Forcepoint Web Security Cloud: 2017 Release Notes

Forcepoint Web Security Cloud | 2017 Release Notes | Last updated 30-Nov-2017

This document details product updates and new features added to Forcepoint Web Security Cloud during 2017.

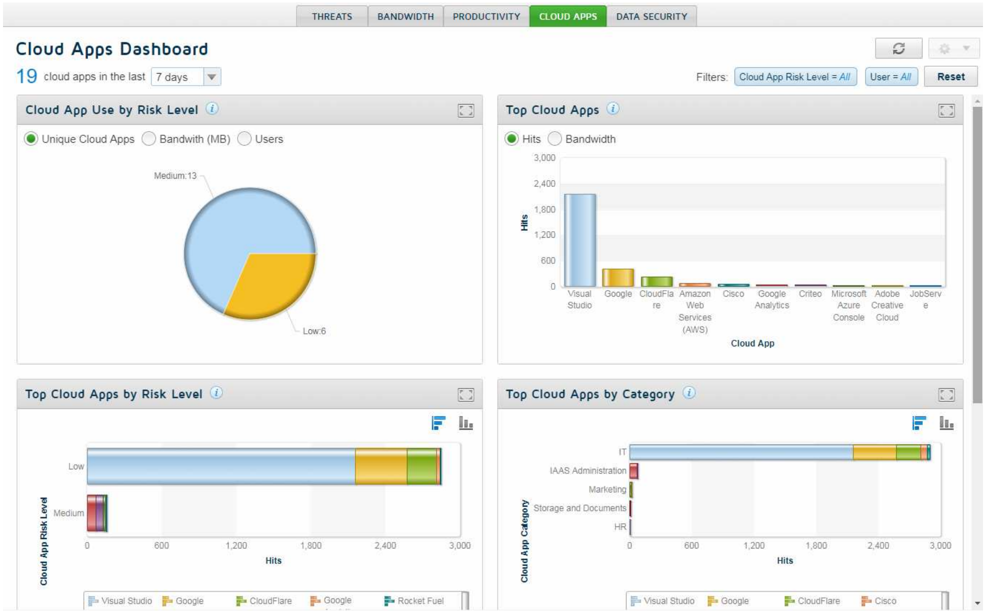
What’s new?

Limited availability: cloud application usage and risk reporting

Added 30-Nov-2017

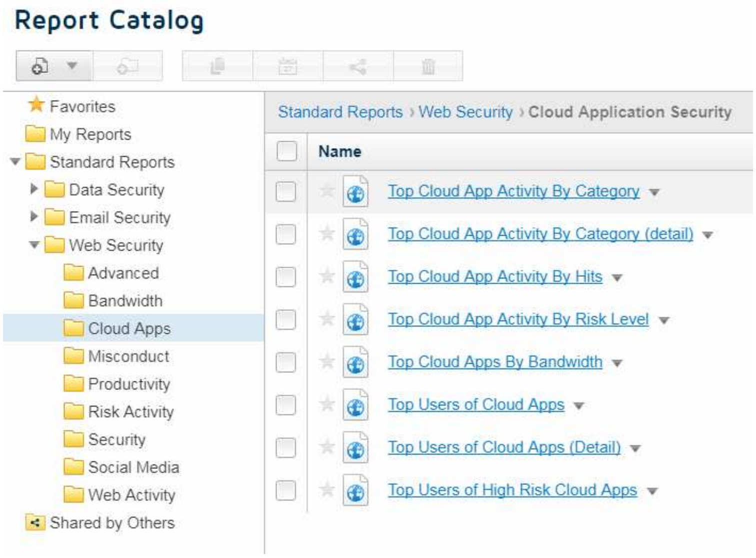
A new set of reporting features is now available within Forcepoint Web Security Cloud, providing visibility over the use of cloud-based applications (cloud apps) in your organization. The new features provide cloud app usage and risk reporting by integrating cloud app intelligence from Forcepoint CASB.

A new cloud apps dashboard provides a real-time summary of cloud app usage, showing the most popular cloud apps being accessed by your users, cloud app usage by risk level, and the top users of cloud apps.



