Forcepoint Web Security Cloud: 2018 Release Notes

Forcepoint Web Security Cloud | 2018 Release Notes | Last updated 10-Dec-2018

This document details product updates and new features added to Forcepoint Web Security Cloud during 2018.

What's new?

New IP address ranges for improved content localization

Added 10-Dec-2018

Forcepoint has released new virtual point of presence (vPoP) IP address ranges for Web Security Cloud customers located in the following countries:

- Colombia
- Israel
- Mexico

The new addresses are a virtual point of presence (vPoP) in these territories, which will result in improved content localization for users. The addresses are within Forcepoint's existing IP address spaces. No customer action is required.

For more information on the Forcepoint vPoP service, see the following article in the Forcepoint Knowledge Base: Improved content localization with virtual point of presence (vPoP) IP addresses.

New PAC file control options for Proxy Connect Endpoint

Added 06-Dec-2018

New options on the Endpoint tab allow administrators to control the PAC file URL used by the Proxy Connect Endpoint to direct web traffic to Web Security Cloud. The new options can be used to select:

- The default PAC file URL
- The alternate PAC file URL (uses port 80 for browsing, useful for networks with non-standard ports locked down)
- An HTTPS PAC file URL to retrieve the PAC file over a secure connection. This option can be used with both the default or the alternate PAC file address.

The new endpoint control options can be found under *Endpoint PAC Control* on the **Web > Policies > [policy name] > Endpoint** tab. For more information about

configuring these options, see Endpoint tab in the Forcepoint Web Security Cloud help.

For customers who have previously enabled this option via a custom policy template, settings will be migrated to use the new interface.

For information about the PAC file URL options and their application in different scenarios, see Proxy auto-configuration (PAC) in the Forcepoint Web Security Cloud help.

Note

The **Retrieve PAC file over HTTPS** option requires Proxy Connect Endpoint build 2826 or later. Earlier versions of Proxy Connect Endpoint will always download the PAC file over HTTP, and are not affected by this setting. You must ensure that your Endpoint clients have connectivity to a Forcepoint data center on TCP ports 8087 or 443, as appropriate, before enabling this option. See Configuring your firewall to connect to the cloud service in the Forcepoint Web Security Cloud help.

Default landing page change

Added 28-Nov-2018

In order to improve the customer log on experience, the default landing page for Security Portal administrators has been changed to the **Account > Licenses** screen. Note that you can change your default landing page at any time, by clicking the arrow next to your logon account name and selecting **Set Landing Page**.

Proxy bypass destination and custom category changes

Added 19-Nov-2018

In order to improve customer experience, Forcepoint is capping the total number of proxy bypass destinations and custom categories that can be used. Based on customer analysis, the changes will provide ample capacity. If you have any questions about these changes, please contact Technical Support.

Improved Google content localization

Added 15-Nov-2018

Forcepoint has introduced improved content localization for Google services (such as search and Google maps). Content localization for Google services can now be based on the user's IP address instead of the IP address of the Forcepoint data center through which traffic is routed. To take advantage of this localization improvement for Google

services, ensure that SSL decryption is enabled for web categories that match Google sites (such as “Search Engines and Portals”). No browser configuration is required.

