Forcepoint Web Security Cloud: 2020 Release Notes

Forcepoint Web Security Cloud | 2020 Release Notes | Last updated 25-Aug-2020

This document details product updates and new features added to Forcepoint Web Security Cloud during 2020.

What's new?

SIEM Storage using Amazon Web Services

Added 25-Aug-2020

Amazon Simple Storage Service (AWS S3) can now be used to store exported Security Information and Event Management (SIEM) data. Use the new **Account > SIEM Storage** page of the Security Portal to select a storage type and configure AWS S3 buckets.

Forcepoint continues to offer storage facilities for those not wishing to use AWS.

With this new feature, SIEM Integration is now available for all customer accounts.

See Getting started with SIEM integration for more details.

Previous updates

Portal rebrand

Added 27-July-2020

Forcepoint is pleased to announce a rebrand of the Forcepoint Security Portal.

A new sign-in page opens to the Forcepoint Cloud Security Gateway Portal. The functionality for Forcepoint Cloud Web Security and Forcepoint Cloud Email Security has not changed but the look and feel of the user interface has been rebranded with new colors and style.

Navigation to CASB

Added 27-July-2020

Customers who have purchased and enabled the Protected Cloud Apps feature will see a new CASB button in the toolbar. Use this button to navigate to the CASB portal.

Forcepoint Web Security Cloud integrates with Forcepoint CASB to provide granular control over the use of cloud-based applications (cloud apps) in your organization.

Note
The Protected Cloud Apps feature requires an additional license. If you would like further information on accessing this feature, please contact your account manager.

See Configure protected cloud apps and the CASB Integration Guide for more information.

Throughput increase for high bandwidth tunneling

Added 18-Jun-2020

Forcepoint IPsec Advanced and Forcepoint GRE now support up to 5Gbps throughput per tunnel and 1,000,000 concurrent connections.

By default, tunnels are configured for 200Mbps throughput. Submit a request to Forcepoint Technical Support if you require more than the default.

Cloud app blocking

Added 7-May-2020

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

Policy enforcement for cloud applications is now available. Requests to cloud applications can be blocked or allowed using options on a new tab available when configuring a policy (**Web > Policy Management > Policies)**.

Use the **Cloud apps** tab to add cloud apps to a **Block Access** or **Allow Access** list. Policy enforcement is done based on the selections on each list.

Note: customers with a Protected Cloud Apps license cannot select cloud apps already configured as protected on the **Web > Settings > Protected Cloud Apps** page. Those apps are automatically selected on the **Allow Access** list. They appear in search results on both lists, but cannot be selected or removed on either. Attempts by an end user to access these apps are forwarded to Forcepoint CASB for analysis and policy enforcement unless the app is in a blocked category (configured on the Web Categories tab).

Filename encoding with file sandboxing

Added 8-Apr-2020

Filename encoding can be used with file sandboxing so that filenames display properly in Report Center reports.

On **Web > Settings > File Sandboxing**, enable **Filename encoding** and select the appropriate character set from the drop-down provided.

Generic SAML support for single sign-on

Added 10-Mar-2020

The single sign-on feature uses the Security Assertion Markup Language (SAML 2.0) data format to send authentication requests to and receive responses from your identity provider. Previously when configuring single sigh-on, a specific identity provider had to be selected from an available list of providers.

This enhancement provides support for any identity provider that supports the SAML 2.0 standard. A new selection, **SAML 2.0 Compliant Identity Provider**, is an option on the **Web > Settings > Single Sign-on** page of the security portal. The metadata for your identity provider is configured as before/

For customers who have not yet configured single sign-on, the Identity provider entry displays only the new option and cannot be changed. For customers who had

configured single sign-on prior to the introduction of this new feature, the previously selected identity provider is displayed and a drop-down list offers the original provider and SAML 2.0 Compliant Identity Provider.

It is recommended that all customers select SAML 2.0 Compliant Identity Provider.

For additional information, see Single Sign-On for Forcepoint Web Security Cloud and Configure Single Sign-on Settings in Forcepoint Security Portal Help.

Remote browser isolation

Added 28-Jan-2020

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

This release introduces the remote browser isolation feature. When enabled in a policy, this feature allows a user to redirect blocked web requests for selected web categories to a third-party remote browser isolation service. The request is forwarded to the provider, allowing the web page to be viewed outside of the organization's network. Remote browser isolation can be enabled at the account level via **Web > Settings > Remote Browser Isolation**. The Blocked - View in Remote Browser block page can be selected for web categories configured with the Block access action within a policy.

Support is provided for the following remote browser isolation service providers:

- Ericom
- Light Point Security

A valid subscription with the remote browser isolation provider is required.

See Configure Remote Browser Isolation in the Security Portal Help for more details.

SIEM Integration

Added 28-Jan-2020

Administrators using Web Security Cloud Email and Email Security Cloud now have the option to download reporting data for use by a third-party Security Information and Event Management (SIEM) solution.

Once SIEM logging is enabled in the Forcepoint Security Portal, you can schedule a regular process to download the logs and save them to a location of your choice. Logs are retained in the cloud service for 14 days.

If you would like to enable this feature for your account, please contact Forcepoint Technical Support.

See Getting started with SIEM integration on the Forcepoint Support site for details.

2019 updates

Last updated 27-Jan-2020

For details of new features added, and issues resolved during 2019, please see the Forcepoint Web Security Cloud 2019 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 - 2020 in the Forcepoint Knowledge Base.

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

Limited availability features

Last updated 8-Apr-2020

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.
Remote Browser Isolation	Send blocked web requests to a third-party remote browser isolation provider, allowing the web page to be viewed outside of the organization's network. For further information, see Configure Remote Browser Isolation in the Security Portal Help.