



End User Quick Start Guide

Forcepoint Email Security Cloud

©2022, Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Document last updated: June 7, 2022

Contents

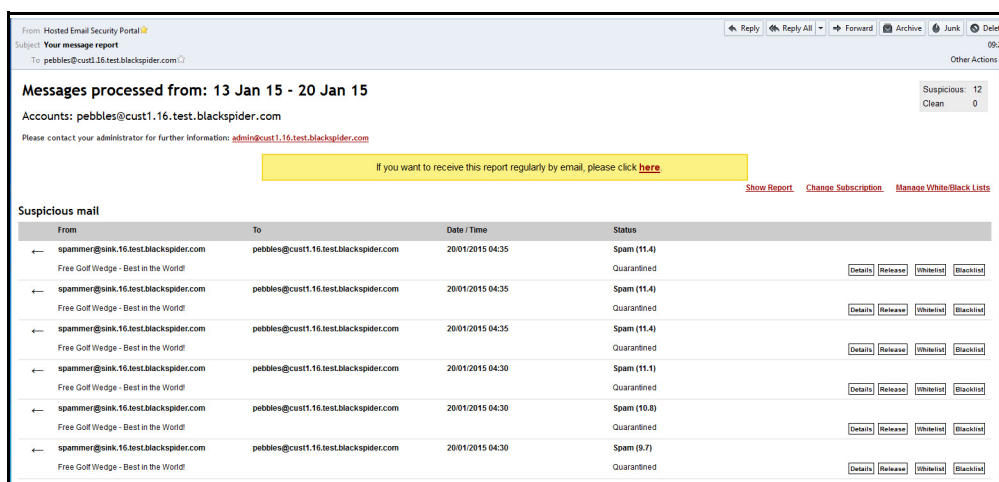
Requesting a message report	1
Scheduling a message report	3
Whitelisting and blacklisting email from certain addresses or domains	4
Modifying records	5
Adding new records	6
Accessing quarantined messages	6
Viewing message details	7
Virus notifications	8
Other notifications	8
“Report this email as spam” link	8

Forcepoint Email Security Cloud: End User Quick Start Guide

Requesting a message report

The Forcepoint Email Security Cloud service allows you to view quarantined messages and take action on them. To do this, first request a personal email report.

1. Visit the webpage: <http://www.websense.com/content/messagereport.aspx>
2. Enter your email address. A message report is emailed to you. Here is an example:



The screenshot shows an email interface with the following content:

- From: Hosted Email Security Portal
- Subject: Your message report
- To: pebbles@cust1.16.test.blackspider.com
- Messages processed from: 13 Jan 15 - 20 Jan 15
- Accounts: pebbles@cust1.16.test.blackspider.com
- Please contact your administrator for further information: admin@cust1.16.test.blackspider.com
- A yellow highlighted box contains the text: "If you want to receive this report regularly by email, please click [here](#)."
- Buttons: Show Report, Change Subscription, Manage White/Black Lists
- Summary: Suspicious: 12, Clean: 0
- Section: Suspicious mail
- Table with columns: From, To, Date / Time, Status, and actions (Details, Release, Whitelist, Blacklist).

From	To	Date / Time	Status	Actions
← spammer@sink.16.test.blackspider.com	pebbles@cust1.16.test.blackspider.com	20/01/2015 04:35	Spam (15.4)	
Free Golf Wedge - Best in the World!			Quarantined	[Details] [Release] [Whitelist] [Blacklist]
← spammer@sink.16.test.blackspider.com	pebbles@cust1.16.test.blackspider.com	20/01/2015 04:35	Spam (15.4)	
Free Golf Wedge - Best in the World!			Quarantined	[Details] [Release] [Whitelist] [Blacklist]
← spammer@sink.16.test.blackspider.com	pebbles@cust1.16.test.blackspider.com	20/01/2015 04:35	Spam (15.4)	
Free Golf Wedge - Best in the World!			Quarantined	[Details] [Release] [Whitelist] [Blacklist]
← spammer@sink.16.test.blackspider.com	pebbles@cust1.16.test.blackspider.com	20/01/2015 04:30	Spam (15.1)	
Free Golf Wedge - Best in the World!			Quarantined	[Details] [Release] [Whitelist] [Blacklist]
← spammer@sink.16.test.blackspider.com	pebbles@cust1.16.test.blackspider.com	20/01/2015 04:30	Spam (16.8)	
Free Golf Wedge - Best in the World!			Quarantined	[Details] [Release] [Whitelist] [Blacklist]
← spammer@sink.16.test.blackspider.com	pebbles@cust1.16.test.blackspider.com	20/01/2015 04:30	Spam (9.7)	
Free Golf Wedge - Best in the World!			Quarantined	[Details] [Release] [Whitelist] [Blacklist]



Note

Your administrator may initiate the message report delivery on your behalf, in which case you do not have to request it. A message report triggered by the administrator includes a link that you can click to subscribe to the report on a weekly basis.





The report provides information about email that you have sent and received, including the status and disposition of each message. If a message was not delivered, it indicates the reason why. Quarantined spam messages include the spam score. The higher the score, the more likely it is that the message is spam.

