Forcepoint Web Security Cloud: 2019 Release Notes

Forcepoint Web Security Cloud | 2019 Release Notes | Last updated 02-Dec-2019

This document details product updates and new features added to Forcepoint Web Security Cloud during 2019.

- *Resolved and known issues*
- *Limited availability features*

What's new?

Comment field for bypass entries

Added 02-Dec-2019

A new Comment box has been made available on the:

- **Add Proxy Bypass** dialog box accessed from the Connections tab of **Policy Management > Policies**.
- **Add Bypass Destination** dialog box accessed from the Proxy Bypass tab of **Settings > Bypass Setting**.

Add text in the comment box that provides helpful information, such as why the entry was created. The comments then become part of the table provided on the main tab.

New account permission name

Added 02-Dec-2019

The account permission Full Traffic Logging has been renamed to Log Export to better reflect what it permits the user to do and to avoid confusion between the permission and the Full Traffic Logging feature.

Support for SSO with Tunneling

Added 02-Dec-2019

Single sign-on is now supported for use with tunneling connectivity (IPsec Advanced, GRE, and EasyConnect) to the cloud service.

Previous updates

Policy-level custom categories now generally available

Added 23-Oct-2019

After a brief period of limited availability, the policy-level custom categories feature is now generally available for all Web Security Cloud customers.

For more information, see the release notes entry for 27 June 2019: *Policy-level custom categories*.

Forcepoint EasyConnect service

Added 23-Oct-2019

EasyConnect services can be applied to multiple Forcepoint NFGW devices connecting to Web Security Cloud by using the same pre-defined key and password pair.

See Managing Network Devices in the Security Portal Administrator Guide for more information.

Local PoP address ranges for improved content localization: July and August 2019

Added 15-Aug-2019

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

Added 17-Jul-2019	Added 15-Aug-2019
• Algeria • Andorra • Angola • Ethiopia • Ghana • Ivory Coast • Kenya • Liberia • Luxembourg • Malta • Mauritius • Monaco • Morocco • Nigeria • San Marino • Switzerland • Tunisia	• Anguilla • Aruba • Bahamas • Barbados • Bermuda • British Virgin Islands • Cayman Islands • Curacao • Dominican Republic • Greenland • Haiti • Jamaica • Puerto Rico • Saint Kitts and Nevis • Trinidad and Tobago • US Virgin Islands

The new addresses are a local point of presence (local PoP) in these territories, which will result in improved content localization for users. This completes our rollout of local points of presence, bringing the total number of points of presence for Forcepoint's cloud web services to 156 data center locations in 142 countries.

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

IPsec Advanced

Added 8-Jul-2019

A new IPsec Advanced tunneling type is now available when adding edge devices. Based on Forcepoint's NGFW technology, IPsec Advanced represents a new generation of architecture upon which new features will be built. IPsec Advanced introduces support for additional third-party devices such as Check Point.

An IPsec Advanced edge device connects to the cloud service using a pre-shared key that is generated when the device is added.

Note that the option to add an IPsec edge device remains available to customers who had similar devices configured prior to the introduction of IPsec Advanced.

For more information, see the Forcepoint IPsec Advanced Guide.

Policy-level custom categories

Added 27-Jun-2019

Note: *This is a Limited Availability feature. If you are interested in enabling this feature for your account, please contact Technical Support.*

Custom categories can now be added to each policy. Enabled on the **Web > Policy Management > Custom Categories** page, this features provides the option to apply a different set of custom categories to each policy and allows local administrators to configure custom categories as they configure their own policies.

When the feature is enabled, a new Custom Categories tab is provided when a policy is added or edited.

Also, at the bottom of both the **Web > Policy Management > Custom Categories** page and the Custom Categories tab are buttons that allow you to **Download sites** to or **Upload sites** from a CSV file. A downloaded file can be edited and then uploaded for easy maintenance of the list of sites for the category. Contact Technical Support if you are interested in enabling this feature.

Multiple Acceptable Use Policy pages

Added 27-Jun-2019

Note: This is a Limited Availability feature. If you are interested in enabling this feature for your account, please contact Technical Support.

Acceptable Use Policy pages can now be created and assigned to individual policies. Added and edited like any other notification page, custom AUP pages appear under **Acceptable Use Policy** on **Web > Block & Notification Pages**.

Block based on previous Advanced Malware Detection result

Added 27-Jun-2019

The option to **Block access to files that have previously been detected as potentially malicious** has been added to **Web > Settings > File Sandboxing**. When this option is enabled, requests to previously known malicious files are blocked without being sandboxed.

Local PoP address ranges for improved content localization: June 2019

Added 17-Jun-2019

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

- Armenia
- Azerbaijan
- Bahrain
- Bangladesh
- Bhutan
- Egypt
- Georgia
- Iraq
- Jordan
- Kazakhstan
- Kuwait
- Lebanon
- Maldives
- Nepal
- Oman
- Pakistan
- Qatar
- Saudi Arabia
- Sri Lanka
- Yemen

The new addresses are a local point of presence (local PoP) in these territories, which will result in improved content localization for users. Further territories will be added in the coming months. For more information on the Forcepoint local PoP service, see the following article in the Forcepoint Knowledge Base: Improved content localization with local point of presence IP addresses.

