Forcepoint

Email Security Cloud

End User Guide

Revision A

Contents

Introduction

Welcome to this User's Guide. Your organization has subscribed to the Forcepoint Email Security Cloud service.

This guide describes how the service works and explains how you can take control of your email and reduce the volume of unwanted junk mail, commonly known as spam.

What is Forcepoint Email Security Cloud?

Forcepoint Email Security Cloud is a service that filters all your inbound and outbound Internet email (that is, email that is outside of your company's internal domain). It scans inbound email before it reaches your network and filters out unwanted messages based on a policy defined by your email administrator.

Typically the cloud service is used to filter out email containing viruses and spam, although it is also able to block other types of content, such as messages with movie or executable file attachments and messages containing obscene or other inappropriate words or phrases.

How will it affect me?

Generally, you won't be aware that the Forcepoint Email Security Cloud service is being used. Your email is delivered normally, but you might notice a reduction in the volume of junk mail you receive.

The cloud service may communicate with you in one of two ways:

1) **Notification email**: Occasionally you may be notified by email that a message has been blocked. This normally occurs only when someone has tried to send you an email message containing a virus or some other type of content that is not permitted. Inside the notification, you may see a link that you can click for more information about the blocked message.

2) **Personal email report**: The cloud service can send you a message report, called the Personal Email Subscription report, at regular intervals. This provides information about all email that you received and sent and allows you to take action on messages that were considered spam. See *How do I know which messages have been blocked?* for more details.

Related concepts

How do I know which messages have been blocked? on page 4

Will the service affect those sending email to me?

No: the service does not notify senders when their inbound mail contains a virus and has been blocked.

How does the service handle spam?

All messages passing through Forcepoint Email Security Cloud are analyzed and given a spam score. The higher the score, the more likely the message is spam. Your company has set a spam threshold and all messages scoring over this threshold are classified as spam.

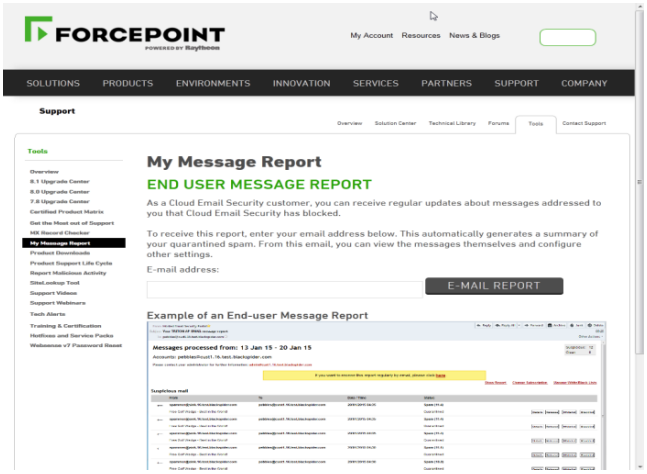
Once classified as spam, messages are typically quarantined and stored for 30 days. Messages with high spam scores may be discarded under the control of the administrator. You are **NOT** notified when you receive spam. In some organizations, 98 percent of inbound email traffic is spam. You would not want to be notified of every spam message you receive.

It is possible for the cloud service to tag spam email; this means the spam is delivered as normal, but the word "SPAM:" is added to its subject line. This feature is most often configured by an email administrator for use during an initial period of evaluation, or to flag email whose spam score is borderline.

How do I know which messages have been blocked?

Forcepoint Email Security Cloud can provide a message report detailing all messages processed for your email address, including those that were blocked.

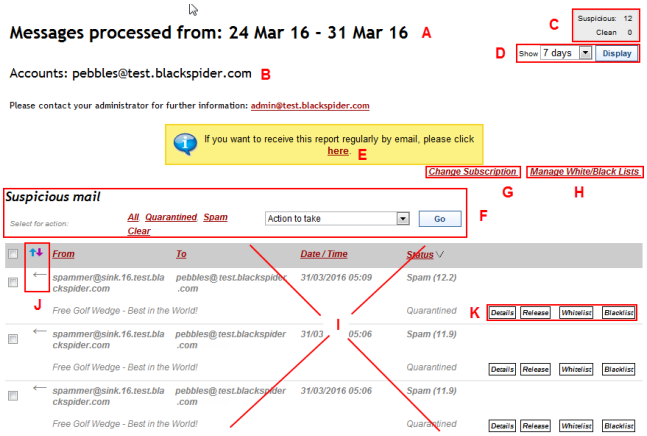
Your administrator may subscribe you to the report – if this happens, you will receive a report via email. The report contains a link that you can click to schedule delivery of the report on a regular basis. Otherwise, to obtain the report, click here.



