Forcepoint Email Security Cloud: 2019 Release Notes

Forcepoint Email Security Cloud | 2019 Release Notes | Last updated 23-Oct-2019

This document details product updates and new features added to Forcepoint Email Security Cloud during 2019.

What's new?

Download quarantined email messages in Message Center

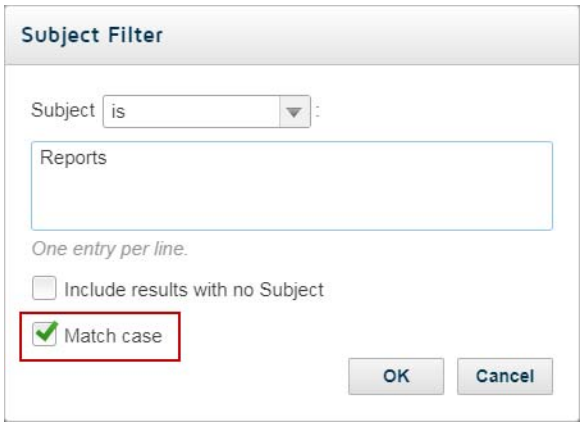
Added 23-Oct-2019

Administrators with the 'View Quarantine' policy permission can now download quarantined messages using the **Download Message** button on the **Email > Message Center > Message Details** screen.

Case-sensitive 'Subject' match in Report Builder

Added 23-Oct-2019

The 'Subject' attribute, available for Email Security reports in the Report Builder, now has an additional option to enable case-sensitive matching when it is applied as a report filter. The filter is no longer case-sensitive by default. Use the **Match case** checkbox to enable case-sensitive matching.



Previous updates

Enhancements to antispam whitelisting and blacklisting controls

Added 08-Jul-2019

This release introduces a number of improvements to the antispam whitelisting and blacklisting controls available on the Antispam tab of a policy, and the Personal Email Subscription report.

IP addresses supported for policy-level whitelists and blacklists

As part of a policy's antispam rules, you can now whitelist or blacklist sender IP addresses, in addition to email addresses and domains. Whitelisting or blacklisting sender IP addresses is useful for blocking persistent spammers who may change email address frequently, or for ensuring that messages from trusted senders are not inadvertently caught by your antispam rules.

To add whitelists or blacklists for your policy, go to the **Antispam** tab. In the White & Blacklists section, enable **Whitelist these addresses** or **Blacklist these addresses**, and click the link to add sender addresses, domains, or IP addresses. For more information, see Defining Email Policies > Antispam tab in the Forcepoint Email Security Cloud help.

For any customers who have previously enabled custom IP address whitelists or blacklists via Forcepoint Technical Support, your custom rules will be unaffected by this change and will still apply. Contact Technical Support for assistance in migrating any custom rules to the interface

Important

Some customers have already added IP addresses to their whitelists and blacklists, instead of domain names, prior to the introduction of this feature. Forcepoint strongly recommends that you review any existing policy-level antispam whitelists and blacklists to ensure that IP address entries are required. Where IP addresses remain in your blacklists and you have an antispam rule that discards messages, there will be no means to recover any messages received from those blacklisted IP addresses.

See the tech alert Forcepoint Email Security Cloud: change to antispam whitelisting and blacklisting behavior for more information.

Simplified configuration for antispam exceptions

Antispam exceptions allow you to set spam options, end user options, and whitelists and blacklists on a per-user, per-domain, or per-group basis. As part of our continual program of service improvement, the configuration for antispam exception whitelists and blacklists has been simplified. The option to 'synchronize' your whitelist and blacklist exceptions with policy-level lists has been replaced with a simplified set of checkboxes that define whether your exception lists are applied in addition to policy-level lists. (Policy-level whitelists and blacklists are always applied.)

This change has been made to make the option more intuitive, and does not affect exception behavior. The change does not alter any existing antispam exception rules.

To configure antispam exceptions, go to **Email > Policies > [policy name] > Antispam tab** and click **Antispam Exceptions**.

For more information about using the antispam exceptions feature, see Defining Email Policies > Antispam tab in the Forcepoint Email Security Cloud help.

Change to default behavior for Personal Email Subscription report whitelisting and blacklisting

In the Personal Email Subscription report available to end users, the default behavior when clicking Whitelist or Blacklist for a suspicious email has been changed. Previously, this option would whitelist or blacklist the sender domain by default (users could select the email address instead by selecting it from a drop-down menu). To make this option more intuitive, the default behavior has been reversed. The default option is to whitelist or blacklist the sender email address, with the option to select the sender domain available via the drop-down menu.

