Forcepoint Web Security Cloud

2023

Release Notes

Revision A

Contents

Introduction

This document details product updates and new features added to Forcepoint Web Security Cloud during 2023.

What’s new?

New filter added in File Sandboxing Report

File not supported filter added in the File Sandboxing Report. This filter option detects a file which was not supported by the Advanced Malware Detection module.

End user facing texts aligned with Forcepoint Inclusive Language Standards

All end user texts used in Forcepoint Cloud Security Gateway Portal have been aligned to use words as per Forcepoint Inclusive language guidelines.

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	29-Mar-2023

Previous updates

For details of new features added, and issues resolved during 2022, 2021, 2020, and 2019, see the Forcepoint Web Security Cloud 2022 Release Notes, Forcepoint Web Security Cloud 2021 Release Notes, Forcepoint Web Security Cloud 2020 Release Notes, Forcepoint Web Security Cloud 2019 Release Notes.

Resolved and known issues

There are no resolved and known issues in this release. To see the latest list of resolved and known issues for Forcepoint Web Security Cloud, see Resolved and known issues for Forcepoint Web Security Cloud - 2023 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.

Feature	Description
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 28 April 2023