There are several actions that you can take from your emailed report, depending on how the email administrator has set up your policy.

You can:

- Subscribe to the report
- Change subscription options
- Change the reporting period
- Configure whitelists and blacklists
- View clean and quarantined messages

You can also take actions on messages. For example, you can release messages from your quarantine. To take action on an individual message, select it, then click one of the buttons on the right:

Button	Description
	View details of the message.
	Release the message from quarantine. The requested message is sent to your inbox.
	Add the email address or domain to your personal whitelist. Messages from this sender will always be allowed into your mailbox, unless they contain a virus or malware.
	Add the email address or domain to your personal blacklist. Messages from this sender will be treated as spam.



Note

To select a message, click in the check box to the left of the message in the message report.



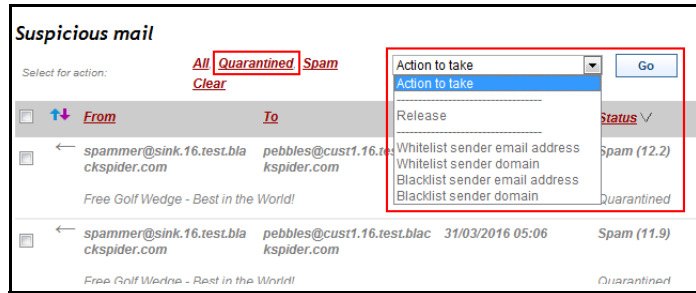
Note

The actions or buttons that are available for a message depend on the message's status.

You can view the online version of the report by clicking **Show Reports**. The online version enables you to take action on several messages at once:

1. Select the messages. You can choose them individually or you can click **Quarantined**, **Spam**, or **All** to select these messages all at once.

- Choose an action from the drop-down list, **Action to take**.



- Click **Go**.

Scheduling a message report

To receive message reports on a regular basis or change an existing report schedule, click the hyperlink, **Change Subscription**, toward the top of the report. Use the resulting page to specify when you want the report sent, and to define how the content of your message reports should be filtered and sorted.

Depending on how your administrator has set up your account, you may be able to 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 personal email 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?

Click **OK** to submit your settings. This becomes the default configuration for all future message reports. You can change this configuration at any time.

Whitelisting and blacklisting email from certain addresses or domains

If you want to block email from certain addresses or domains, and if your administrator has enabled this feature, you can add them to your personal blacklist. Click **Manage White/Black Lists** on the message report that is emailed to you. You can also configure the report to always accept mail from certain addresses or domains. This is called your whitelist.

When you click **Manage White/Black Lists**, a search screen appears. If you have already added a list of email addresses or domains to your blacklist and whitelist, use

this screen to select which email addresses and domains to display in your list. (Use it to filter the view of your list so you can modify the appropriate records more quickly.)

Blacklist & Whitelist

Search Criteria

Email address or domain contains:

Description contains:

Sort results by:

Maximum results to display:

Show blacklisted:

Show whitelisted:

You have no entries in the White or Black list matching your search criteria.

[Click here](#) to add new entries to your White/Black list.

If you want to create a new list or add a new email address or domain to an existing list, click **Click here to add new entries to your White/Black list.** (See [Adding new records](#) for more details.)



Note

Whitelists always take priority over blacklists. If you have blacklisted an email address and also inadvertently whitelisted it, messages from that sender are not blocked.

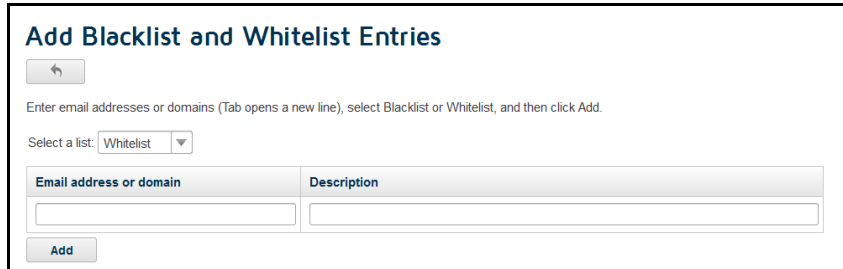
Modifying records

Once you have conducted a search on an existing whitelist or blacklist, you can modify addresses or domains in the list or delete them. To delete an entry, select the entry (by clicking in the check box to the left), then click **Delete**. You can change the disposition of the record from whitelist to blacklist or vice versa by clicking the appropriate button.

You can sort the list by clicking a column heading.

Adding new records

If you want to create a new list or add a new email address or domain to an existing list, click **Click here to add new entries to your White/Black list**.



Enter an address or domain name, a description (if desired), then select the appropriate list the drop-down list (Whitelist or Blacklist). For each line you add, another blank line appears. Click **Add** when done.