Enter your email address into the space provided, and the report is emailed to you. This normally takes no longer than a few minutes depending on the amount of data.

What is included on the message report?

The message report contains a variety of useful information. The example below shows the online version of the report, which you can access by clicking **Show Reports** in the email version.



	Contents
A	The date range for which the report was processed
B	Your email address
C	The number of suspicious and clean messages that were processed for you during the period
D	An option to change the number of days shown in the report
E	A link to receive this report by email on a regular basis
F	The ability to select all quarantined and/or spam message and take actions on them, such as whitelist or release
G	A link to change your report subscription
H	A link to manage your personal whitelist and blacklist
I	A list of your email arranged in the following order (list depends on user and account configuration): ■ Suspicious messages you received or sent ■ Clean messages you received or sent If you are looking at the online version of your report, you can change the order of the messages by clicking a column heading link. For example, you can sort by the **From** or **To** column, the **Date/Time** column, or the **Status** column.
J	An indication of whether a message has been received, or sent.
K	The actions you can take action on a message. (Select a message by clicking in the check box on the left.) Options include: ■ **Details** - Access details about the message ■ **Release** - Release the message from quarantine. (This is not possible for all messages, such as those containing known viruses.) ■ **Whitelist** - Add this email address or domain to your personal whitelist. This tells the cloud service to always allow messages from this sender or domain, unless they contain a virus or malware. ■ **Blacklist** - Add this email address or domain to your personal blacklist. This tells the cloud service to never allow messages from this sender or domain.

Information included on the message summary section:

- An indication of whether the message was inbound or outbound
- The message sender
- The message recipient
- The time and date that the cloud service logged the email

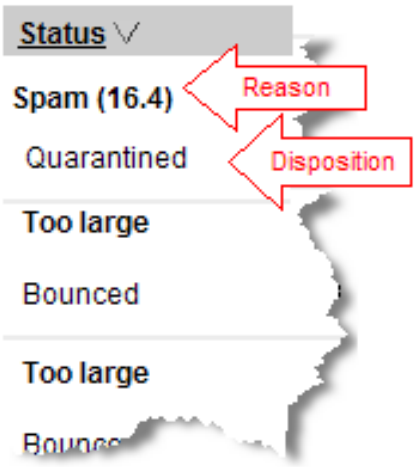
- The status of the email. This includes a reason and a disposition. (See *What does the Status mean?* for more information.)
- The subject line of the message

Related concepts
What does the Status mean? on page 6

What does the Status mean?

The **Status** column of the personal email report includes a reason (such as Spam) and a disposition (such as Quarantined).

If a message was not delivered, the first (bold) word in this column indicates the reason why. The word below it indicates the action taken on the message, also known as the disposition of the message.



Quarantined spam messages include the spam score. The higher the score, the more likely it is that the message is spam.

The following table explains the possible reasons you may see:

Reason	Explanation
Access control	The message was blocked because of an access control rule set up by your administrator.
Access rule	The message was blocked because of an access control rule set up by your administrator.
Blocked attachment	The message contains an attachment whose type has been blocked by your policy.
Blocked executable	The message contains an executable attachment and executables have been blocked by your policy.
Blacklisted	The email address or domain of this sender is in your personal blacklist or your policy's blacklist.