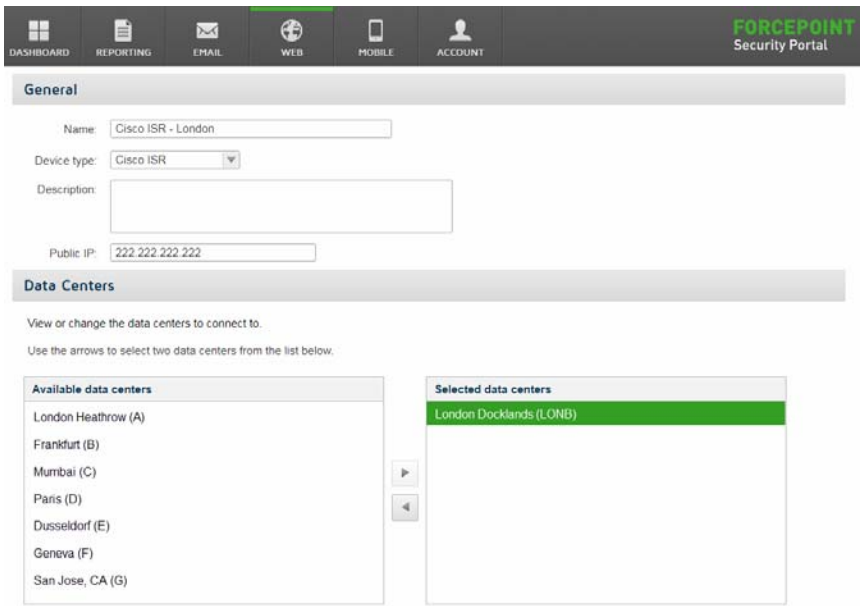
GRE connectivity for Forcepoint Web Security Cloud

Added 08-Nov-2018

Following a successful beta trial, Forcepoint is pleased to announce that GRE tunneling connectivity is now available for Web Security Cloud and Web Security Hybrid customers.

Generic Routing Encapsulation (GRE) is a widely inter-operable, easy-to-configure tunneling protocol that is supported by a wide range of edge devices. The Forcepoint GRE service can be used to transparently redirect traffic from your sites to the cloud service. Forcepoint GRE supports NTLM identification, allowing users to browse the Internet without explicitly providing credentials. Because tunneling allows the customer’s private IP address space to be visible to the cloud service, policy enforcement and reporting can be based on internal IP address ranges.

Use the updated Device Management interface to add, manage, and import edge devices for GRE connectivity. The interface is accessed via **Web > Device Management**.



For each device, Forcepoint provides two geographically separate data center connections, providing connection redundancy. For organizations with multiple sites, a CSV import simplifies the process of bulk adding devices.

For more information on adding edge devices for GRE connectivity, see Managing edge devices in the Forcepoint Security Portal help.

The interface also provides a real-time status indicator, showing the current health of each tunnel connection. The status panel shows whether the connection is up, down, or unknown, and displays the date and time that activity was last detected from the tunnel.

GRE connectivity can be used by any type of organization, but can be particularly beneficial for scenarios where ease of setup is important, or where other deployment methods (such as endpoint installation, GPO, or a browser configuration) are problematic. These include organizations with remote offices, guest WiFi networks, or unmanaged devices.

The Forcepoint GRE service uses Forcepoint's industry-leading Next Generation Firewall (NGFW) to terminate tunnels in the cloud, delivering excellent performance, high availability, and load balancing.

For more information on deploying GRE, see the Forcepoint GRE Guide on the Support website.

Notes

To enable GRE connectivity for your account, please contact your Forcepoint account manager.

By default, customers can create 2 tunnels (GRE or IPsec) connecting to the cloud service. For additional capacity requirements, please contact your sales account manager.

Virtual point of presence address ranges for improved content localization

Added 05-Nov-2018

To improve content localization, Forcepoint has made available new IP address ranges for Web Security Cloud customers located in countries where Forcepoint does not have a physical data center presence. On 5 November, new addresses were made available for customers in the following countries:

- Argentina
- Norway

- Spain

The new addresses are a virtual point of presence (vPoP) in these territories, which will result in improved content localization for users. The addresses are within Forcepoint's existing IP address spaces. No customer action is required.

With this new service, Forcepoint is expanding its worldwide reach for Web Security Cloud to points of presence in 30 countries. Additional vPoPs will be announced in 2019. For a full list of cloud service IP addresses, see the article Cloud service data center IP addresses and port numbers in the Forcepoint Knowledge Base.

Report Builder has also been updated with a new attribute, **Localized Country**, to enable reporting on the vPoP location for web transactions. This attribute shows when a vPoP IP address was used, and records the country where the vPoP is located. For more information on web reporting, see Web Reporting Tools in the Forcepoint Web Security Cloud help.

