Forcepoint Email Security Cloud: 2017 Release Notes

Forcepoint Email Security Cloud | 2017 Release Notes | Last updated 14-Dec-2017

This document details product updates and new features added to Forcepoint Email Security Cloud during 2017.

What’s new?

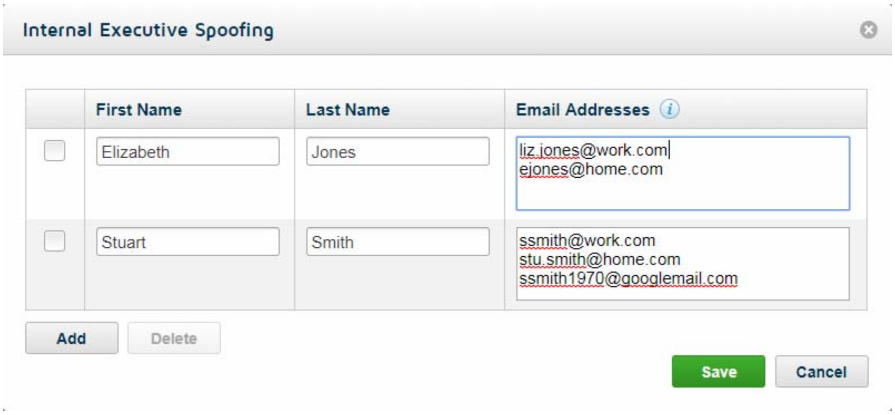
Internal Executive Spoofing: protect against targeted email attacks

Added 14-Dec-2017

The new Internal Executive Spoofing feature available in Forcepoint Email Security Cloud provides protection against targeted email attacks that impersonate named individuals within your organization.

Targeted email attacks may be crafted to impersonate senior executives within your business, sometimes requesting that the recipient urgently sends money or information, or compromised with phishing scams or other types of fraudulent content. These types of attack may come from addresses that look legitimate, for example using a variant of the executive’s name at a free email domain. The email address used may not be spoofed, meaning that the message passes other spoofing checks. However, fraudsters attempt to take advantage of the human element, relying on social engineering and using the perceived authority of the sender to trick users into complying.

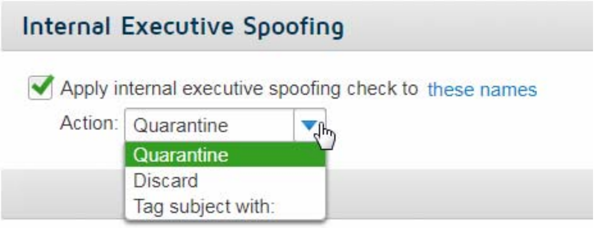
Internal Executive Spoofing allows you to protect the names of a set of users within your organization, by filtering messages that attempt to impersonate them. Enter a set of names to protect (as first name/last name pairs), along with all of the email addresses that the individual uses. These addresses should include work as well as personal addresses.



	First Name	Last Name	Email Addresses
☐	Elizabeth	Jones	liz.jones@work.com ejones@home.com
☐	Stuart	Smith	ssmith@work.com stu.smith@home.com ssmith1970@googlemail.com

If an incoming email appears to be from one of the named users you have added, the feature checks that the message comes from one of the approved addresses for that individual. The email display name is checked for various combinations of the individual’s first and last names (for example “Elizabeth Jones”, as well as “Jones, Elizabeth”). Messages that appear to come from a named executive but originate from an address you have not added will be treated as spoofed, and the action you define will be taken (quarantine, discard, or tag).

If the email does come from an address you have added for the individual, the usual spoofing checks are performed against the email address to check that the message is genuinely from that sender.



Internal Executive Spoofing

☑ Apply internal executive spoofing check to these names

Action: Quarantine

Messages detected as impersonating named individuals will be logged in reports as “Spoofed-Targeted” under the Filtering Reason attribute. Messages quarantined for this reason are excluded from end users’ Personal Email Subscription reports, in order to prevent users from inadvertently acting upon a targeted phishing message.

Internal Executive Spoofing is part of a set of new email protection features available to users of Forcepoint Email Security Cloud, helping you to respond to evolving security threats, and protecting the human point.

The Internal Executive Spoofing option can be found on the Antispam tab of your email policies. For more information on using the Internal Executive Spoofing feature, please see Defining Email Policies > Antispam tab in the Forcepoint Email Security Cloud help.