Reason	Explanation
Clean	The message does not violate any of your policy settings.
Dangerous content	The message contains content that may be dangerous to your machine. This reason can have many sub-reasons: ■ **Double extension file** - An attachment filename has a double file extension that can be used to mask the real function of the file. ■ **Empty archive** - The message contains an empty archive file. ■ **Executable in service message** - The message is a delivery status message that contains executable content. ■ **openrelay(block)** - The message sender should not have been able to send mail via the sending mail server. ■ **Spoofed virus** - The message contains a virus. The message sender appears to have been forged. ■ **Suspicious attachments** - ThreatSeeker found a suspicious attachment $1 in the message. ■ **Zero byte archive** - The message contains an empty archive attachment. This is probably because a virus has been removed. ■ **Zero byte executable** - The message contains an empty executable attachment. This is probably because a virus has been removed.
Extension masked	The message contains an attachment whose extension has been renamed as configured by your policy. For example, an executable extension may have been named “.ex_” to prevent it from being executed.

Reason	Explanation
Format	The Format reason can have many sub-reasons: ■ **Archive extraction failed** - The service was unable to unpack an archive file and could not scan it. ■ **Attachment missing filename** - An attachment in the mail does not have a specified filename. This can be used to exploit some mail clients. ■ **Email not multipart** - The structure of the message is potentially malicious and can be used to attack some mail clients. ■ **Encrypted** - The message or an attachment is encrypted. ■ **Expansion level exceeded** - The mail contained too many levels of nested archives. Unable to scan the archive contents. ■ **Filename blocked** - An attachment name matched a service configured rule. ■ **Filename too long** - The subject contains a filename that is too long. This can be used to attack some mail clients. ■ **Header blocked** - The message header breaches a configured policy rule. ■ **Header contains large data blocks** - The message header contains a block of data longer than the permitted maximum. ■ **Header length exceeds** - The message header is longer than the permitted maximum. This can be used to attack some mail clients. ■ **Message subject blocked** - The message subject matches a service configured rule. ■ **MIME type blocked** - The message contains an attachment that is blocked by the configured policy. ■ **Partial message body** - The message cannot be scanned because it is missing parts of an attachment and has been blocked. ■ **Password protected archive** - The message contains a password protected archive file. This cannot be scanned therefore was blocked. ■ **Potential outlook exploit** - The date or subject in the message are too long. These can be used to attack mail clients like old versions of MS Outlook. ■ **Signed** - The message has been cryptographically signed. This message cannot be scanned and was quarantined. ■ **Suspicious body characters** - The message body contains binary information where it was not expected. This might be malicious.

Reason	Explanation
	■ **Suspicious header characters** - The message header contains binary information where it was not expected. This might be malicious. ■ **Unroutable recipient** - The email policy blocks delivery of mail to this subdomain. ■ **Unroutable sender** - The email policy blocks delivery of mail from users in this subdomain.
Lexical rule	The message contains content that breaks a lexical rule set up in your policy.
Macro	The message contains a suspected macro virus.
Message loop	The service detected a message delivery loop.
Operational	The message was blocked for operational reasons.
Potential virus	The message contains a potential virus that could be harmful to your machine.
Spam (n)	The message has been classified as spam by your email policy. Quarantined spam messages include a spam score. The higher the score, the more likely it is that the message is spam.
System	The message failed to be processed for system reasons.
Tempfailed	The mail server is down and temporarily could not receive mail.
Too large	This message is larger than the maximum size specified in the policy.
Unknown	The message encountered an unknown problem.
Virus	The message contains a known virus that is harmful to your machine.
Whitelisted	The email address or domain of this sender is in your personal whitelist or your policy's whitelist.

The following table lists possible dispositions:

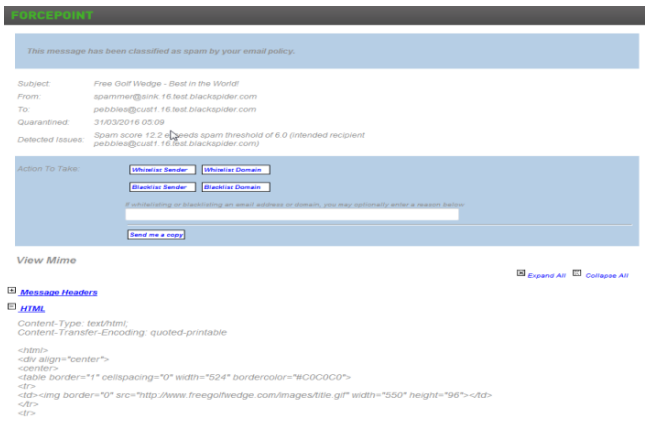
Disposition	Explanation
Accept	The message was accepted and delivered.
Bcc	A blind copy of the message was sent; that is, the recipient's name has been obscured.
Bcc, subject tagged	A blind copy of the message was sent with the subject line tagged.
Bounced	The message was returned to the sender, undeliverable.
Bypass	The message bypassed the email security system.
Discarded	The message was deleted from the archive.

