. (EI-6881)

Endpoint

- When auto-installation of Web endpoint clients is enabled for an organization, end users with Chrome browsers now receive a redirect page to inform them that auto-installation requires Internet Explorer or Firefox.

Reporting

- The Connection IP was shown as “Not available” in reports for explicit proxy and i-Series clients. The egress IP address is now shown as the Connection IP for these client types. (EI-7249)

i-Series appliances

- The option to bypass Office 365, offered on the **Web** > **Settings** > **Bypass Settings** page under **Cloud Applications**, is now supported by i-Series appliances.

2016 Release 2 Notes for Forcepoint Cloud Web Protection Solutions

Cloud Web Protection Solutions | 20-May-2016

2016 Release 2 of our web protection products offers new features and product corrections:

- *What's new in 2016 Release 1?*
  - *File Sandbox reporting options*, page 6
  - *Firewall redirect supports HTTPS and non-proxied destinations*, page 8
- *Resolved and known issues*
  - *Resolved issues*

What's new in 2016 Release 2?

Cloud Web Protection Solutions | 20-May-2016

File Sandbox reporting options

For organizations whose accounts include the Web Sandbox Module, a new attribute is available in the Report Builder and Transaction Viewer. In addition, 2 new sandboxing reports have been added to the Report Catalog.

Report Builder and Transaction Viewer

File Sandbox Status, found under **Security** in the Attributes list, can be used to find information about files submitted for sandboxing analysis. There are 3 possible status values:

- **Malicious** indicates that sandbox analysis detected potentially damaging, malicious behavior.
- **No threat detected** indicates that sandbox analysis did not detect any malicious behavior.
- **Pending** indicates that a file has been submitted to the sandbox and is queued for analysis.

When sandboxing analysis is performed for one or more files associated with a transaction, the Transaction Details pane in the Transaction Viewer includes a **File Sandbox** tab. The tab lists each file submitted for sandbox analysis, as well as its status. If one or more of the files associated with the transaction is found to be malicious, the File Sandbox tab label is displayed in red.

Report Catalog

The **Web** > **Security** folder in the Report Catalog contains two new reports:

- **Detailed File Sandboxing Report** provides details about files downloaded by end users that were sent for sandbox analysis in the last 7 days.
- **Top File Sandboxing Results** gives an overview of the top results returned by sandbox analysis in the last 7 days.

Firewall redirect supports HTTPS and non-proxied destinations

The Firewall Redirect connection method can be used to transparently redirect web traffic from offices to the cloud service. This feature has been enhanced to support:

- HTTPS traffic
- Non-proxied destinations configured both on the **Web** > **Bypass Settings** > **Proxy Bypass** page, and within web security policies

Administrators in environments that use firewall redirect can now configure domains (such as those used by Windows Update) to bypass filtering.

Important

Currently, the firewall redirect feature does not provide automatic data center failover. Where transparent redirect and automatic failover is required, please use the IPsec VPN connection method. Contact Technical Support for details.

Resolved and known issues

Cloud Web Protection Solutions | 20-May-2016

Resolved issues

- The cloud service now accepts **.online** as a valid top-level domain.
- The EPS (Encapsulated PostScript) format has been reclassified as an image file type. It will no longer be blocked when executable file blocking is enabled.
- The **Web** > **Policies** > **Time Access Exceptions** page in the cloud portal now links to the correct Help page.

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 1?*
  - *Data Security (DLP) support for blocking*, page 10
  - *New Direct Connect web endpoint client*, page 12
  - *Enhanced management for i-Series appliances and edge devices*, page 12
  - *New and enhanced DLP classifiers*, page 13
  - *Features now generally available*, page 14
- *Resolved and known issues*
  - *Resolved issues*

What's new in 2016 Release 3?

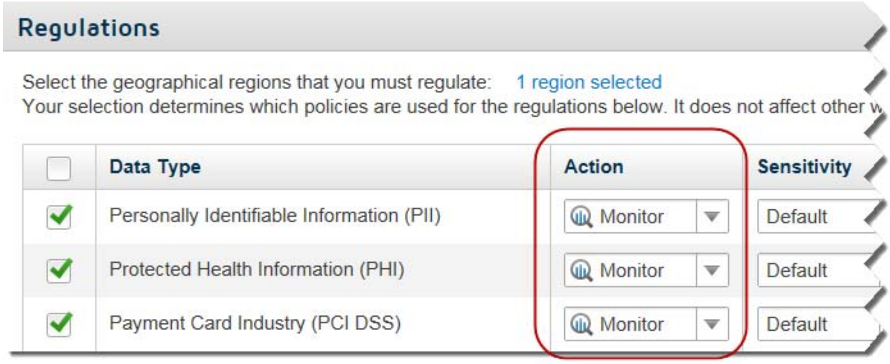
Cloud Web Protection Solutions | 27-Jul-2016

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.