For more information on the Forcepoint vPoP service, see the following article in the Forcepoint Knowledge Base: Improved content localization with virtual point of presence (vPoP) IP addresses.

Cloud App Control: integration with Forcepoint CASB

Added 28-Sep-2018

Cloud App Control is a new add-on module for Forcepoint Web Security Cloud and Web Security Hybrid that integrates with Forcepoint CASB to provide granular control over the use of cloud-based applications (cloud apps) in your organization.

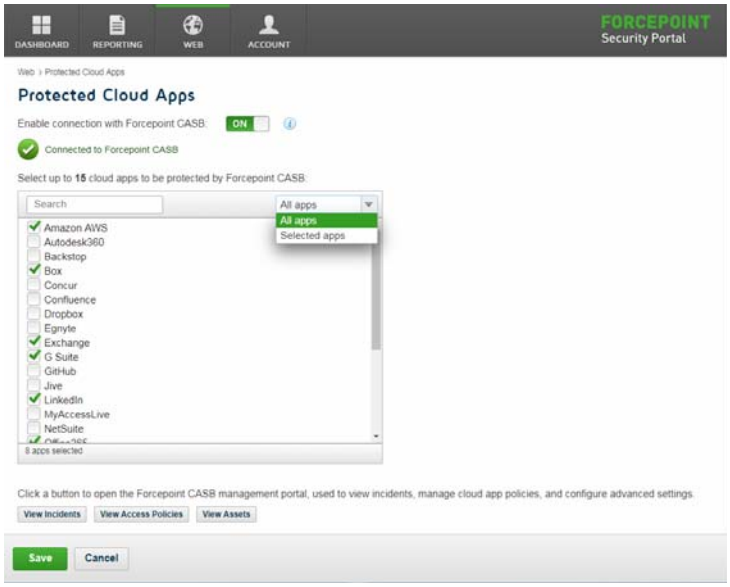
Cloud App Control lets you nominate a set of cloud apps sanctioned for use within your organization to be protected. When a user accesses one of your protected cloud apps, the service forwards traffic to Forcepoint CASB for analysis, and CASB determines whether to allow the request or apply an enforcement action, based on your CASB configuration.

Notes

Cloud App Control requires an additional license. If you would like further information on purchasing this feature, please contact your account manager.

Cloud App Control cannot be used with the Direct Connect endpoint.

In the Security Portal, use the new Protected Cloud Apps page to connect your service to Forcepoint CASB, to manage the applications that are protected, and to open the Forcepoint CASB management portal.



In the CASB portal, you can monitor activity using risk summary dashboards, user risk analysis reports and timelines, and real-time audit logs, as well as set your CASB policy to apply enforcement actions. Policy breaches are aggregated into incidents for ease of management. Click a button beneath the app selection box in the Security Portal to log on to CASB and open one of the following pages:

- **View Incidents**: open the incident log to view alerts and policy violations.
- **View Access Policies**: manage user access policies for cloud apps within Forcepoint CASB.
- **View Assets**: manage settings for the cloud apps protected by Forcepoint CASB.

The Protected Cloud Apps page can be accessed via **Web > Settings > Protected Cloud Apps**. See Configuring Web Settings > Configure protected cloud apps in the Forcepoint Web Security Cloud help for more information.

Note

For hybrid users, the Protected Cloud Apps page is accessed in the Security Manager (from version 8.5) via **Web > Settings > CASB Configuration > Protected Cloud Apps**. See Server Administration for Web Protection Solutions > Protected cloud apps in the Forcepoint Security Manager help for more information.

Report Builder has also been updated with a new attribute, **Cloud App Forwarded**, to enable reporting on CASB activity for your protected cloud apps. This attribute shows when a transaction involving one of your protected cloud apps has been forwarded to CASB for analysis. For more information, see Web Reporting Tools in the Forcepoint Web Security Cloud help.

The new Protected Cloud Apps feature and cloud app usage and risk reporting features leverage Forcepoint CASB to provide visibility and control over official and unofficial use of cloud apps within your organization. Forcepoint CASB is an integrated solution for cloud application access discovery, activity analysis, access control, security monitoring and enforcement, governance, policy compliance, and data loss prevention. To learn more about the Forcepoint CASB solution, please visit the product page on the Forcepoint website: Forcepoint CASB.