Disposition	Explanation
Quarantined	The message is being held in the email quarantine.
Spam forwarded	This spam message was forwarded to a recipient.
Subject tagged	The message subject was tagged.
Temp failed	The mail server is down and temporarily could not receive mail.
Unknown	The resulting action is not known.
Void	No action was taken.

If you require a message that has been blocked or quarantined because of your policy settings, please see your email administrator.

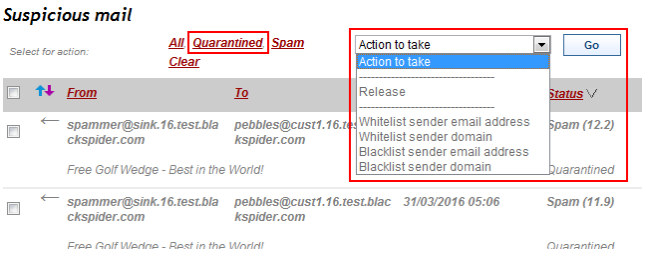
How do I access my email?

On your message report, you can see at a glance all the messages that have been sent to you from outside of your network, including messages that have been classified as spam and those that have been quarantined for other reasons. If you want to view the content of a message, select the message (by clicking in the check box on the left), then click **Details**. The details of a message may look something like this:



In this example, a message was quarantined, because it was classified as spam by the policy. The administrator is allowing you to add the sender or sending domain to a whitelist or blacklist. He is also allowing you to send a copy of the message to yourself. If these features were not enabled by the administrator, the buttons would not be on the screen. In some cases, you may be allowed to release a message as well. If the email was quarantined because it contains a virus or offensive words, however, you would not be able to release a copy regardless of how the administrator has configured the service.

To take an action on all your quarantined messages at once, click **Quarantined** under **Select for action** on your message report, then choose and action to take. You can release items from the quarantine, whitelist the addresses or domains from which they came, or blacklist them.



You can perform actions on specific messages by clicking individual check boxes, then choosing an action button such as **Whitelist** or **Blacklist**.

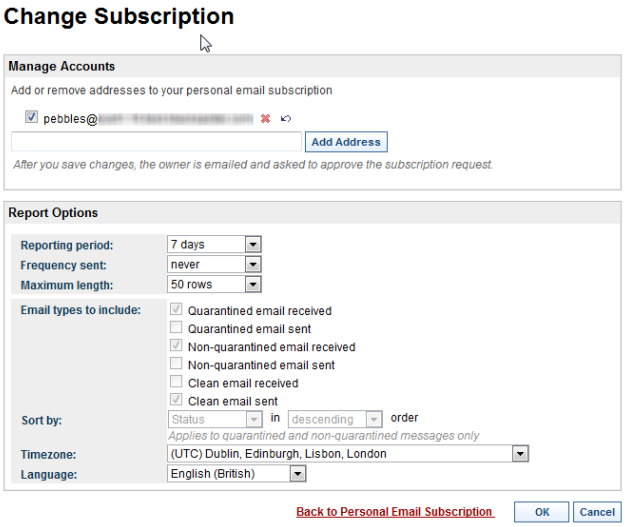
Does the service keep a copy of my email?

By default, the cloud service does not keep copies of messages unless they are quarantined, although your email administrator may configure your system differently. Quarantined messages are automatically deleted after 30 days or your administrator can delete them whenever necessary.

If you click a link on the message report to a clean message, only the email log entries are shown because the message is no longer available to Forcepoint Email Security Cloud.

Can the service automatically send me the message report?

If you have received a report set up by your administrator, click the link in the report to receive it on a weekly basis. Otherwise, to define subscription details request a report, then on the report, click the link to set up the report subscription. You are presented with a screen similar to the one shown below.