Allowed spoofing addresses

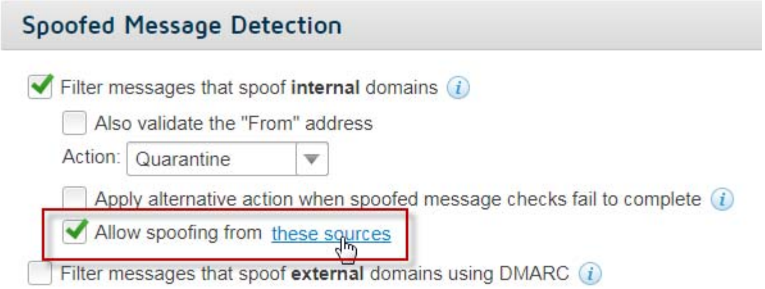
Added 30-Nov-2017

Forcepoint Email Security Cloud allows you to filter incoming messages that spoof your organization’s domains, protecting your users from receiving messages from external senders that appear to come from your own addresses. Spoofing an organization’s internal addresses is a common tactic in spear phishing campaigns.

This feature has now been enhanced with a new option that allows you to bypass this spoofing filter for trusted senders. The ability to whitelist the domains or IP addresses of trusted senders is useful for organizations that use third-party providers to send messages to their users from legitimately spoofed internal email addresses.

For example, if a third-party provider is allowed to send messages to your users from a spoofed internal address, you can add that provider’s domain as a trusted sender. This means that you do not have to edit your SPF record to allow the sender domain, reducing the complexity of SPF record management for domains that send messages on your behalf.

The new option can be found on the **Antispam** tab of your email policies, when the **Filter messages that spoof internal domains** setting is applied.



Spoofed Message Detection

☑ Filter messages that spoof **internal** domains

□ Also validate the "From" address

Action: Quarantine

□ Apply alternative action when spoofed message checks fail to complete

☑ Allow spoofing from these sources

□ Filter messages that spoof **external** domains using DMARC

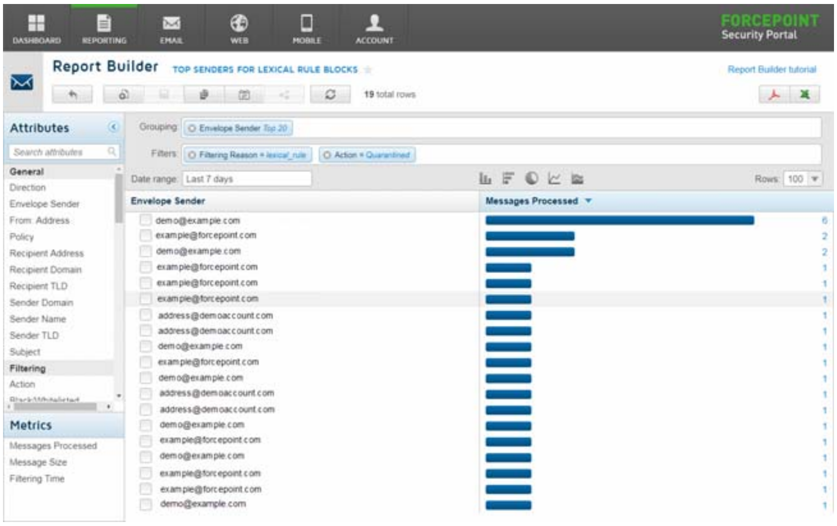
Select **Allow spoofing from these sources** to apply a whitelist of allowed domains or IP addresses. Messages originating from the domains or IP addresses you configure are allowed to spoof addresses from the domains that you own (set on the **Domains** tab in your policy).

For more information on using this feature, see [Defining Email Policies > Antispam tab]() in the Forcepoint Email Security Cloud help.

Report Center package now generally available

Added 30-Nov-2017

The Report Center package, previously a limited availability feature, is now enabled for all Forcepoint Email Security Cloud customers. The Report Center provides a Report Catalog that includes a set of predefined reports, and a Report Builder tool that allows you to create detailed, customized reports.



Report Builder TOP SENDERS FOR LEXICAL RULE BLOCKS

19 total rows

Grouping: Envelope Sender Top 20

Filters: Filtering Reason = lexical_rule; Action = Quarantined

Date range: Last 7 days

Rows: 100

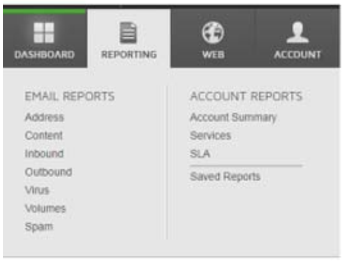
Envelope Sender	Messages Processed
demo@example.com	6
example@forcepoint.com	2
demo@example.com	2
example@forcepoint.com	1
example@forcepoint.com	1
example@forcepoint.com	1
address@demoaccount.com	1
address@demoaccount.com	1
demo@example.com	1
example@forcepoint.com	1
demo@example.com	1
address@demoaccount.com	1
address@demoaccount.com	1
demo@example.com	1
example@forcepoint.com	1
demo@example.com	1
example@forcepoint.com	1
example@forcepoint.com	1
demo@example.com	1

