Forcepoint Email Security Cloud: 2018 Release Notes

Forcepoint Email Security Cloud | 2018 Release Notes | Last updated 04-Dec-2018

This document details product updates and new features added to Forcepoint Email Security Cloud during 2018.

- *What's new?*
  - *DKIM signing: authenticate outbound messages*
  - *Default landing page change*
  - *Additional cloud delivery IP addresses*
  - *New cloud status monitoring service*
  - *Update to Help > Data Privacy menu*
- *2017 updates*
- *Resolved and known issues*
- *Limited availability features*

What's new?

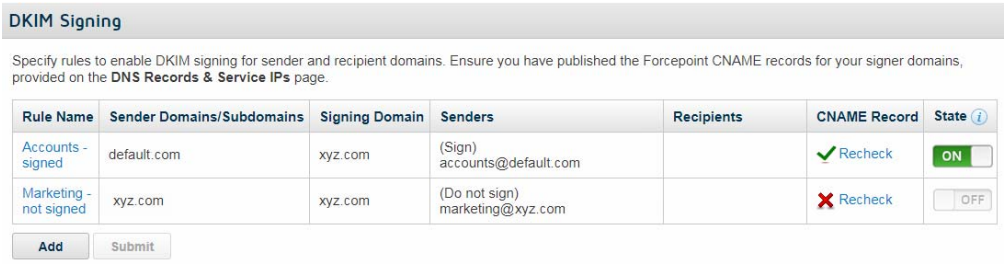
DKIM signing: authenticate outbound messages

Added 04-Dec-2018

Forcepoint is re-releasing the DomainKeys Identified Mail (DKIM) signing feature for Email Security Cloud. The new DKIM signing options are now available to all administrators in the Forcepoint Security Portal.

DKIM is an authentication method designed to protect email recipients from spoofed messages. The DKIM signing feature, available on the **Encryption** tab of your email policies, can be used to digitally sign outbound messages, providing sender address and message integrity validation for message recipients.

When DKIM signing is enabled, the cloud service signs outgoing messages from specified sender domains/subdomains with a private key, adding a *DKIM-Signature* header. Recipient servers can use the information in this header to verify the message signature against Forcepoint's public key, validating that the sender address has not been forged, and the message has not been altered in transit.



DKIM signing rules can be configured on the **Email > Policies > [policy name] > Encryption** tab. Define DKIM signing rules to authenticate sender domains or subdomains, using one of your domains as a signing domain. Granular sender/recipient options are available to include or exclude specific sender addresses, or sender/recipient combinations.

All customers have an account-specific private and public key pair, used to sign and validate messages. Keys are managed by Forcepoint, and are rotated periodically for additional security.

Before enabling a DKIM signing rule, customers must publish Forcepoint-provided DNS CNAME records for each of their signing domains. These CNAME records enable recipient mail servers to look up the customer's Forcepoint public key in order to validate messages. Details of the CNAME records you must publish can be found on the renamed **DNS Records and Service IPs** page (formerly Service IP Addresses). For guidance on configuring CNAME records, see DNS Records and Service IPs in the Forcepoint Email Security Cloud help.

For more information on configuring DKIM signing rules, see Encryption tab > DKIM signing in the Forcepoint Email Security Cloud help.

Note

Customers who have previously enabled DKIM signing via a custom policy rule are advised to contact Forcepoint Technical Support to assist with the process of migrating their DKIM signing rules to use the new interface.

Default landing page change

Added 28-Nov-2018

In order to improve the customer log on experience, the default landing page for Security Portal administrators has been changed to the **Account > Licenses** screen. Note that you can change your default landing page at any time, by clicking the arrow next to your logon account name and selecting **Set Landing Page**.

Encrypted Message Bypass

Added 09-Mar-2018

A new feature in Forcepoint Email Security Cloud allows you to bypass encrypted message filter settings for individual users and groups.

The encrypted message settings, found on the **Antivirus** tab of an email policy, are used to quarantine messages that contain encrypted archive files, and messages encrypted using a standard such as PGP or S/MIME. Such messages pose a security risk because the service cannot scan the content of encrypted messages and

attachments. With these settings enabled, encrypted messages are quarantined in order to prevent potential virus infection.

The new Encrypted Message Bypass feature is used to override these settings for specific users or groups, allowing them to receive encrypted messages from certain addresses or domains, or to send encrypted messages to certain addresses or domains.

The option appears beneath the **Encrypted messages** settings in both the inbound rule and outbound rule sections of the **Antivirus** tab of your policies. Click the **Encrypted Message Bypass** link to enter a set of sender/recipient email addresses, groups, or domains that are permitted to send or receive encrypted messages through the service.

For more information on using this feature, see Antivirus exceptions in the Forcepoint Email Security Cloud help.

For customers with existing encrypted message bypass settings that were manually configured by Technical Support, these settings will be migrated to the new Encrypted Message Bypass feature. Manually configured bypass settings will become visible in the portal, and can be edited using the options described above.