Important: storage location for CASB data

At service launch, all CASB data for cloud and hybrid deployment types will be stored in US data centers only. Forcepoint is currently targeting the end of 2018 to remove this constraint. Following the removal of this constraint, new deployments will be able to choose US or EMEA data centers to store CASB data.

After initial configuration, CASB data cannot be migrated to a new data center location. Because of this, only customers who choose to store their CASB data in US data centers, and who are comfortable with any privacy and regulatory implications of this, should use this service add-on until the data storage location constraint is removed. A further announcement will be made when EMEA data center locations are available for cloud and hybrid deployments.

Note that this constraint affects only CASB data, and has no impact on the storage location for Forcepoint Web Security Cloud/Hybrid data.

Google redirect override feature removed

Added 18-Jul-2018

The **Override Google redirect behavior** feature has been removed from web policies. Due to a recent change in Google's redirect behavior, this feature no longer functioned as intended. Users can now set their default location using the Google home page, via Settings > Search Settings > Region Settings.

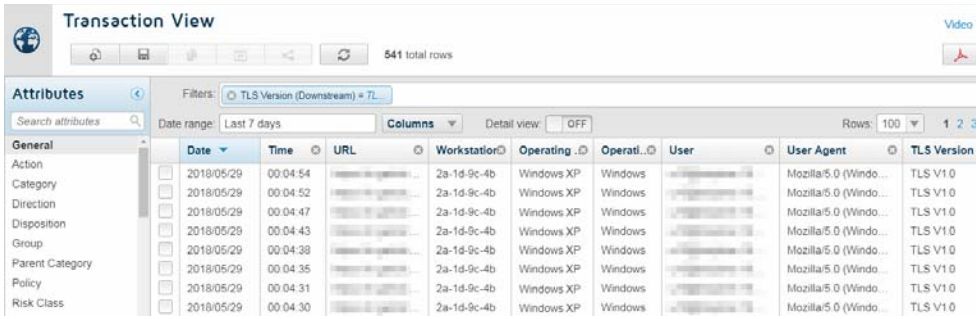
New Report Builder attribute: TLS Version (Downstream)

Added 19-Jun-2018

Report Builder has been updated with a new attribute, *TLS Version (Downstream)*. This attribute has been added to provide administrators with visibility of the TLS versions that are in use for downstream connections between your organization and the Forcepoint cloud proxy.

The new attribute is designed to assist organizations to identify legacy applications still using TLS version 1.0. TLS 1.0 is no longer accepted in the industry as a secure protocol, and Forcepoint has previously announced that support for TLS version 1.0 will be withdrawn in a future release.

The *TLS Version (Downstream)* attribute can be used as part of a Transaction Viewer report to see details of any users or workstations in your network connecting to the cloud proxy via TLS version 1.0, enabling you to take appropriate action.



For guidance on the withdrawal of support for TLS version 1.0 in connections to the Forcepoint cloud service, refer to the following article in the Forcepoint Knowledge Base: TLS 1.0 deprecation guidance for Forcepoint Web Security Cloud and Web Security Hybrid customers.

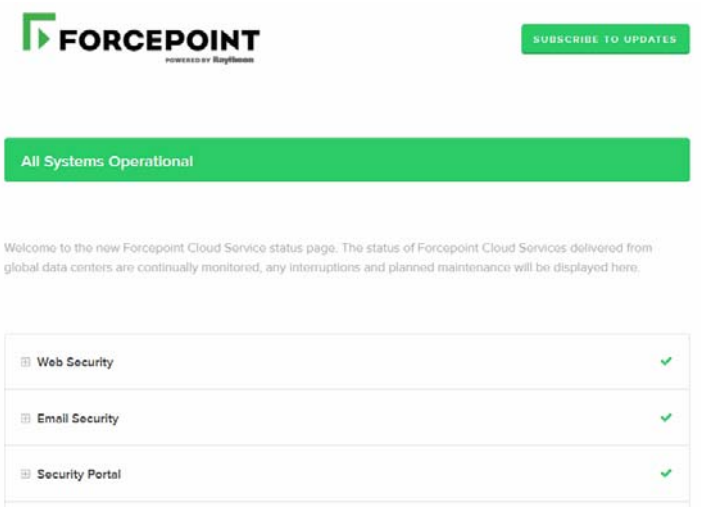
The article includes guidance on which operating systems and applications support TLS version 1.1 and 1.2, and steps showing how to build a Transaction Viewer report using the new attribute to gain visibility of TLS version 1.0 usage.