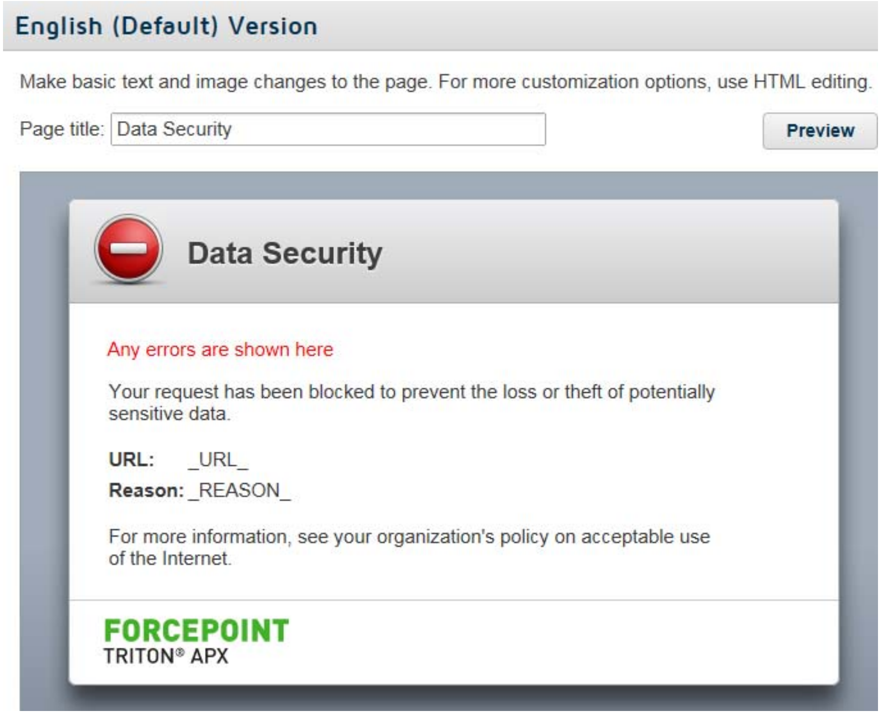
Regulations

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

☐	Data Type	Action	Sensitivity
☑	Personally Identifiable Information (PII)	Monitor	Default
☑	Protected Health Information (PHI)	Monitor	Default
☑	Payment Card Industry (PCI DSS)	Monitor	Default

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



English (Default) Version

Make basic text and image changes to the page. For more customization options, use HTML editing.

Page title: Data Security

Data Security

Any errors are shown here

Your request has been blocked to prevent the loss or theft of potentially sensitive data.

URL: _URL_

Reason: _REASON_

For more information, see your organization's policy on acceptable use of the Internet.

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

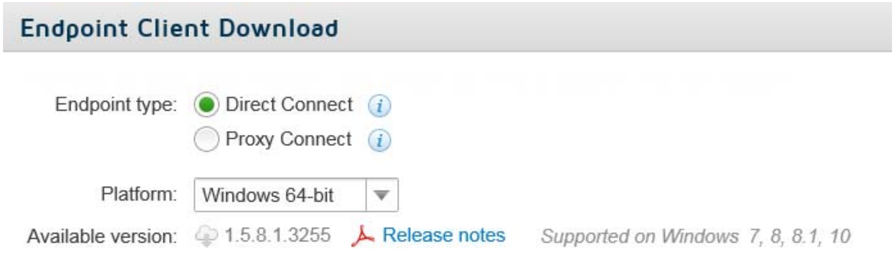
TRITON AP-ENDPOINT Web now includes 2 endpoint client options:

