Forcepoint

Web Security Cloud

2022

Release Notes

Revision A

Contents

Introduction

This document details product updates and new features added to Forcepoint Web Security Cloud during 2022.

What's new?

Single Sign-On for Cloud Portal Administrators

Cloud Security Portal administrators can now be authenticated using SSO (Single Sign-On). Selection of authentication method is made using a new **Login options** setting on the **Account** > **Contacts** page. Three options are provided.

- **Password Only** - The default setting.
- **SSO or Password** - Both methods can be used, aiming to help with migration to SSO.
- **SSO Only** - Enforces SSO for all administrators. Restricted fall-back to Password method for administrators with Manage Users permission for use in the event of Identity Provider system issues.

To select one of the SSO options you must use the new **Account** > **Administrator Single Sign-On** page to define your preferred identity provider. When using SSO related login options **you must access the portal using the following url** https://admin.forcepoint.net/portal.

Note

If enabling the **SSO Only** option, remember to review your existing Administrator permissions and remove the **Manage User** permission from any Administrator that should not be able to login using their username and password as a fallback option.

Two-factor authentication continues to work with all Password logins. Additional information can be found in online help for Administrator Single Sign-On and Login Options.

Support for auto tunneling of WebSocket traffic

For web applications using WebSockets for communication, a new option now makes it possible to automatically tunnel traffic flow, significantly reducing the need to add SSL decryption bypasses.

Using the cloud portal, Cloud Web administrators can enable/disable WebSocket auto tunneling at the individual policy level allowing for phased roll-out. See **Auto tunneling of WebSocket traffic** in Forcepoint Web security Help for more information.

Support for new F1E Endpoint

The Forcepoint F1E 22.06 version for Windows platforms and associated release notes are now available for download via the Cloud Web Security portal.

Security Enhancements

There is an on-going effort to improve the security of Forcepoint products. To that end, Forcepoint Security Labs Analysts continually assess potential security vulnerabilities which can be introduced by third-party libraries. Security improvements have been made in several areas.

Description	References	Date
Improper handling of input during generation of a web page	Cross-site Scripting (XSS) vulnerability	21-July
OpenJDK updates	CVE-2022-21426, CVE-2022-21434, CVE-2022-21476, CVE-2022-21496, CVE-2022-21443	21-July

Previous updates

Cloud portal Resource Center enhancements

The Resource Center, recently added to the cloud portal, has been enhanced.

- A new **Need help with Policies** button has been added to the **Web** > **Policy Management** > **Policies** portal pages.
  A list of commonly asked themes is provided, from which you can select the one that most closely matches your objective. Then, select whether you want to be guided to the corresponding configuration page or review the associated task-based documentation.

- New search functionality has been added within the Resource Center. Find task-based content across the user interface by entering keywords in the new Search bar. This allows you to get assistance for anything not on the current portal page.
- The Resource Center is now available to Email Security Cloud customers. The overall functionality has been activated for Forcepoint Email Security Cloud customers. However, the new **Need help with Policies** button is specific to Web Security Cloud policies.

New requirements for anti-tampering passwords

When anti-tampering passwords are added for the classic endpoint agents (Proxy Connect and Direct Connect), specific requirements must now be met. Anti-tampering passwords entered on the **General** tab of the **Web** > **Settings** > **Endpoint** portal page must now:

- Be between 14 and 32 characters.
- Contain upper case characters.
- Contain lower case characters.
- Contain numbers.

Other minor maintenance changes were included with this new feature.

New File Sandboxing for Hybrid portal page

A new page has been added to the cloud portal that allows Forcepoint Web Security Hybrid Module customers to configure file sandboxing options rather than use the default settings used by the cloud service. By default, **Submit additional document types** and **Block access to files that have previously been detected as potentially malicious** are both enabled for cloud users.

See File Sandboxing for Hybrid in Forcepoint Web security Help for more information.

Web Category enhancements

Several web categories have been renamed:

- **Non-Traditional Religions** is now known as **Lesser-Known Religions**.
- **Traditional Religions** is now known as **Widely-Known Religions**.
- **Society and Lifestyles** is now known as **Human Interests**. This applies both to the parent and child category.
- **Gay or Lesbian or Bisexual Interest** is now known as **LGBTQIA**.
- **Illegal or Questionable** is now known as **Illegal or Unethical**.

This is a renaming change only. There is no impact on customer policies.

Support for SCIM

The cloud service now provides the option to use System for Cross-domain Identity Management (SCIM), a protocol used to provision user and group identity data from a cloud-based identity provider to the cloud service. Synchronization of user and group data occurs automatically after the identity provider is configured.

Note

Okta and Microsoft Azure Active Directory are the only identity providers currently supported.

Additional information about SCIM and how to configure it in the Security Portal is provided in Cloud Security Gateway Portal Help.

General Availability of End-user Single Sign-on

The end-user single sign-on feature that has previously been made available only by request is now available for use by all Forcepoint Web Security Cloud customers.

When single sign-on is enabled, end users connecting to the cloud proxy are redirected to a third-party identity provider that authenticates user identity, attributes, and roles using your enterprise directory, enabling seamless end-user login.

Content Localization (vPoP) via Tunneling

Edge device management now provides for the option of selecting the two most appropriate points of presence (Data Center of local Pop) for your location. Based on your selection, your end-users receive localized content when visiting sites not in their home country.

Updated Forcepoint End User License Agreement

The latest version of the Forcepoint subscription agreement has been uploaded to the Cloud Security Gateway Portal and can be downloaded from **Account** > **Licenses**.

You can also review it on the Forcepoint Subscription Agreement page of the Forcepoint website.

UPN with Endpoint

The endpoint agents running on client machines now provide a User Principal Name (UPN) as well as an NTLM ID for user identification. The UPN is used by the cloud service to match the user, using the user's provisioned email address, to an appropriate policy. If there is no UPN match, or if the UPN is not available, the NTLM ID is used.

Cloud portal Resource Center

The Cloud Security Gateway portal now provides a Resource Center that offers users various forms of assistance with product configuration and routine tasks.

As you navigate through the portal, click Resource Center in the lower right of each portal page to open a list of context-sensitive selections. Depending on the page in use, one or more of the following is offered:

- Resources Related to This Page.
- Forcepoint Remote Browser Integration.
- Remote Browser Isolation Powered by Ericom.
- Forcepoint Security manager and CASB integration Tasks.
- Reporting Documentation.
- Email Security Cloud Product Documentation.

These lists may include how-to guides, videos, or links to documentation related to the tasks to be performed on the current portal page.

The following appear for every portal page:

- Web Security Cloud Product Documentation.
  This section offers links to product documents and guides.
- Useful Links.
  Links to Forcepoint Technical Support and other training resources are provided.

  New options are added to the Resource Center as they become available.

‘2021 updates

For details of new features added, and issues resolved during 2021, please see the Forcepoint Web Security Cloud 2021 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 - 2022 in the Forcepoint Knowledge Base.

You must log on to the Customer Hub to view the list.

Limited availability features

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.
Full traffic logging	Allows administrators to download full fixed format 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. Forcepoint recommends using the more recent and more flexible SIEM Integration option. Take advantage of Bring your own storage for closer SIEM tool integration or switch between Forcepoint storage and your own See Configuring SEIM storage in Web Security Cloud Help.
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.

Published 09 November 2022