Cloud Service Status link

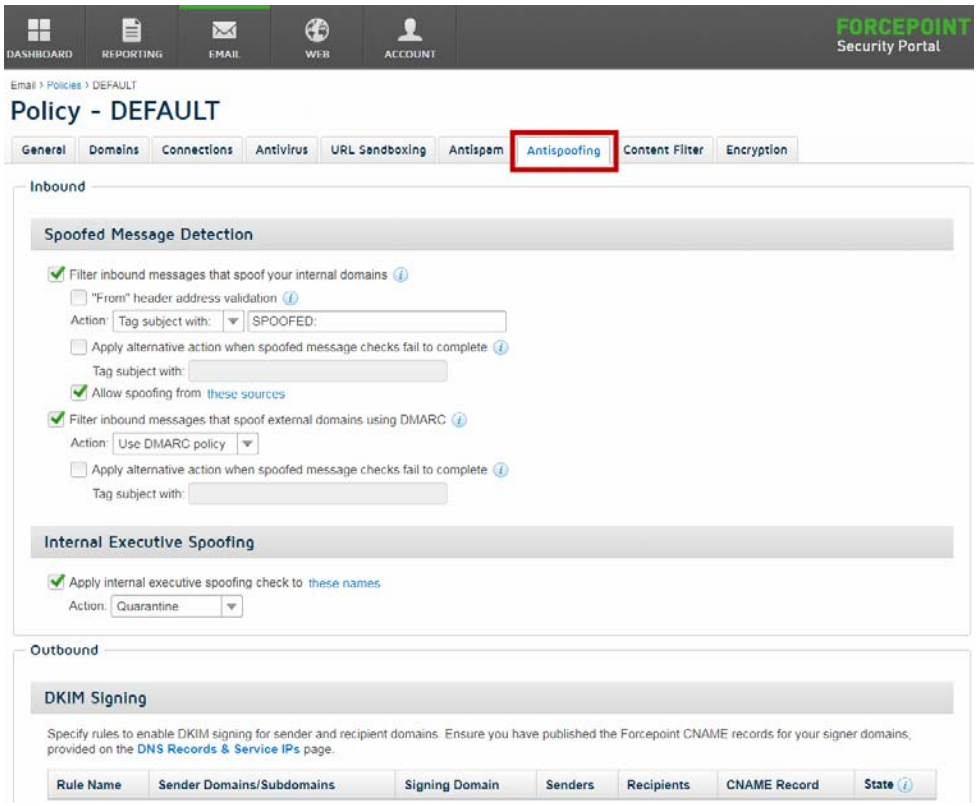
Added 02-Apr-2019

A **Cloud Service Status** link has been added to the Forcepoint Security Portal, providing easy access to the Cloud Service Status page. The page provides up-to-date information on the status of the cloud service and steps being taken to mitigate any current issues. It should be the first place to look if you are experiencing any kind of pervasive problem with your service.

Antispoofing enhancements

Added 28-Jan-2019

The antispoofing controls in Forcepoint Email Security Cloud have been enhanced and moved to a new, dedicated **Antispoofing** policy tab.



Inbound spoofing controls

The existing inbound antispoofing controls (Spoofed Message Detection and Internal Executive Spoofing) were previously located on the **Antispam** policy tab. These controls are designed to protect your users against receiving messages from forged email addresses, and spear phishing messages which purport to be from named individuals within your organization.

Outbound spoofing controls

The Antispoofing tab also includes Forcepoint's new outbound spoofing controls:

- DKIM Signing
- Antispoofing Checks

DKIM Signing

The DKIM signing feature, released in December 2018, allows you to sign your outbound messages to better protect recipients against messages that attempt to spoof your domains. 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.

The DKIM signing feature was previously found on the **Encryption** tab.

For more information about the DKIM signing feature, see DKIM signing: authenticate outbound messages in the Forcepoint Email Security Cloud 2018 Release Notes.

Antispoofing Checks

The new tab introduces a new outbound antispoofing check, designed to better protect message recipients from receiving messages that attempt to spoof your domains. The new **strict outbound message authenticity check** performs additional tests on outbound messages processed by the policy. With the option enabled, the service checks that outbound messages either originate from an IP address defined in the policy, or have a valid DKIM signature from your third-party email provider.

Messages that fail the test are quarantined, providing additional protection to prevent your domains being spoofed by a third party.

This check is particularly useful for customers who use hosted service providers such as Microsoft Office 365 or Google Apps, to help ensure that your domains can not be spoofed by other users of the service.

Note

To use this check, users of hosted email service providers must ensure that a DKIM signature is applied by their provider. If you require further assistance, please contact Technical Support.

For more information about the antispoofing features in Forcepoint Email Security Cloud, see Defining Email Policies > Antispoofing tab in the Email Security Cloud help.

2018 updates

Last updated 4-Jan-2019

For details of new features added, and issues resolved during 2018, please see the Forcepoint Email Security Cloud 2018 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 - 2019 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.