

Quick Start Guide for Email End Users

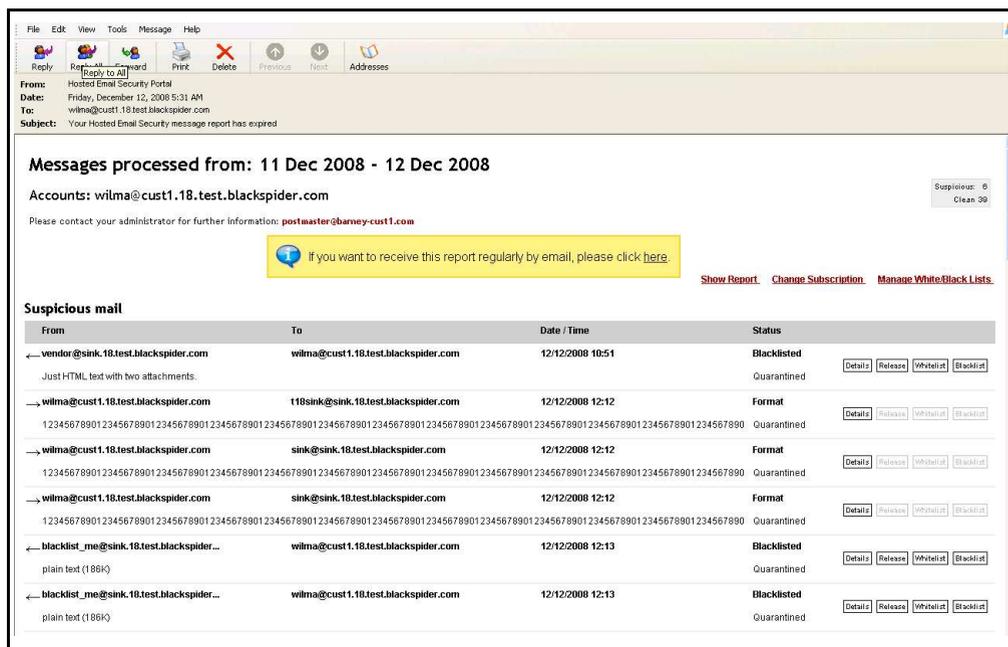
Requesting a message report

The TRITON AP-EMAIL cloud service allows you to view quarantined messages and take action on them. To do this, first request a message report.

1. Visit the webpage:
<http://www.websense.com/content/messagereport.aspx>

2. Enter your email address.

A message report is emailed to you shortly. Here is an example:



The screenshot shows an email report interface. At the top, it displays the sender as 'Hosted Email Security Portal' and the subject as 'Your Hosted Email Security message report has expired'. Below this, it shows the period 'Messages processed from: 11 Dec 2008 - 12 Dec 2008' and the accounts 'Accounts: wilma@cust1.18.test.blackspider.com'. A yellow box highlights a link: 'If you want to receive this report regularly by email, please click here.' Below this, there are links for 'Show Report', 'Change Subscription', and 'Manage White/Black Lists'. The main section is titled 'Suspicious mail' and contains a table with columns for 'From', 'To', 'Date / Time', and 'Status'. The table lists several messages, including one from 'vendor@sink.18.test.blackspider.com' which is 'Blacklisted', and several from 'wilma@cust1.18.test.blackspider.com' which are 'Quarantined'.

From	To	Date / Time	Status
← vendor@sink.18.test.blackspider.com	wilma@cust1.18.test.blackspider.com	12/12/2008 10:51	Blacklisted
Just HTML text with two attachments.			
→ wilma@cust1.18.test.blackspider.com	t18sink@sink.18.test.blackspider.com	12/12/2008 12:12	Format
1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890			
→ wilma@cust1.18.test.blackspider.com	sink@sink.18.test.blackspider.com	12/12/2008 12:12	Format
1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890			
→ wilma@cust1.18.test.blackspider.com	sink@sink.18.test.blackspider.com	12/12/2008 12:12	Format
1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890			
← blacklist_me@sink.18.test.blackspider...	wilma@cust1.18.test.blackspider.com	12/12/2008 12:13	Blacklisted
plain text (186k)			
← blacklist_me@sink.18.test.blackspider...	wilma@cust1.18.test.blackspider.com	12/12/2008 12:13	Blacklisted
plain text (186k)			



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 white lists and black lists
- ◆ 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 white list. 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 black list. 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.



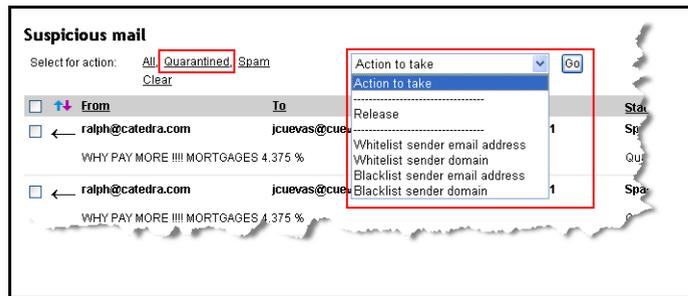
Note

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.