Note

Previously, bypass settings that were manually configured by Technical Support could be set to apply to all new policies by default. In a slight change of behavior, these settings will now apply only to the policies in which they are configured, and will no longer automatically apply to any new policies you create. For more information, contact Technical Support.

Additional cloud delivery IP addresses

Added 12-Feb-2018

As part of a program of continual service improvement, Forcepoint routinely reviews service usage, and upgrades capacity at its cloud data centers as required. As part of this process, additional message delivery IP addresses have been added for Forcepoint Email Security Cloud. The additional delivery IP addresses will help ensure messages are still delivered in the event a Forcepoint relay IP address is placed on a public Real-time Blacklist (RBL).

If your firewall policies allow specific IP addresses for SMTP delivery, you should ensure that all Forcepoint Email Security Cloud IP subnets are permitted. The full list of IP addresses for the cloud email service can be found in the Forcepoint Security Portal by navigating to **Email > Settings > Service IP Addresses**, or in the following knowledge base article: Cloud service data center IP addresses and port numbers.

For outbound connections to the cloud service, configure your mail server to use your customer-specific outbound mail DNS entry, which is listed in the Forcepoint Security Portal under **Email > Settings > Service IP Addresses > MX Record DNS Entries**.

Please also ensure that your SPF record is updated to include our full set of IP ranges. An incorrect or incomplete SPF record may cause message delivery failures. For detail on how to configure your SPF record, refer to the knowledge base article Setting up an SPF record if the outbound email uses Forcepoint Email Security Cloud.

Feature recall notice: DKIM signing

Added 20-Aug-2018

The DKIM signing feature, previously announced on 2 August 2018, has been withdrawn.

An issue with the current implementation of the new outbound DKIM signing feature has been identified. In Forcepoint's ongoing commitment to excellence, we are temporarily removing the DKIM signing feature from the Security Portal. If you have already enabled this feature, please contact Forcepoint Technical Support for assistance. Forcepoint is committed to delivering outbound DKIM signing, and we will alert you when it is available.

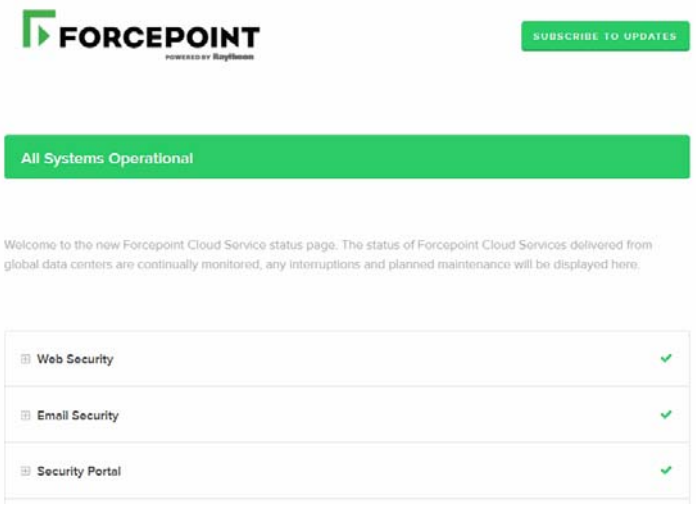
New cloud status monitoring service

Added 19-Jun-2018

Forcepoint has launched a new cloud status monitoring service, displaying the current service status for the global network of Forcepoint data centers for Web Security

Cloud, Email Security Cloud and related services. The page details any interruptions to service and displays any planned maintenance to Forcepoint data centers. You can subscribe to service updates via email, SMS, or RSS feed, to be notified whenever Forcepoint adds or updates an incident.

The new service status page can be accessed at: https://trust.forcepoint.net/



Customers using the previous service status page at https://status.forcepoint.net will be redirected to the new service. However, this redirect will be withdrawn 30 days from the date of this announcement. Please ensure any bookmarks are updated to use the new address.

Update to Help > Data Privacy menu

Added 07-Jun-2018

The **Help > Data Privacy** menu within the Security Portal has been revised to include updated documentation on the management of personal data within the Forcepoint cloud infrastructure. The relevant menu options appear depending on your product licensing, and provide updated information on Forcepoint Web Security Cloud and Forcepoint Email Security Cloud. The updated documents replace the previous Data Privacy FAQ.

The documents are intended to answer customer queries on the use of personal data by the Forcepoint cloud service, and form part of the wider Forcepoint Cloud Trust Program. Details available at: https://www.forcepoint.com/forcepoint-cloud-compliance

To review the updated documents, use the links in the **Help** menu within the Forcepoint Security Portal:

- **Help > Data Privacy > Web Security Cloud**

- **Help > Data Privacy > Email Security Cloud**

2017 updates

Last updated 13-Mar-2018

For details of new features added, and issues resolved during 2017, please see the Forcepoint Email Security Cloud 2018 Release Notes.

Resolved and known issues

Last updated 26-Nov-2018

To see the list of issues resolved for Forcepoint Email Security Cloud during 2018, see Resolved and known issues for Forcepoint Email Security Cloud - 2018 in the Forcepoint Knowledge Base.

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

Limited availability features

Last updated 13-Mar-2018

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.