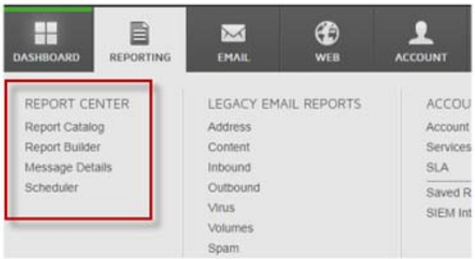
The Report Catalog consists of a number of pre-built reports covering common reporting scenarios for email usage, security, and spam. Reports in the Report Catalog can be customized and saved using the Report Builder.

The Report Builder tool lets you create flexible, multi-level reports, dashboards and trend charts, allowing you to analyze information from different perspectives and gain insight into your organization's email messaging. If a high-level summary shows areas of potential concern, you can drill down to find more detail.

Predefined or custom reports can also be sent to an email distribution list automatically, using the **Scheduler** option.

Report Center features are available in a new area of the **Reporting** menu. Existing email reports remain available, under the menu item **Legacy Email Reports**.





For more information on using the Report Center, see Email Reporting Tools > Email Report Center in the Forcepoint Email Security Cloud Help.

Withdrawal of support for 3DES and RC4 ciphers

Added 17-Oct-2017

In line with industry best practices, Forcepoint continually reviews and updates the security strength of encrypted email connections.

As part of this process, Forcepoint has now disabled the use of 3DES and RC4 ciphers in SMTP email connections that are made to and from the Forcepoint cloud email relays. Forcepoint has previously taken steps to avoid the use of these less-secure protocols and ciphers for SMTP connections.

This change also affects hybrid email customers who use the cloud email relays to accept inbound messages.

Please see the Tech Alert for this update here:

- Update to Forcepoint Email Security Cloud - 3DES and RC4 ciphers, 01-Sep-2017.

Additional cloud delivery IP addresses

Added 10-Oct-2017

As part of a program of continual service improvement, Forcepoint routinely reviews service usage and upgrades capacity at our cloud data centers. 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 only allow specific IP addresses for SMTP delivery, you should ensure that all Forcepoint Email Security Cloud IP subnets are permitted. Your current SPF record will continue to function, provided it is configured as per the instructions in the following Knowledge Base article: How do I set up an SPF record if my outbound email uses Forcepoint Email Security Cloud?

Email service IP addresses can be found in the Forcepoint Security Portal under **Email** > **Settings** > **Service IP Addresses**. IP addresses for Forcepoint cloud services are also listed in the following Knowledge Base article: Cloud service data center IP addresses and port numbers.

Please see the Tech Alert for this update here:

- Update to Forcepoint Email Security Cloud delivery IP addresses, 01-Sep 2017.

Terms of use for administrators

Added 29-Jun-2017

The new **Terms of use** option allows you to display a page that requires administrators to agree to your company's terms of use before logging on to the Forcepoint Security Portal. The setting is configured on the **Account** > **Contacts** page under Administrator Account Management.

When enabled, this setting applies to all portal administrators. The next time portal administrators log on, they will be prompted to either accept your terms of use, or log off.

✓ **Note**

By default, a generic "Agree to Terms of Use" block page is provided. Before enabling this feature, ensure you customize this page to include details of (or a link to) your company's terms of use.

See the Forcepoint Security Portal Help for details of how to customize block pages.

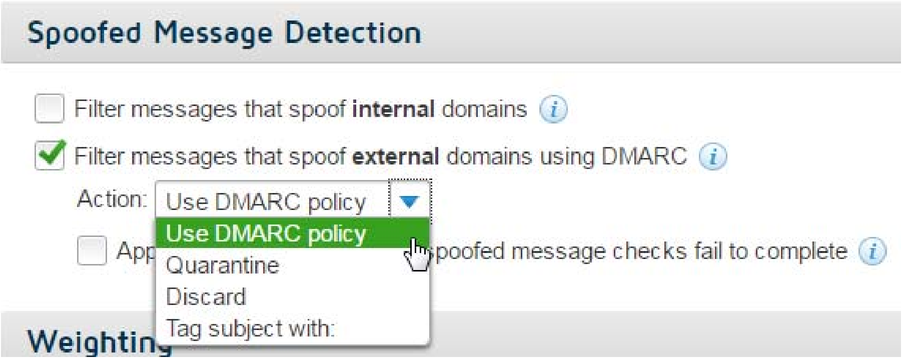
Enhanced email spoofing detection with DMARC

Added 01-Jun-2017

Forcepoint Email Security Cloud now offers Domain-based Message Authentication, Reporting and Conformance (DMARC) validation for incoming email messages from external domains.