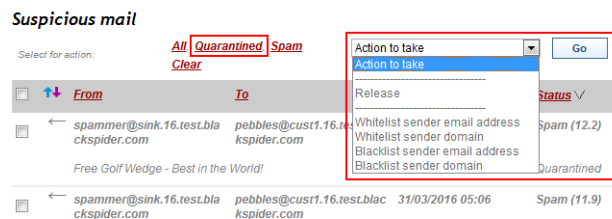
You are notified if the address or domain already exists in the list. For example:

Address entered more than once: "domain.com"

Accessing quarantined messages

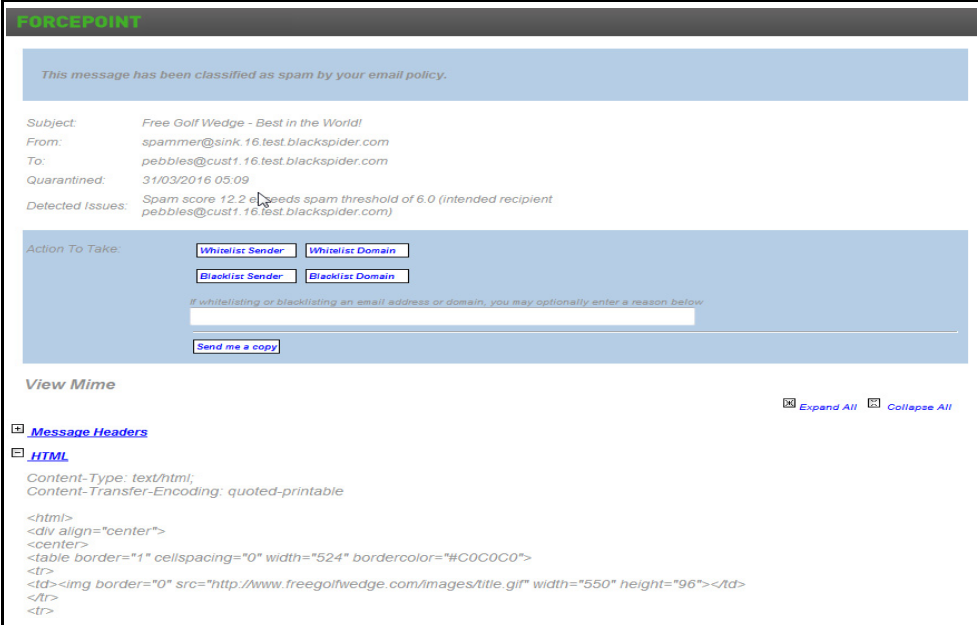
You can sort messages by their status. To view quarantined messages, sort on the **Status** column then scroll to the quarantined section. To view an individual message and learn why it has been quarantined, click **Details** for the message. You then have options of what to do with the message. (See [Viewing message details](#).)

To take action on all of the messages in your quarantine at once, click **Quarantined**, then select an action to take from the drop-down list.



Viewing message details

To view the details of an individual message, select the message (by clicking the check box next to it) then click **Details**. A message log like this appears:



The screenshot shows a Forcepoint interface with a message classified as spam. The message details are as follows:

Subject: Free Golf Wedge - Best in the World!
From: spammer@sink.16.test.blackspider.com
To: pebbles@cust1.16.test.blackspider.com
Quarantined: 31/03/2016 05:09
Detected issues: Spam score 12.2 exceeds spam threshold of 6.0 (intended recipient pebbles@cust1.16.test.blackspider.com)

Action To Take: Buttons for **Whitelist Sender**, **Whitelist Domain**, **Blacklist Sender**, and **Blacklist Domain**. Below these is a text input field with the placeholder: "If whitelisting or blacklisting an email address or domain, you may optionally enter a reason below". A **Send me a copy** button is also present.

View Mime (with **Expand All** and **Collapse All** options)

Message Headers

HTML

```
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable

<html>
<div align="center">
<center>
<table border="1" cellspacing="0" width="524" bordercolor="#C0C0C0">
<tr>
<td></td>
</tr>
</div>
```

If the message is classified as spam, you can perform any of the following tasks:



Note

The tasks available to you depend on the privileges that your email administrator has set up.

- Send a copy to yourself.
- Add the sender to your personal whitelist - any future messages from that sender are not quarantined as spam.
- Add the sending domain to your personal whitelist - any future messages from anyone at the sender's domain (for example., ANYUSER@example.com) are not quarantined as spam.
- Add the sender to your personal blacklist - any future messages from that sender are always quarantined as spam.
- Add the sending domain to your personal blacklist - any future messages from anyone at that domain (for example, ANYUSER@example.com) are always quarantined as spam.

Virus notifications

The cloud service notifies you by email if you are sent a message that contains a virus. Click the link in the notification if you want to view details of the message.



Note

Notification options may be changed by your email administrator.

Other notifications

Your email administrator may have configured email security policies that monitor messages for offensive or inappropriate words, phrases, or other restricted content. If you receive or send such an email, you may be notified of this as well.

“Report this email as spam” link

Spam is subjective - you may think that it is spam, but others may not.

If your administrator has set up a “Report this email as spam” link, please take advantage of it to help us tune the service to better recognize spam.

Whenever you receive spam that you believe should have been blocked, please click the link “Report this email as Spam.”

Note that this does not necessarily mean that all similar, future messages are blocked, but it does contribute to the spam identification process.