You can specify the following subscription options:

- Add or remove email addresses to your report. Approval requests are sent to added email addresses.
- Set report options
  - Scheduling
    - What time period do you want reported: the last 1, 2, 7, 14, or 30 days?
    - How often should the report be delivered: daily, weekdays, weekly, biweekly, monthly, or never?
    - How many rows do you want on each page in the report: 20, 50, 100, 200, or 500?

Note

Subscriptions to the Forcepoint Email Security Cloud message report lapse after 90 days. 62 days after subscribing, each time you receive a report, you are reminded that you should renew your subscription.

  - Email types to include
    - What sections do you want included in the report: suspicious messages received or sent, clean messages received or sent?
    - In what order do you want the information to appear: date/time, subject, from, to, status? Ascending or descending?
  - Localization
    - What time zone should the report assume?
    - In what language do you want the report delivered?

How do I discontinue my report subscription?

You can discontinue your message report subscription any time you want. On any report, click the link **Change subscription**. On the subscription configuration screen, select **never** in the **Frequency** drop-down box under **Scheduling**, then click **Apply**.

Regardless of the settings for the scheduled report, you can also request a report on-demand by filling out the report request form.

Can I change the settings on my message report?

You can change the details of your message report subscription any time you want. On any report, click the link **Change subscription**. Using the same screen you used to subscribe to the report, change the subscription options to your liking.

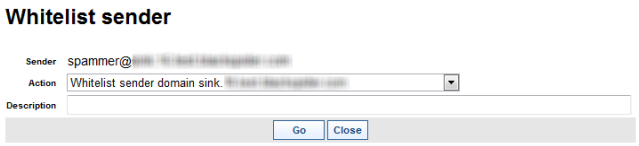
How does the service detect spam?

Forcepoint Email Security Cloud uses a highly advanced spam detection engine that is constantly updated to identify new types of junk mail. Because spam is continuously evolving, the cloud service uses an adaptive engine that learns from previous experience and input from end users. We also have spam analysts on staff to review questionable email and update the detection engines when appropriate.

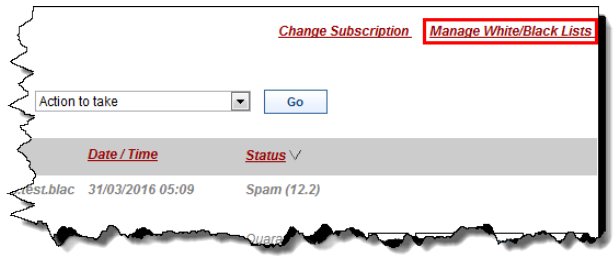
How do I stop the service from blocking messages I want?

The definition of spam is subjective; one user's spam is another user's valid email. Because of this, it is possible for the cloud service to occasionally block email that you want to receive. This typically occurs with newsletters and mail blasts that have spam characteristics. To stop the cloud service from blocking these messages in future, you can add the sender to your personal whitelist (if your administrator has given you this option). Email originating from someone in your whitelist is never classified as spam. To add a sender to your whitelist, find the email in the message report, select the message by clicking its check box, then click the **Whitelist** button.

From the resulting screen, use the drop-down list to choose an action to take: **Whitelist sender email address** or **Whitelist sender domain**, then click **Go**.

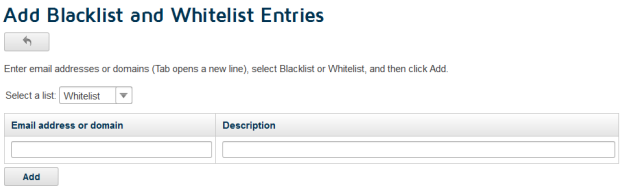


To view or manage your entire whitelist, select **Manage White/Black Lists** from your message report.



On the resulting screen, you can search for email addresses or domains in your whitelist. Click **Show whitelisted**, enter some search criteria, such as the address to find, then click **Search**. You can specify how to sort the results and how many results to display.

If you do not see an address in your whitelist but you want to whitelist it, click the link **Click here to add new entries to your White/Black list**.



On this screen, enter the email address or domain to be whitelisted, then choose **Whitelist** from the **Select a list** drop-down list.