The DMARC email validation system detects messages from external sources with forged sender addresses, providing increased protection against phishing and spam. DMARC is built on Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) validation, and allows the genuine owner of a domain to publish a policy that defines how the receiver should deal with spoofed messages.

When this feature is enabled, DMARC validation can be configured on the **Antispam** tab of your email policy. The **Filter messages that spoof external domains** option detects spoofed incoming messages that appear to be sent from legitimate external domains, but which fail DMARC validation.



Spoofed Message Detection

☐ Filter messages that spoof **internal** domains

☑ Filter messages that spoof **external** domains using DMARC

Action: Use DMARC policy

☐ App spoofed message checks fail to complete

Weighting

Administrators can select the action to take when spoofed messages are detected, including applying the domain owner's policy, quarantining, discarding, or tagging the message subject line. An alternative action can be applied if the validation check fails to complete.

Messages that fail DMARC validation will appear in reporting with "Spoofed-External" as the Filtering Reason.

For more information on using DMARC validation, see the Forcepoint Email Security Cloud Help.

ISO 27018 certification for Forcepoint Cloud Protection Solutions

Added 01-Jun-2017

Forcepoint recently added ISO 27018 certification to its Cloud Trust Program, to provide a robust system of controls for privacy protection of personal data. This enhances the compliance of the cloud service with the General Data Protection Regulation (GDPR) that comes into effect in May 2018.

Forcepoint runs a dedicated Cloud Trust Program that encompasses ISO 27001, ISO 27018, and CSA STAR certifications with Service Organization Control (SOC) attestations. All Forcepoint cloud service certifications can be viewed in the Security Portal, under **Help** > **Privacy & Security**.

Product renaming

Added 20-Apr-2017

As part of a rebranding program for the Forcepoint product set, TRITON AP-EMAIL Cloud is now called Forcepoint Email Security Cloud.

You will see the new product name and logos within the cloud portal, which is now called the Forcepoint Security Portal (formerly the Cloud TRITON Manager).

The following Forcepoint Email Security Cloud product modules have also been changed:

- Forcepoint Advanced Malware Detection for Email (formerly Threat Protection Cloud - Email, or Email Sandbox Module)
- Forcepoint Email Security - Encryption Module (formerly Email Encryption Module)
- Forcepoint Email Security - Image Analysis Module (formerly Email Image Analysis Module)

The new branding for all Forcepoint products can be seen at the Forcepoint website.

Phishing Education feature now generally available

Added 20-Apr-2017

The Phishing Education feature is now available to all subscribers of Forcepoint Email Security Cloud (formerly TRITON AP-EMAIL Cloud).

Raising awareness among an organization’s end users about the characteristics of phishing email is an important corporate goal. The Phishing Education feature provides security to the enterprise as well as giving information to users on how to avoid becoming a victim of phishing, delivered in a way that ensures users will take notice.

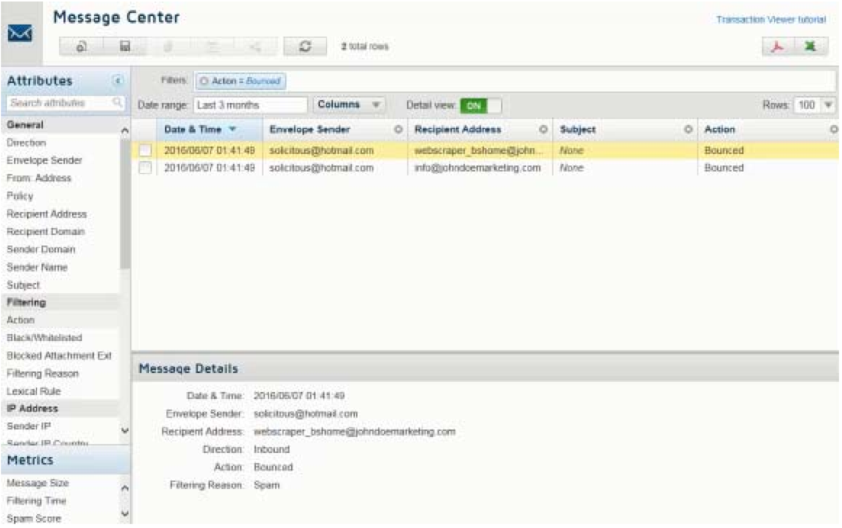
When Phishing Education is enabled and configured, users who click a phishing link in an email are shown an administrator-customizable page that informs the user that the email was a phishing attack, and provides tips on how to avoid such attacks in future.