Clicking an item in the dashboard lets you drill down to a more detailed view in the Report Center. The new dashboard is accessed by navigating to the new Cloud Apps tab on the **Dashboard** page.

For detailed historical reporting, 8 new predefined cloud app reports are available in the Report Catalog, showing cloud app usage, hits and bandwidth used, broken down by category, risk level, and individual users. These reports can be accessed by navigating to **Reporting > Report Catalog**, and opening the **Standard Reports > Web Security > Cloud Apps** folder.



Standard Reports › Web Security › Cloud Application Security

Name
Top Cloud App Activity By Category
Top Cloud App Activity By Category (detail)
Top Cloud App Activity By Hits
Top Cloud App Activity By Risk Level
Top Cloud Apps By Bandwidth
Top Users of Cloud Apps
Top Users of Cloud Apps (Detail)
Top Users of High Risk Cloud Apps

In Report Builder and Transaction Viewer, a new set of cloud app attributes provide the ability to drill down and create detailed, customized reports on cloud app usage across your organization.

For more information on using these reporting features, see the Forcepoint Security Portal Help.

For many organizations, the growing use of cloud apps creates the potential for security and compliance blind spots. The new cloud apps reporting features are designed to help your organization to eliminate those blind spots by providing detailed information on cloud app usage risks and trends. Further cloud app features within Forcepoint Web Security Cloud are planned for release in 2018, helping you respond to evolving security threats.

To learn more about the Forcepoint CASB solution, please visit the product page on the Forcepoint website: Forcepoint CASB.

✓ **Note**

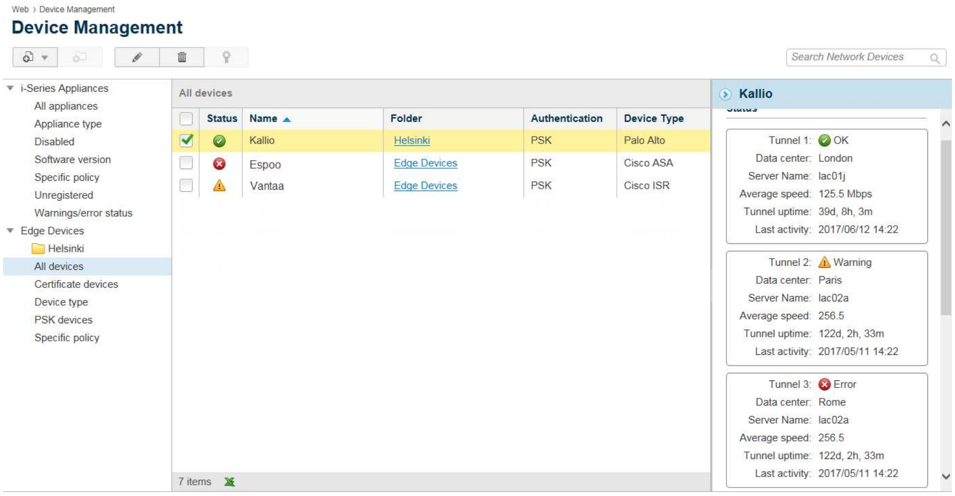
The cloud app usage and risk reporting features are currently limited availability and may not be available in your account. Please contact your support representative if you require further information, or wish to enable the feature for your account.

IPsec tunnel status

Added 30-Nov-2017

The Forcepoint Web Security Cloud Device Management interface has been updated with a new feature displaying the current status of IPsec tunnels connecting your edge devices to the cloud service. The interface is accessed via **Web > Device Management**.

A status icon is displayed for each device, showing the health of the connection to the Forcepoint cloud service, including any cause codes associated with the condition.