If the message that was blocked was not from a newsletter or mail blast and you believe the cloud service incorrectly classified it, you can send a copy of the message to spam@mailcontrol.com. Forcepoint's spam research team reviews these messages and, if appropriate, updates the detection engine.

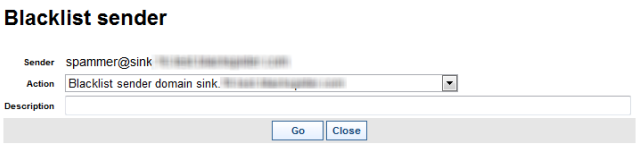
Why didn't the service block the spam I received?

Forcepoint is constantly updating the spam-filtering engine to detect new forms of spam. Forcepoint Email Security Cloud consistently detects over 99 percent of all spam entering the service. However, spam is subjective; one user's spam is another user's valid email.

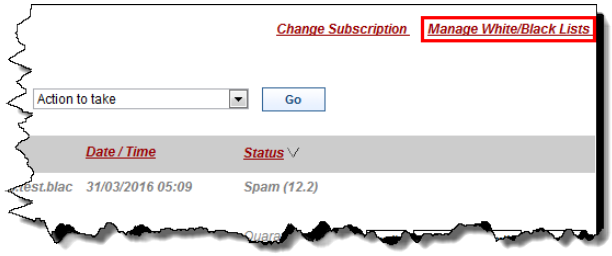
To stop the cloud service from delivering messages from a particular sender in the future, you can add the sender to your blacklist (assuming your administrator has given you this option). Email originating from someone in your blacklist is always classified as spam.

To add a sender to your blacklist, find the email in the message report, select the message by clicking its check box, then click the **Blacklist** button.

From the resulting screen, use the drop-down list to choose an action to take: **Blacklist sender email address** or **Blacklist sender domain**, then click **Go**.

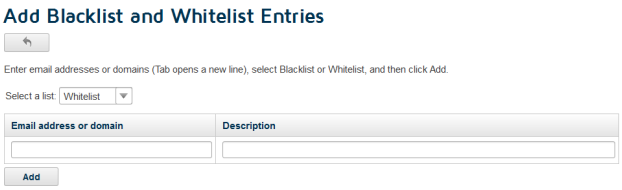


To view or manage your entire blacklist, select **Manage White/Black Lists** from your message report.



On the resulting screen, you can search for email addresses or domains in your blacklist. Click **Show blacklisted**, enter some search criteria, such as the address to find, then click **Search**. You can specify how to sort the results and how many results to display.

If you do not see an address in your blacklist but you want to blacklist it, click the link **Click here** to add new entries to your White/Black list.



On this screen, enter the email address or domain to be blacklisted, then choose **Blacklist** from the **Select a list** drop-down list.

If you believe the cloud service incorrectly classified the message, please inform Forcepoint if you are given the option. This helps us to tune Forcepoint Email Security Cloud. If your administrator has allowed this feature, there is a link at the bottom of the message saying “Click here to report this email as spam.” When you click the link, you receive a confirmation notice.

As previously explained, because the definition of spam is subjective, Forcepoint cannot automatically classify all email similar to this one as spam. Your submission helps us to tune our service. This ultimately benefits all customers. If you want to ensure that you receive no further email from the sending address in question, please add it to your blacklist.

Recommendations for handling spam

Situation	Action to take
You receive email from a single person from whom you no longer want to receive email.	Add the sender to your personal blacklist. (This feature must be enabled by your administrator.)
You receive an email message that you do not consider to be spam.	Add the sender to your personal whitelist. (This feature must be enabled by your administrator.)
You receive unsolicited commercial email.	Select the **Report this email as spam** link at the bottom of the email. Using this service helps improve future spam detection. For text only email where this link does not appear, forward it to spam@mailcontrol.com.
You no longer want to receive e-newsletters or marketing literature that you previously received.	Unsubscribe from the mailing or blacklist the sender. Do not click the **Report this email as spam** link, because others may not consider such email to be spam.
You receive e-newsletters or offers from a company with whom you have had contact, but you were not expecting the communications. (You may have inadvertently agreed to be added to their mailing list.)	Unsubscribe from the mailing or blacklist the sender. Do not click the **Report this email as spam** link, because others may not consider such email to be spam.

Published 14 February 2024