The screenshot shows the 'Configure subscription' form. It has three main sections:

- Report content:** A 'Show mail' section with checkboxes for 'Suspicious' and 'Clean' messages, and 'Received' and 'Sent' options. Below this are 'Order by' dropdowns for 'DateTime' and 'descending' for both 'Suspicious' and 'Clean'.
- Scheduling:** Fields for 'Reporting period' (1 day), 'Maximum length' (1 row), and 'Frequency' (weekly).
- Localisation:** Fields for 'Timezone' (GMT -11:00) and 'Language' (English (U.S.A.)).

 An 'Apply' button is at the bottom right. A link 'Back to the Message Report' is at the bottom left.

Report content

This section is available only if your administrator has allowed it. Use the check boxes to indicate which of the 4 possible sections to include in your report: suspicious messages (received and sent) or clean messages (received and sent).

For each section that you want to include, indicate the order in which you want the content to be sorted (options depend on the section).

- ◆ Date/Time
- ◆ Subject
- ◆ From
- ◆ To
- ◆ Status

Also indicate whether you want the section to be sorted in ascending or descending order.

Scheduling

Specify the number of days you want included in the report and the maximum number of rows in the results table. Also specify how often you want to receive the report: daily, weekdays, weekly, biweekly, or monthly. (Select **never** to cancel the report.)

Localization

Select the language and time zone you want reflected in the report. By default, these are derived from the browser from which you requested the report.

Click **Apply** 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 black list. 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 white list.

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 black list and white list, 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.)

View black and/or white lists by search criteria

Search criteria

Email address or domain contains: Show whitelisted: Sort results by: Address ▾ ascending ▾

Description contains: Show blacklisted: Maximum results to display:

Listed below are the email addresses and domains that you have chosen to whitelist or blacklist within your search criteria.

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

Select for action: All Whitelisted Blacklisted

Clear

Email address or domain ▾	Status	Description	Edit	Delete	Whitelist	Blacklist
<input type="checkbox"/> 00002blackaddress@company.com	Whitelisted	20000 Description of the address 00002	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Whitelist"/>	<input type="button" value="Blacklist"/>
<input type="checkbox"/> 00003blackaddress@company.com	Blacklisted	30000 Description of the address 00003	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Whitelist"/>	<input type="button" value="Blacklist"/>
<input type="checkbox"/> 00004blackaddress@company.com	Blacklisted	40000 Description of the address 00004	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Whitelist"/>	<input type="button" value="Blacklist"/>
<input type="checkbox"/> 00005blackaddress@company.com	Blacklisted	50000 Description of the address 00005	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Whitelist"/>	<input type="button" value="Blacklist"/>
<input type="checkbox"/> 00006blackaddress@company.com	Blacklisted	60000 Description of the address 00006	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Whitelist"/>	<input type="button" value="Blacklist"/>

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](#), page 5 for more details.)



Note

White lists always take priority over black lists. 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 white or black list, 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 on 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](#).

Add addresses and domains to your Black and White lists

Please enter the email addresses or domains to be acted upon, select an Action for each, then click "Add". (Note that for each address you add, a new blank line appears. Do not click "Add" until you have entered all of the addresses or domains you want to add.)

Please select ▼

Email address or domain	Description
<input type="text" value="address1@comp.com"/>	<input type="text" value="Description of address1@comp.com"/>
<input type="text" value="address2@comp.com"/>	<input type="text" value="Description of address2@comp.com"/>
<input type="text"/>	<input type="text"/>

[Go to address and domain search](#)

Enter an address or domain name, a description (if desired), then select an action to take from 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:

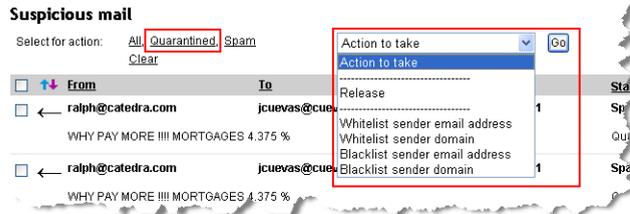
Address entered more than once: "domain.com"

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](#), page 6.)

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:

Message Details

This message has been classified as spam by your email policy.

Subject: **Free Golf Wedge - Best in the World!**
 From: **admin@mailcontrol.com**
 To: **jcuevas@cuevasout.com**
 Quarantined: **15/12/2008 06:43**

Action to take

Whitelist Sender

Whitelist Domain

Blacklist Sender

Blacklist Domain

If whitelisting or blacklisting an email address or domain, you may optionally enter a reason below

Expand all Collapse All

Message headers
 Received: from cluster-0.blade.mailcontrol.com (cluster2-02.odd.blackspider.com [10.5.133.153]) by devblade2-02.odd.blackspider.com (8.13.8/8.13.8) with ESMTP id mBFBhQK004800for <jcuevas@cuevas.com>; Mon, 15 Dec 2008 11:43:18 GMT
 Received: from devblade2-02.odd.blackspider.com (host.blade.mailcontrol.com [10.250.1.1]) by rty010.blade.mailcontrol.com (MailControl) with ESMTP id mBFBhCRS028415(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NO) for <jcuevas@cuevas.com>; Mon, 15 Dec 2008 11:43:13 GMT

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 white list - any future messages from that sender are not quarantined as spam.

- ◆ Add the sending domain to your personal white list - any future messages from anyone at the sender's domain (for example, ANYUSER@acme.com) are not quarantined as spam.
- ◆ Add the sender to your personal black list - any future messages from that sender are always quarantined as spam.
- ◆ Add the sending domain to your personal black list - any future messages from anyone at that domain (for example, ANYUSER@acme.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.