Local PoP address ranges for improved content localization: May 2019

Added 14-May-2019

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

- Albania
- Austria
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Greece
- Hungary
- Italy
- Macedonia
- Moldova
- Montenegro
- Romania
- Serbia
- Slovakia
- Slovenia

The new addresses are a local point of presence (local PoP) in these territories, which will result in improved content localization for users. These addresses use the new IP address range announced in January 2019 (see the Forcepoint Tech Alert: Action required: new IP address range for Forcepoint Web Security Cloud and Web Security Hybrid). All customers are advised to update their firewall rules to allow access to the new address range.

Further territories will be added in the coming months. For more information on the Forcepoint local PoP service, see the following article in the Forcepoint Knowledge Base: Improved content localization with local point of presence IP addresses.

New Forcepoint One Endpoint platform

Added 26-Apr-2019

Forcepoint Web Security Cloud now offers the Forcepoint Web Security Proxy Connect and Direct Connect Endpoints as part of a new Forcepoint One Endpoint platform. Forcepoint One Endpoint combines all installed Forcepoint One Endpoint agents, which now includes Forcepoint DLP Endpoint and Forcepoint Web Security Endpoints, under a single system tray icon.

This new Endpoint release, available for download from the **Web > Endpoint** page of the cloud portal, contains the Forcepoint Web Security Endpoint functionality familiar to current customers. No Forcepoint Web Security Endpoint functionality was removed in the transition to Forcepoint One Endpoint.

For additional information, see the Release Notes for Forcepoint One Endpoint, available in the portal on the **Web > Endpoint > General** page., or at the following link: Release Notes for Forcepoint One Endpoint v19.03.

Local PoP address ranges for improved content localization: April 2019

Added 15-Apr-2019

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

- Belarus
- Canada
- Denmark
- Estonia
- Gibraltar
- Iceland
- Ireland
- Jersey
- Latvia
- Lithuania
- Poland
- Portugal
- Russia
- Sweden
- Ukraine

The new addresses are a local point of presence (local PoP) in these territories, which will result in improved content localization for users. These addresses use the new IP address range announced in January 2019 (see the Forcepoint Tech Alert: Action required: new IP address range for Forcepoint Web Security Cloud and Web Security Hybrid). All customers are advised to update their firewall rules to allow access to the new address range.

Further territories will be added in the coming months. For more information on the Forcepoint local PoP service, see the following article in the Forcepoint Knowledge Base: Improved content localization with local point of presence IP addresses.

Enhanced Report Center predefined reports

Added 2-Apr-2019

Predefined endpoint reports have been enhanced to include a new Authentication Method column. The following reports, located in the Advanced folder of Web Security Standard Reports, now include this new column by default.

- Endpoint Authentication Details
- Endpoint User Traffic,
- Installed Endpoint Client Statistics

Cloud Service Status link

Added 2-Apr-2019

A **Cloud Service Status** link has been added to the Forcepoint Security Portal, providing easy access to the Cloud Service Status page. The page provides up-to-date information on the status of the cloud service and steps being taken to mitigate any current issues. It should be the first place to look if you are experiencing any kind of pervasive problem with your service.

Local PoP address ranges for improved content localization: March 2019

Added 11-Mar-2019

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

- Brunei
- Cambodia
- Fiji

- French Polynesia
- Indonesia
- Laos
- Macau
- Malaysia
- Mongolia
- Myanmar
- Papua New Guinea
- Philippines
- South Korea
- Taiwan
- Thailand
- Timor-Leste
- Venezuela
- Vietnam

The new addresses are a local point of presence (local PoP) in these territories, which will result in improved content localization for users. These addresses use the new IP address range announced in January 2019 (see the Forcepoint Tech Alert: Action required: new IP address range for Forcepoint Web Security Cloud and Web Security Hybrid). All customers are advised to update their firewall rules to allow access to the new address range.

Further territories will be added in the coming months. For more information on the Forcepoint local PoP service, see the following article in the Forcepoint Knowledge Base: Improved content localization with local point of presence IP addresses.

Local PoP address ranges for improved content localization: February 2019

Added 25-Feb-2019

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

- Belize
- Bolivia
- Chile
- Costa Rica
- Ecuador
- El Salvador
- French Guiana

- Guatamala
- Guayana
- Honduras
- Panama
- Paraguay
- Peru
- Suriname
- Uruguay

The new addresses are a local point of presence (local PoP) in these territories, which will result in improved content localization for users.

These addresses use the new IP address range announced in January 2019 (see the Forcepoint Tech Alert: Action required: new IP address range for Forcepoint Web Security Cloud and Web Security Hybrid). All customers are advised to update their firewall rules to allow access to the new address range.