- 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 ○ Proxy Connect

Platform: Windows 64-bit

Available version: 1.5.8.1.3255 Release notes Supported on Windows 7, 8, 8.1, 10

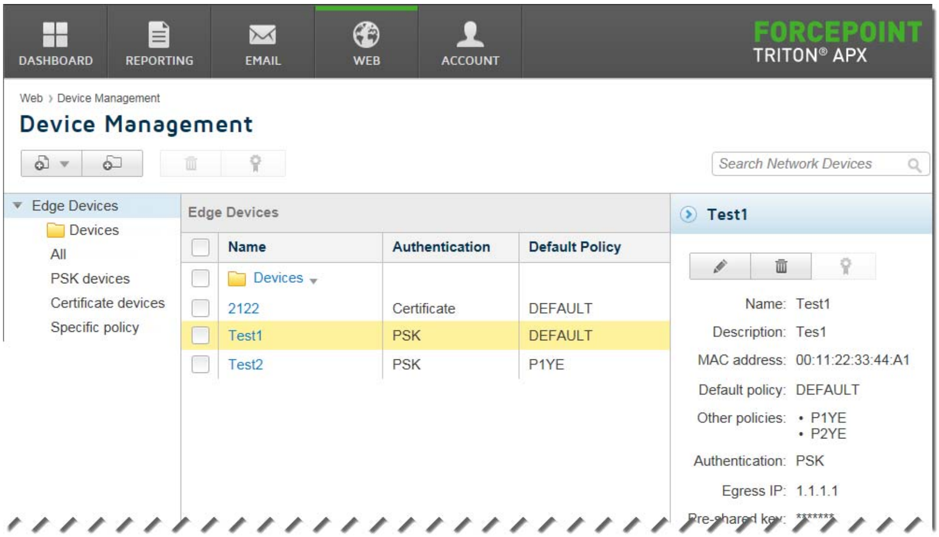
Automatic initial deployment is not supported for Direct Connect web endpoints. Both the Direct Connect and Proxy Connect web endpoints, however, can optionally receive automatic updates.

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



Name	Authentication	Default Policy
Devices		
2122	Certificate	DEFAULT
Test1	PSK	DEFAULT
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 P**olicy 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 logon 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.”

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 1?*
  - *First logon wizard for new accounts*, page 18
  - *Define trusted categories for Data Security*, page 19
  - *Enhanced proxy bypass definitions*, page 20
- *Resolved and known issues*
  - *Resolved issues*

What's new in 2016 Release 4?

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

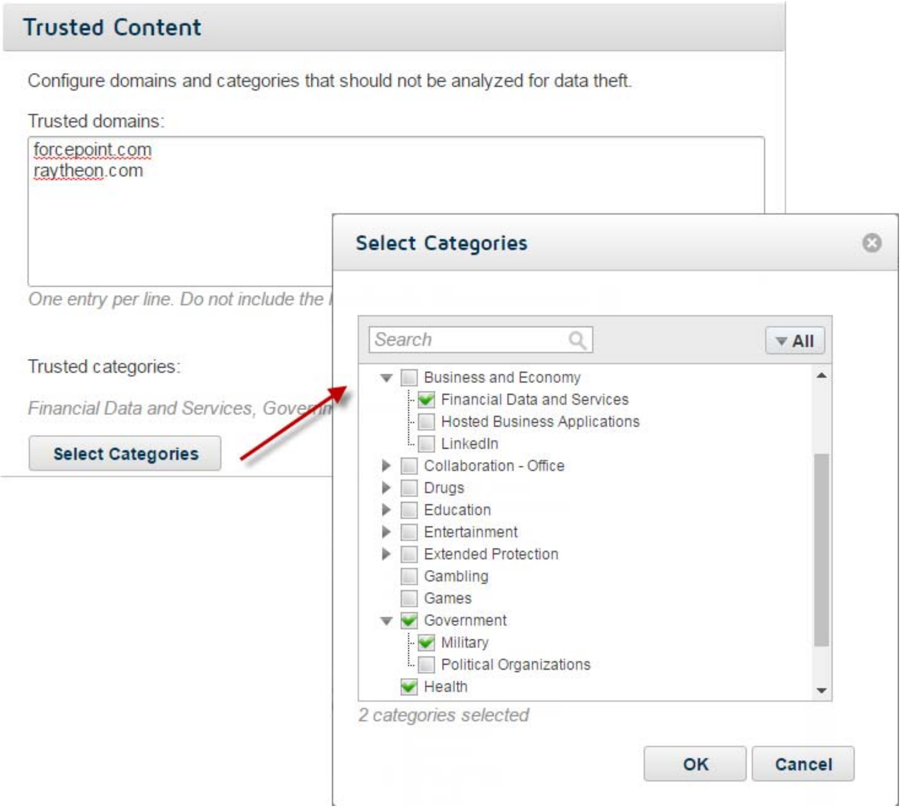
First logon wizard for new accounts

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.