Web › Device Management

Device Management

Search Network Devices

- i-Series Appliances
  - All appliances
  - Appliance type
  - Disabled
  - Software version
  - Specific policy
  - Unregistered
  - Warnings/error status
- Edge Devices
  - Helsinki
  - All devices
  - Certificate devices
  - Device type
  - PSK devices
  - Specific policy

All devices

□	Status	Name ▲	Folder	Authentication	Device Type
☑	✓	Kallio	Helsinki	PSK	Palo Alto
□	✗	Espoo	Edge Devices	PSK	Cisco ASA
□	⚠	Vantaa	Edge Devices	PSK	Cisco ISR

7 items

Kallio

	Tunnel 1	Tunnel 2	Tunnel 3
Status	✓ OK	⚠ Warning	✗ Error
Data center:	London	Paris	Rome
Server Name:	lac01j	lac02a	lac02a
Average speed:	125.5 Mbps	256.5	256.5
Tunnel uptime:	39d, 8h, 3m	122d, 2h, 33m	122d, 2h, 33m
Last activity:	2017/06/12 14:22	2017/05/11 14:22	2017/05/11 14:22

If a device has multiple tunnels, hovering your mouse over the status indicator in the list reveals the status for each tunnel.

The device detail panel on the right side of the screen has also been updated, with new panels displaying detailed information for each tunnel, including the average speed, uptime, and last detected activity. Open the details panel by clicking a device in the list.

For more information on managing your edge devices using the Device Management interface, see Managing edge devices in the Forcepoint Security Portal Help.

These changes will improve your ability to maintain and monitor connectivity to your web protection product. Forcepoint is working on additional connectivity options and features for release in 2018, to help customers continually adapt their security to meet the challenges of new technology, best practices and a changing threat landscape.

Note

IPsec is a connectivity method that allows you to securely forward traffic to the cloud service from a supported edge device over a virtual private network (VPN). For more information on the Forcepoint IPsec service, see the Forcepoint IPsec Guide.

YouTube Restricted mode

Added 19-Sep-2017

The YouTube for Schools feature, used to restrict access to video content, has been replaced with a new option, **YouTube Restricted mode**. The setting is available for the YouTube category, under Bandwidth on the Web Categories tab of your policies.

This setting allows you to limit access to potentially inappropriate content on YouTube by removing videos that YouTube has flagged as restricted. The content that appears in Restricted mode is controlled by YouTube. Videos may be flagged by YouTube as restricted if mature content is detected by an automated system, or if a reviewer has set an age restriction to a video.

For more information on using this feature, see Youtube Restricted mode in the Forcepoint Security Portal help.

Withdrawal of support for SSLv3 and RC4 ciphers

Added 24-Aug-2017

In line with industry best practices, Forcepoint continually reviews and updates the security of encrypted Web connections. As part of this process, Forcepoint Web Security Cloud has now disabled the use of SSLv3, and RC4 ciphers, in downstream connections received from clients. Forcepoint has previously taken steps to avoid the use of less-secure protocols and ciphers such as these for upstream connections to origin servers.

Please see the Tech Alert for this update here:

- Update to supported cipher suite, 8-Aug-2017

Terms of use for administrators

Added 29-Jun-2017

The new **Terms of use** option allows you to display a page that requires administrators to agree to your company's terms of use before logging on to the Forcepoint Security Portal. The setting is configured on the **Account > Contacts** page under Administrator Account Management.

When enabled, this setting applies to all portal administrators. The next time portal administrators log on, they will be prompted to either accept your terms of use, or log off.

✓ **Note**

By default, a generic “Agree to Terms of Use” block page is provided. Before enabling this feature, ensure you customize this page to include details of (or a link to) your company’s terms of use.

See the Forcepoint Security Portal Help for details of how to customize block pages.

Accessing PAC files via HTTPS

Added 29-Jun-2017

Accessing proxy auto-config (PAC) files over an HTTPS connection provides an additional level of security. Forcepoint Web Security Cloud allows both standard and policy-specific PAC files to be retrieved via HTTPS.

The HTTPS URLs for your PAC files are now displayed alongside the HTTP addresses on the **Web > General** page, and on the **General** tab of your web policies.

The standard HTTPS PAC file URL retrieves the PAC file on port 8087. Browsing is performed via port 8081.

For users accessing the service via networks where these ports are locked down, the alternate HTTPS PAC file URL should be used. This uses port 443 to access the PAC file, and port 80 for browsing.

For more information, see the Forcepoint Security Portal Help.