Further territories will be added in the coming months. For more information on the Forcepoint local PoP service, see the following article in the Forcepoint Knowledge Base: Improved content localization with local point of presence IP addresses.

Data center launch: Dubai, United Arab Emirates

Added 11-Feb-2019

To support continued expansion in the region, a new Forcepoint data center for Web Security Cloud and Web Security Hybrid has been launched in Dubai, United Arab Emirates. Details for the new data center are as follows:

- ID: DXBA
- City: Dubai
- Country: United Arab Emirates
- IP address range: 85.115.46.0/24

No customer action is required to make use of the new data center. By default, end user web traffic is automatically directed to the nearest cloud data center based on your DNS or egress IP. For more information, see Configuring Web Settings > Configure General Settings in the Forcepoint Web Security Cloud help.

For more information about Forcepoint's global points of presence and IP address ranges, see the article Cloud service data center IP addresses and port numbers in the Forcepoint Knowledge Base.

New IP address range for Web Security Cloud and Web Security Hybrid

Added 11-Feb-2019

To support the continued expansion of the Forcepoint vPoP service, a new IP address range has been added for Web Security Cloud and Web Security Hybrid.

All customers are advised to update their firewall rules to allow access to the new IP range:

- CIDR: 157.167.0.0/16
- Range: 157.167.0.0 - 157.167.255.255
- Subnet: 157.167.0.0
- Mask: 255.255.0.0

Important

Failure to update your firewall rules to allow access to the new address range may result in users being unable to browse websites or download web content via Web Security Cloud and Web Security Hybrid.

For details of all IP addresses and port numbers required for access to Forcepoint Web Security Cloud and Hybrid, see the article Cloud service data center IP addresses and port numbers in the Forcepoint Knowledge Base.

European data center launch for the Cloud App Control module

Added 23-Jan-2019

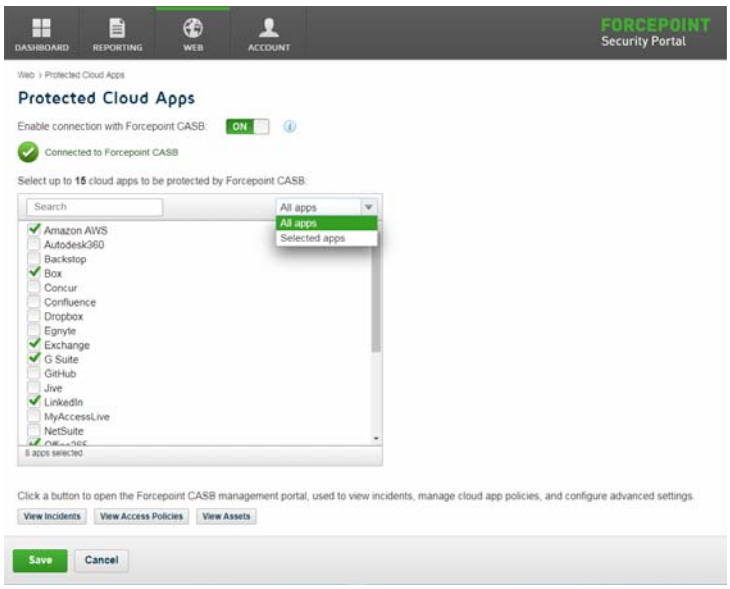
The Cloud App Control module for Web Security Cloud and Web Security Hybrid is now available for customers located in the EMEA region, using data centers located in Europe (Frankfurt).

Cloud App Control was first launched in September 2018, using US-located data centers for CASB log data storage. Customers opting to purchase this feature can now select data centers located in the US or Europe for CASB data storage, providing greater freedom to satisfy privacy and data sovereignty requirements.

Cloud App Control is an optional add-on license 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. You can 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.

With this module enabled, use the Protected Cloud Apps page in the Security Portal 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.

A new attribute in Report Builder, **Cloud App Forwarded**, can be used to report 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 Cloud App Control module and the cloud app usage and risk reporting features in Web Security Cloud 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.

Notes

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

The Cloud App Control data storage location affects only data stored by Forcepoint CASB when using this module. Data storage locations for Web Security Cloud and Hybrid are unchanged. After initial configuration, CASB data cannot be migrated to a different data center location.

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

Local point of presence address ranges for improved content localization: January 2019

Added 21-Jan-2019

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

- Nicaragua
- New Zealand
- Belgium
- Finland

The new addresses are a local point of presence (local PoP) 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 local PoP program, see the following article in the Forcepoint Knowledge Base: Improved content localization with local point of presence IP addresses.

2018 updates

Last updated 7-Jan-2019

For details of new features added, and issues resolved during 2018, please see the Forcepoint Web Security Cloud 2018 Release Notes.

Resolved and known issues

To see the latest list of known and resolved issues for Forcepoint Web Security Cloud, see Resolved and known issues for Forcepoint Web Security Cloud - 2019 in the Forcepoint Knowledge Base.

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

Limited availability features

Last updated 23-Oct-2019

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.
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.