Forcepoint Email Security Cloud: 2020 Release Notes

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

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

- *What's new?*
  - *SIEM Storage using Amazon Web Services*
- *Previous updates*
  - *Portal rebrand*
  - *SIEM Integration*
  - *2019 updates*
- *Resolved and known issues*
- *Limited availability features*

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.

SIEM Integration

Added 28-Jan-2020

Administrators using Email Security Cloud and Web Security Cloud Email 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 28-Jan-2020

For details of new features added, and issues resolved during 2019, please see the Forcepoint Email Security Cloud 2019 Release Notes.

Resolved and known issues

To see the latest list of known and resolved issues for Forcepoint Cloud Email Protection Solutions, see Resolved and known issues for Forcepoint Email Security Cloud - 2020 in the Forcepoint Knowledge Base.

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

Limited availability features

Last updated 4-Jan-2019

The table below lists Forcepoint Email 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
Attachment wrapping	When suspicious email attachments are identified, administrators can choose to place them in password-protected zip files that are delivered to the recipient. The file is delivered along with a report that includes the message details, a preview of the attachment content, and a link to retrieve the password to the secured file. For further information, see the 2016 Release 6 Notes for Cloud Email Protection Solutions.