Blocking top-level domains in custom categories

Added 01-Jun-2017

In addition to URLs, IP addresses, and address ranges, top-level domains (such as *.xzy) can now be blocked on the **Web > Policy Management > Custom Categories** page. Wildcards (*) can be used at the beginning of a string to block any sites with the specified domain extension.

For more information, see the Forcepoint Security Portal Help.

ISO 27018 certification for Forcepoint Cloud Protection Solutions

Added 01-Jun-2017

Forcepoint recently added ISO 27018 certification to its Cloud Trust Program, to provide a robust system of controls for privacy protection of personal data. This enhances the compliance of the cloud service with the General Data Protection Regulation (GDPR) that comes into effect in May 2018.

Forcepoint runs a dedicated Cloud Trust Program that encompasses ISO 27001, ISO 27018, and CSA STAR certifications with Service Organization Control (SOC) attestations. All Forcepoint cloud service certifications can be viewed in the Security Portal, under **Help** > **Privacy & Security**.

Product renaming

Added 20-Apr-2017

As part of a rebranding program for the Forcepoint product set, TRITON AP-WEB Cloud is now called Forcepoint Web Security Cloud.

You will see the new product name and logos within the cloud portal, which is now called the Forcepoint Security Portal (formerly the Cloud TRITON Manager).

The following Forcepoint Web Security Cloud product modules have also been changed:

- Forcepoint Web Security Endpoint (formerly TRITON AP-ENDPOINT Web)
- Forcepoint Advanced Malware Detection for Web (formerly Threat Protection Cloud - Web, or Web Sandbox Module)
- Forcepoint URL Filtering (formerly Websense Web Filtering & Security)
- Forcepoint Threatseeker Intelligence (formerly Threatseeker Intelligence Cloud)
- Forcepoint I Series appliance (formerly i-Series appliance)

The new branding for all Forcepoint products can be seen at the Forcepoint website.

Two-factor authentication for administrators

Added 02-Mar-2017

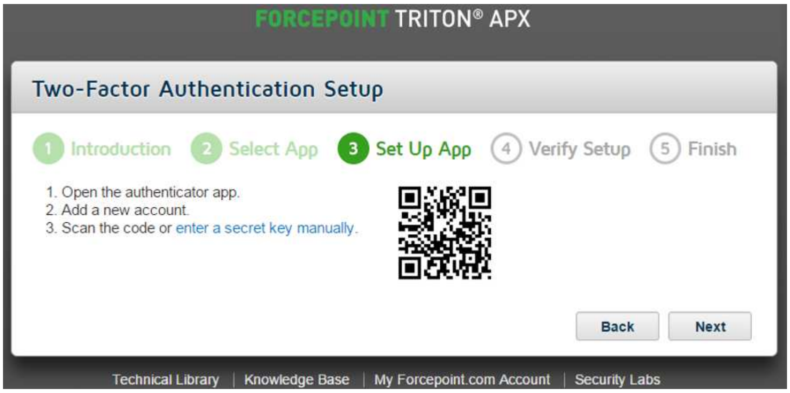
Two-factor authentication can now be enabled for portal users, providing an additional level of security for access to the cloud portal. When this feature is enabled, all administrators are required to enter both their password and a code generated by an authenticator app to access the portal.

Note

Compatible authenticator apps are available for Android, iOS, Blackberry, and Windows Phone. Desktop and browser-based apps are also available for Microsoft Windows, Mac OS, and Linux. Forcepoint validates this feature with the Microsoft Authenticator app, but alternative apps that use the Time-based One-time Password Algorithm (TOTP) protocol, such as Google Authenticator, are also supported.

Administrators can enable or disable two-factor authentication for portal administrators using the **Account > Contacts** page.

When users log on with two-factor authentication for the first time, a setup wizard guides them through the configuration process.



Two-Factor Authentication Setup

1. Open the authenticator app.
2. Add a new account.
3. Scan the code or enter a secret key manually.

For portal users who are unable to use their authenticator app, two-factor authentication can be reset on the **User** page. This requires portal users to repeat the authenticator app setup process.