New cloud status monitoring service

Added 19-Jun-2018

Forcepoint has launched a new cloud status monitoring service, displaying the current service status for the global network of Forcepoint data centers for Web Security Cloud, Email Security Cloud and related services. The page details any interruptions to service and displays any planned maintenance to Forcepoint data centers. You can subscribe to service updates via email, SMS, or RSS feed, to be notified whenever Forcepoint adds or updates an incident.

The new service status page can be accessed at: https://trust.forcepoint.net/



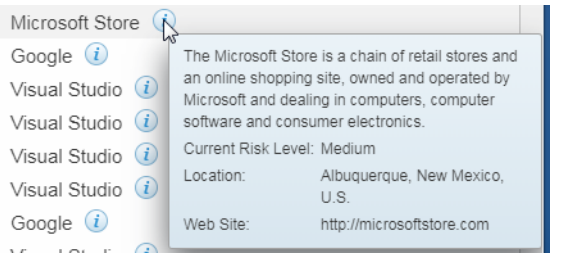
Customers using the previous service status page at https://status.forcepoint.net will be redirected to the new service. However, this redirect will be withdrawn 30 days from the date of this announcement. Please ensure any bookmarks are updated to use the new address.

Enhancements to cloud application usage and risk reporting features

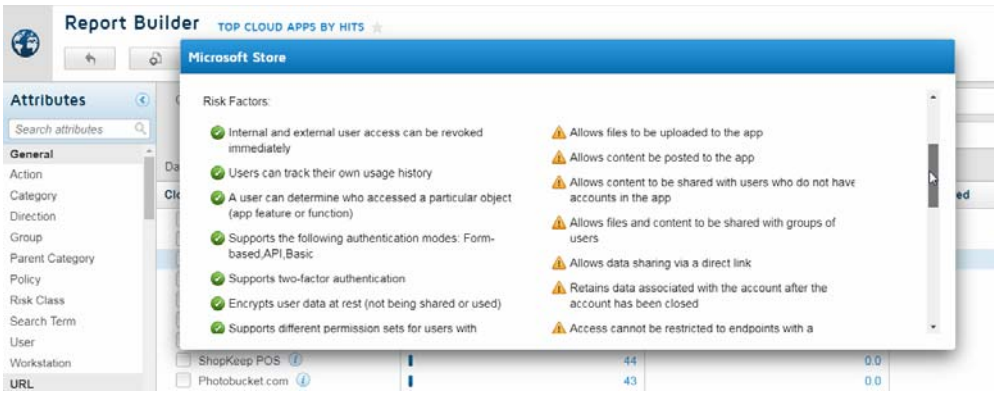
Added 07-Jun-2018

Forcepoint Web Security Cloud now includes additional cloud application usage and risk reporting features, designed to provide administrators with a detailed view of cloud app usage within their organization.