Trusted Content

Configure domains and categories that should not be analyzed for data theft.

Trusted domains:

forcepoint.com
raytheon.com

One entry per line. Do not include the

Trusted categories:

Financial Data and Services, Govern

Select Categories

Select Categories

Search ▾ All

- ☐ Business and Economy
  - ☑ Financial Data and Services
  - ☐ Hosted Business Applications
  - ☐ LinkedIn
- ☐ Collaboration - Office
- ☐ Drugs
- ☐ Education
- ☐ Entertainment
- ☐ Extended Protection
- ☐ Gambling
- ☐ Games
- ☑ Government
  - ☑ Military
  - ☐ Political Organizations
- ☑ Health

2 categories selected

OK Cancel

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

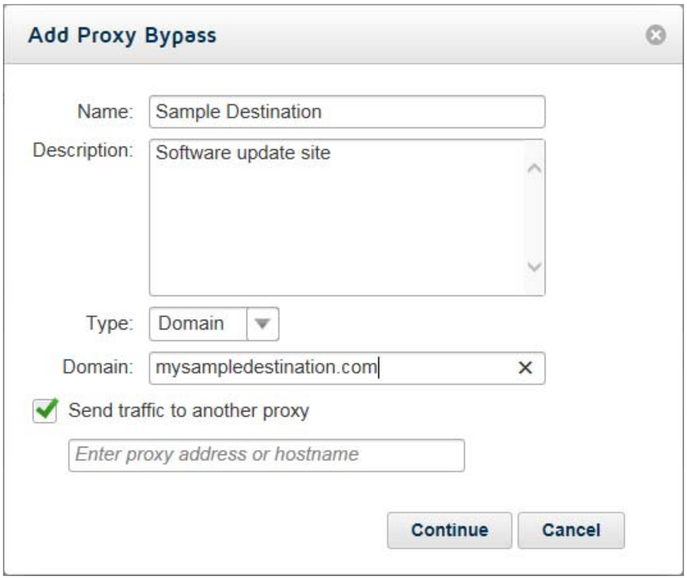
As with trusted domains, trusted category definitions are:

- 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).



Add Proxy Bypass

Name: Sample Destination

Description: Software update site

Type: Domain

Domain: mysampledestination.com

☑ Send traffic to another proxy

Enter proxy address or hostname

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 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.

2016 Release 3 & 4 Notes for IPsec Service

2016 Release 3 & 4 Notes | IPSec Service | 17-October-2016

The IPsec Service is a part of the cloud infrastructure that supports VPN tunneling for TRITON AP-WEB Cloud.

In this release, the IPsec Service has received updates to enhance support for Stonesoft Next-Generation Firewall (NGFW) connections to the cloud service

For more information about using NGFW to connect to the cloud service, see IPsec Tunneling with Stonesoft NGFW.

New cloud service VPN ID

The VPN ID for the cloud service VPN has changed from "vpn.gns.forcepoint.com" to **vpn.gns.forcepoint.net**.

To support this change, new certificates were issued for organizations using NGFW. This includes changes to the CA.

The documentation has also been updated to reflect this change.

Stability enhancements

- Two issues that could cause "service unavailable" errors have been corrected in the IPsec service.
- Shutdown procedures for services in the IPsec Service infrastructure have been improved to ensure that IPsec tunnels are terminated cleanly.

2016 Release 5 Notes for Forcepoint Cloud Web Protection Solutions

Cloud Web Protection Solutions | 2016 Release 5 | 17-Nov-2016

2016 Release 5 of our web protection products offers new features and product corrections:

- *What's new in 2016 Release 1?*
  - *Increased efficiency for scheduled report jobs*
  - *Cloud Connection Speed Test enhancement*
  - *Internal IP address test for network devices*
  - *Define trusted categories for Data Security*
  - *Enhanced device management interface available*

What's new in 2016 Release 5?