The process of enabling and using two-factor authentication is detailed in the Forcepoint Security Portal Help.

Device type attribute for third-party firewalls

Added 02-Mar-2017

The **Network Devices > Device Management** page is used by customers connecting to the cloud service via IPsec, using a third-party firewall or a Forcepoint I Series appliance. This page now includes a new attribute of **Device type** for third-party firewall devices and routers. This attribute is shown in the Edge Devices table and the device information panel, and can be used to filter the table by the make/model of the device.

This attribute is now required when devices are added to the portal or imported from a CSV file. The device type attribute for existing devices will show as “Not configured”. A device type can be assigned to each device using the **Edit Edge Device** page, if required.

Single sign-on support for Okta

Added 02-Mar-2017

Okta, the cloud-based identity management solution, is now a supported provider for use with single sign-on (SSO). SSO provides seamless authentication for end users accessing the cloud proxy. When SSO is enabled, end users connecting to the proxy are redirected to the identity provider specified in their policy. Once users have been authenticated by the provider, they are redirected to the proxy, and the appropriate policy applied. Clients who have authenticated once do not need to re-authenticate for a set period of time, defined as the session timeout period for the policy.

For more information on using single sign-on feature, see Single Sign-On for Forcepoint Web Security Cloud.

✓ **Note**

Single sign-on is a limited-availability feature and may not be available in your account. Please contact your support representative if you require further information, including details of the providers we currently support across our cloud and hybrid solutions.

Improved single sign-on support for roaming users

Added 22-Feb-2017

For customers accessing proxy auto-config (PAC) files using port 80, these PAC files now include a new hostname that supports single sign-on (SSO) authentication for connections to the cloud service via port 80. This allows seamless use of SSO services for both local users and roaming users in locations where non-standard ports may be locked down.

For more information on using single sign-on feature, see Single Sign-On for Forcepoint Web Security Cloud.

✓ **Note**

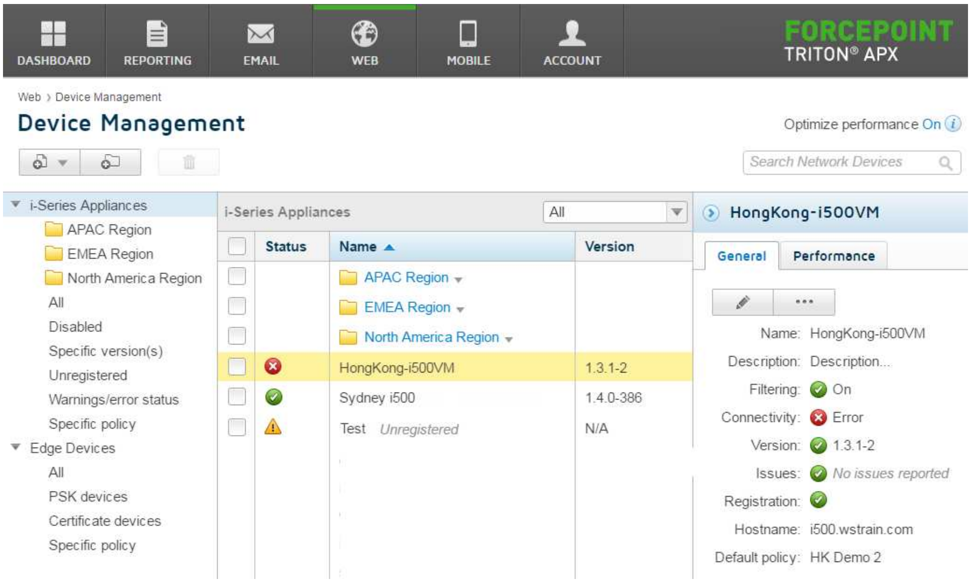
Single sign-on is a limited-availability feature and may not be available in your account. Please contact your support representative if you require further information.

Enhanced device management interface

Added 30-Jan-2017

Forcepoint Web Security Cloud has been updated with a new device management interface, which provides an easier and more efficient way to manage and configure I Series appliances and edge devices. The new interface allows you to:

- Organize devices into folders for streamlined management
- Find devices via search
- Perform bulk operations to update multiple devices at once
- Access device details from within the Device Management page, without opening sub-pages or pop-ups.