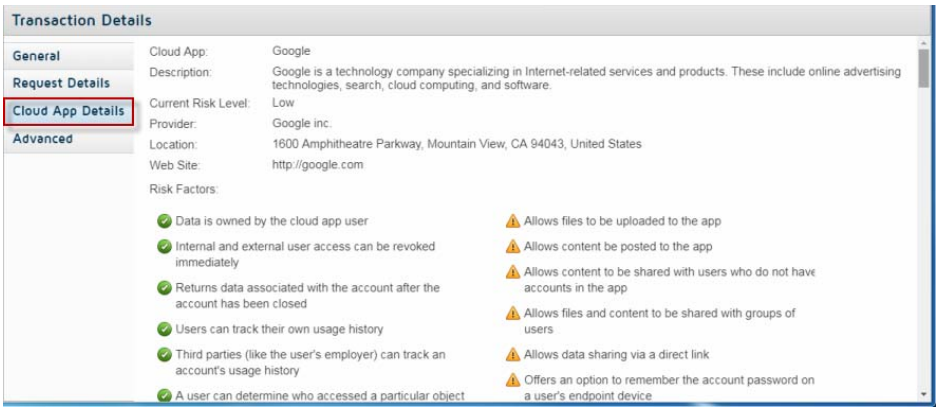
In Report Builder, summary information for each cloud app is available by hovering your mouse over the “i” icon for each cloud app listed in a report:



Click this icon to open a panel showing cloud app details and risk factors, enabling you to assess a cloud app at a glance.



This information is also available for each cloud app that appears in Transaction Viewer (**Reporting > Report Center > Transaction Viewer**). Toggle the **Detail view** setting to **ON**. Transactions that involve cloud apps have a "Cloud App Details" tab, where extended information on the cloud app can be found:



Report Builder has also been updated with the following new metrics to assist in creating detailed reports on cloud app usage:

- **Cloud App Count** (metric): displays the number of unique cloud apps involved in transactions for the selected attributes and filters.
- **User Count** (metric): displays the number of unique users involved in transactions for the selected attributes and filters.

The growing use of cloud apps within many organizations (sometimes referred to as "shadow IT") has the potential to create security and compliance blind spots. The new cloud app reporting features, integrating information from Forcepoint CASB, are designed to help your organization to eliminate those blind spots by providing detailed information on cloud app usage trends and risks. For more information on the cloud application usage and risk reporting features available in Forcepoint Web Security Cloud, see *Cloud application usage and risk reporting now generally available*, page 12.

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

Update to Help > Data Privacy menu

Added 07-Jun-2018

The **Help > Data Privacy** menu within the Security Portal has been revised to include updated documentation on the management of personal data within the Forcepoint cloud infrastructure. The relevant menu options appear depending on your product licensing, and provide updated information on Forcepoint Web Security Cloud and Forcepoint Email Security Cloud. The updated documents replace the previous Data Privacy FAQ.

The documents are intended to answer customer queries on the use of personal data by the Forcepoint cloud service, and form part of the wider Forcepoint Cloud Trust Program. Details available at: https://www.forcepoint.com/forcepoint-cloud-compliance

To review the updated documents, use the links in the **Help** menu within the Forcepoint Security Portal:

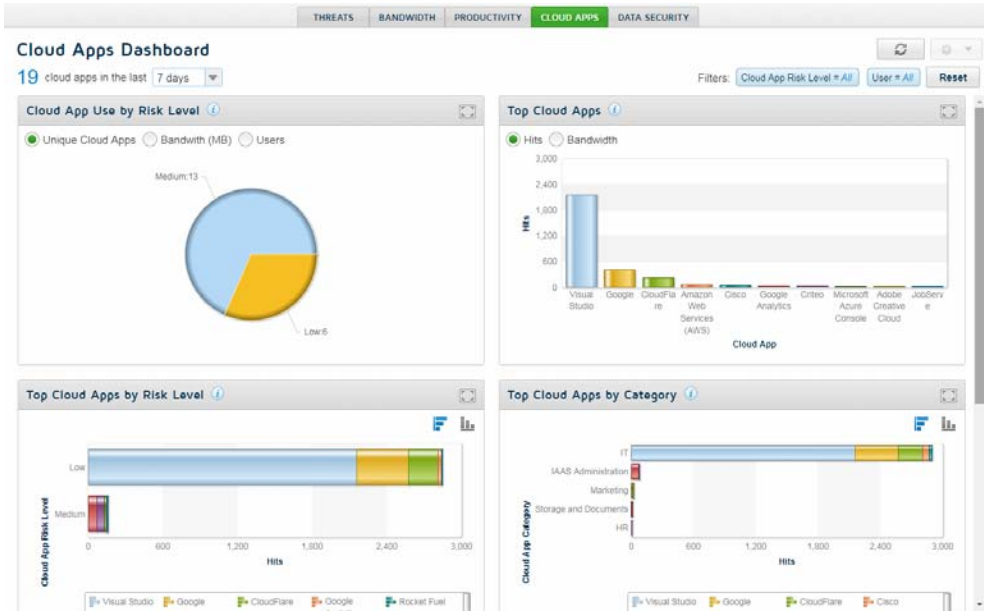
- **Help > Data Privacy > Web Security Cloud**
- **Help > Data Privacy > Email Security Cloud**