Cloud Web Protection Solutions | 2016 Release 5 | 17-Nov-2016

Increased efficiency for scheduled report jobs

In order to increase resiliency for accounts that have many or very large scheduled report jobs, changes have been made to:

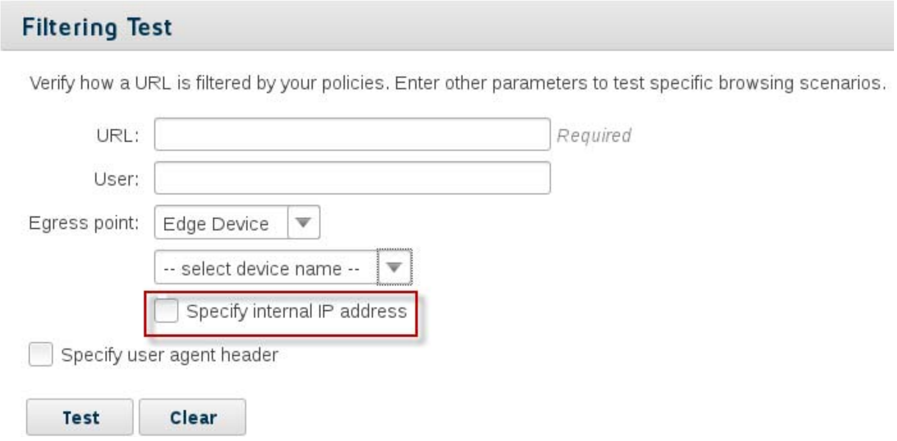
- Increase the job timeout period to allow jobs that take more than 15 minutes to complete
- Distribute the start time when multiple jobs are scheduled
- Increase the frequency with which the scheduler runs to every 5 minutes

Cloud Connection Speed Test enhancement

When an administrator runs the Cloud Connection Speed Test, the results now show the IP address in addition to the name of the data center used for the test.

Internal IP address test for network devices

The Filtering Test option on the **Web** > **Policies** page in the cloud portal has been enhanced. When administrators select an edge device or appliance as the egress point, they now have the option to specify also an internal IP address, to validate how requests from that address are managed.



Filtering Test

Verify how a URL is filtered by your policies. Enter other parameters to test specific browsing scenarios.

URL: Required

User:

Egress point: Edge Device

-- select device name --

□ Specify internal IP address

□ Specify user agent header

Proxy bypass for firewall redirect and IPsec tunneling deployments

Proxy bypass is now supported for those who use firewall redirect or IPsec tunneling to direct traffic to the cloud service. This applies to both policy-level and account-level bypass definitions, which may be IP addresses, subnets, or domains.

The cloud service allows traffic to these sites without authentication or decryption. The traffic is, however, logged, and does appear in reports.

> ✓ **Note**
>
> In IPsec deployments, proxy bypass does not work correctly if the request is redirected from HTTP to HTTPS.

Enhanced device management interface available

Administrators now have the option of using either of 2 interfaces for managing i-Series appliances and edge devices: the original Network Devices page or the new Device Management page. Switch between the interfaces easily:

- Click **Check out the new Device Management page** near the top of the old page to switch to the new interface.
- Click **Revert Interface** at the bottom of the new page to return to the original interface.

A separate document provides more information about the new interface.

2016 Release 6 Notes for Forcepoint Cloud Web Protection Solutions

Cloud Web Protection Solutions | 2016 Release 6 | 15-Dec-2016

2016 Release 6 of our web protection products offers new features and product corrections:

- *What's new in 2016 Release 1?*
  - *Limited availability Setup Wizard for new accounts*
- *Resolved and known issues*
  - *Resolved issues*
  - *Known issues*

What's new in 2016 Release 6?

Cloud Web Protection Solutions | 2016 Release 6 | 15-Dec-2016

Limited availability Setup Wizard for new accounts

This release introduces a Setup Wizard to guide administrators of new accounts through the initial configuration process. When this feature is enabled for a new account, it guides the administrator through the process of:

- Verifying their firewall setup
- Adding or synchronizing end user information
- Deploying PAC files
- Creating a policy
- Verifying their filtering setup

The wizard provides a streamlined version of the process described in the Cloud Web Getting Started Guide.

Resolved and known issues

Cloud Web Protection Solutions | 2016 Release 6 | 15-Dec-2016

Resolved issues

Network device management

- The title of the pop-up message used to show connection details for an i-Series appliance or edge device has been changed to View Connection Details.

Proxy bypass settings

- When administrators mark **Send traffic to another proxy** on the Add Bypass Destination page, they now have the option to specify a non-standard port for the proxy (for example, sampleproxy:8080).

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.