Phishing settings are configured on the Antivirus tab of your email policy. You can customize the page shown to users via **Email** > **Policy Management** > **Block & Notification Pages**.

Report Center package now available

Added 20-Apr-2017

The Report Center package, previously a limited availability feature, is now enabled by default for new accounts. If you would like to enable the advanced reporting package for your account, please contact Forcepoint Technical Support.



Filters: Action = Bounced

Date range: Last 3 months

Detail view: ON

Rows: 100

	Date & Time	Envelope Sender	Recipient Address	Subject	Action
□	2016/06/07 01:41:49	solicitous@hotmail.com	webscraper_bshome@john...	None	Bounced
□	2016/06/07 01:41:49	solicitous@hotmail.com	info@johndoemarketing.com	None	Bounced

Message Details

Date & Time: 2016/06/07 01:41:49
Envelope Sender: solicitous@hotmail.com
Recipient Address: webscraper_bshome@johndoemarketing.com
Direction: Inbound
Action: Bounced
Filtering Reason: Spam

The Report Center provides a Report Catalog with a number of predefined reports covering common scenarios, and a Report Builder tool that can be used to create flexible, multi-level reports that allow you to analyze information from different perspectives and gain insight into your organization's email message trends. If a high-level summary shows areas of potential concern, you can drill down to find more detail.

For details of the Email Report Center, see the Forcepoint Email Security Cloud Help.

Note

Updated 30-Nov-2017: The Report Center package is now generally available for all Forcepoint Email Security Cloud customers. See *Report Center package now generally available*, page 4

Two-factor authentication for administrators

Added 02-Mar-2017

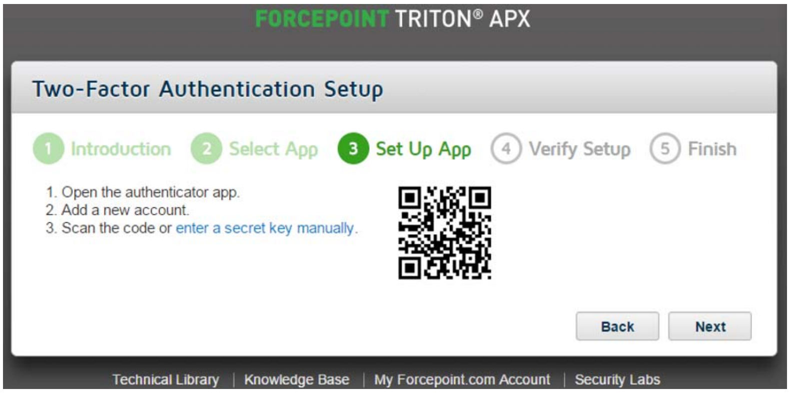
Two-factor authentication can now be enabled for portal users, providing an additional level of security for access to the cloud portal. When this feature is enabled, all administrators are required to enter both their password and a code generated by an authenticator app to access the portal.

✓ **Note**

Compatible authenticator apps are available for Android, iOS, Blackberry, and Windows Phone. Desktop and browser-based apps are also available for Microsoft Windows, Mac OS, and Linux. Forcepoint validates this feature with the Microsoft Authenticator app, but alternative apps that use the Time-based One-time Password Algorithm (TOTP) protocol, such as Google Authenticator, are also supported.

Administrators can enable or disable two-factor authentication for portal administrators using the **Account** > **Contacts** page.

When users log on with two-factor authentication for the first time, a setup wizard guides them through the configuration process.


FORCEPOINT TRITON® APX
Two-Factor Authentication Setup
1 Introduction
2 Select App
3 Set Up App
4 Verify Setup
5 Finish
Back
Next
Technical Library | Knowledge Base | My Forcepoint.com Account | Security Labs

1. Open the authenticator app.
2. Add a new account.
3. Scan the code or enter a secret key manually.

For portal users who are unable to use their authenticator app, two-factor authentication can be reset on the **User** page. This requires portal users to repeat the authenticator app setup process.

The process of enabling and using two-factor authentication is detailed in the [Forcepoint Security Portal Help](#).

Resolved and known issues

Last updated 14-Dec-2017

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 - 2017 in the Forcepoint Knowledge Base.

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

Limited availability features

Last updated 14-Dec-2017

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.