Cloud application usage and risk reporting now generally available

Added 10-Jan-2018

Following a period of time in limited availability, a new set of cloud application usage and risk reporting features is now available to all Forcepoint Web Security Cloud administrators. These features provide visibility over the use of cloud-based applications (cloud apps) in your organization, integrating cloud app intelligence from Forcepoint CASB.

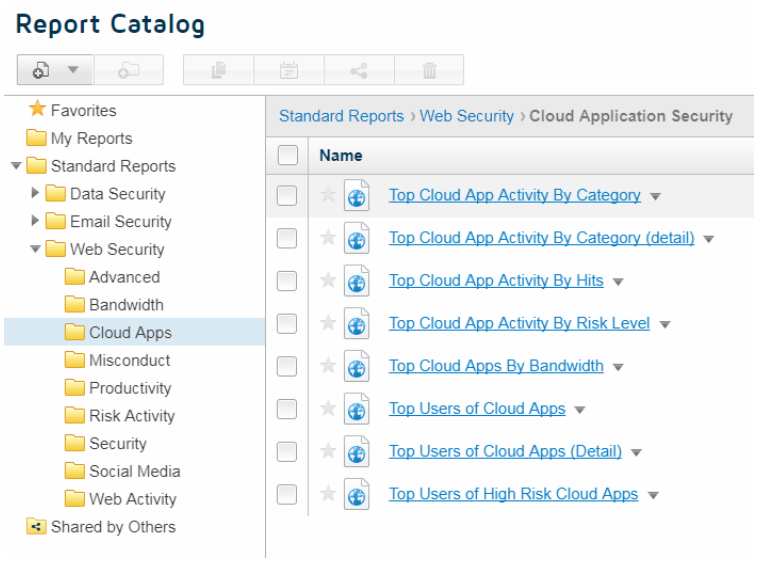
A new cloud apps dashboard provides a real-time summary of cloud app usage, showing the most popular cloud apps being accessed by your users, cloud app usage by risk level, and the top users of cloud apps. Access the page by navigating to the **Dashboard > Cloud Apps** tab.



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.



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 these reporting features, see Cloud portal dashboards and Web reporting tools in 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 app 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 later 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.

2017 updates

Last updated 10-Jan-2018

For details of new features added, and issues resolved during 2017, please see the Forcepoint Web Security Cloud 2017 Release Notes.

Resolved and known issues

Last updated 15-Nov-2018

To see the list of issues resolved for Forcepoint Web Security Cloud during 2018, see Resolved and known issues for Forcepoint Web Security Cloud - 2018 in the Forcepoint Knowledge Base.

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

Limited availability features

Last updated 10-Jan-2018

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.
IPsec connectivity	Enables customers to connect to the Forcepoint cloud service using IPsec tunneling. Edge devices and digital certificates can be added and managed in the cloud portal. For further information, supported devices, and supported configurations, see the article IPsec configuration settings in the Forcepoint Knowledge Base.
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.

Feature	Description
Web performance monitoring tool	The performance monitoring tool can be used to test connection latency and speed when accessing specific websites via the cloud proxy. This is useful for testing and troubleshooting purposes. The tool is currently only supported in Microsoft Internet Explorer. For further information, see the Forcepoint Security Portal Help.