Device Management

- i-Series Appliances
  - APAC Region
  - EMEA Region
  - North America Region
  - All
  - Disabled
  - Specific version(s)
  - Unregistered
  - Warnings/error status
  - Specific policy
- Edge Devices
  - All
  - PSK devices
  - Certificate devices
  - Specific policy

i-Series Appliances — All

□	Status	Name ▲	Version
□		APAC Region	
□		EMEA Region	
□		North America Region	
□	☒	HongKong-i500VM	1.3.1-2
□	✓	Sydney i500	1.4.0-386
□	⚠	Test *Unregistered*	N/A

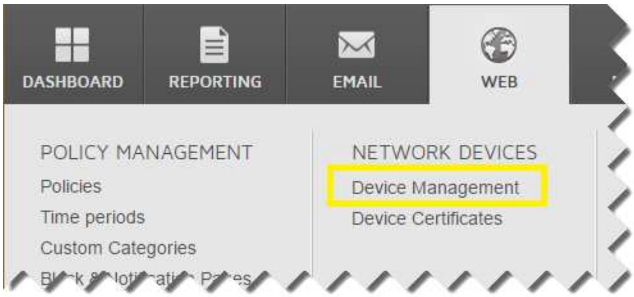
HongKong-i500VM

General | Performance

Name: HongKong-i500VM
Description: Description...
Filtering: ✓ On
Connectivity: ☒ Error
Version: ✓ 1.3.1-2
Issues: ✓ *No issues reported*
Registration: ✓
Hostname: i500.wstrain.com
Default policy: HK Demo 2

The management page has also been moved to a new section in the reorganized Web menu.

- Previous location: **Web > Settings > Network Devices**
- New location: **Web > Network Devices > Device Management**



Resolved and known issues

Last updated 30-Nov-2017

To see the latest list of known and resolved issues for Forcepoint Cloud Web Protection Solutions, see Resolved and known issues for Forcepoint Web Security Cloud - 2017 in the Forcepoint Knowledge Base.

You must log on to My Account to view the list.

Limited availability features

Last updated 30-Nov-2017

The table below lists Forcepoint Web Security Cloud features that are in a limited availability status. Limited availability features may have been released recently, or may need to be approved by your account manager before being added for your organization, due to additional configuration requirements, or other considerations.

If you are interested in enabling any of these features for your account, please contact Technical Support.

Feature	Description
Acceptable use policy	Allows administrators to require that end users periodically accept the terms of an acceptable use policy (AUP) before continuing to browse via the proxy. The feature can be set per policy, and users are required to accept the AUP every 1, 7, or 30 days. The AUP confirmation screen can be customized under **Web > Policy Management > Block & Notification Pages**. For further information, see the Forcepoint Security Portal Help.
Cloud app usage and risk reporting	Cloud app usage and risk reporting features provide visibility over the use of cloud-based applications. A cloud apps dashboard provides a real-time summary of cloud app usage, while a catalog of pre-built reports provides data for common reporting scenarios. A set of Report Builder metrics and attributes provide the ability to drill down and create detailed, customized reports. For further information, see the Forcepoint Security Portal Help.
Password policy for end users	Allows you to apply the same password policy requirements both for administrators accessing the cloud portal, and end users manually authenticating with the proxy. Password policy settings are configured on the **Account > Contacts** page. For further information, see the Forcepoint Security Portal Help.
Single sign-on	Single sign-on (SSO) allows seamless authentication for end users accessing the cloud proxy, using a supported identity provider. Suitable for pure cloud or hybrid solutions. Please contact Technical Support for details of currently supported identity providers. For further information, see Single Sign-On for Forcepoint Web Security Cloud.
Full traffic logging	Allows administrators to download full web traffic logs for retention and analysis, which can be useful for integration with third-party SIEM tools. Logs can be downloaded for 14 days and are provided in JSON format. For further information, see Configuring Full Traffic Logging on the Forcepoint Support website.