



End User Guide

Websense® Cloud Email Security

2012 Release 6

©1996–2012, Websense Inc.
All rights reserved.
10240 Sorrento Valley Rd., San Diego, CA 92121, USA
Published July 5, 2012
Printed in the United States of America and China.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. 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.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

Topic 1	Using Cloud Email Security	1
	What is Cloud Email Security?	1
	How will it affect me?	1
	Will Cloud Email Security affect those sending email to me?	2
	How does Cloud Email Security handle spam?	2
	How do I know which messages have been blocked?	3
	What is included on the message report?	3
	What does the Status mean?	5
	How do I access my email?	10
	Does Cloud Email Security keep a copy of my email?	11
	Can Cloud Email Security automatically send me the message report?	11
	How do I consolidate end-user message report data from multiple addresses into one report?	13
	How do I discontinue my report subscription?	13
	Can I change the settings on my message report?	14
	How does Cloud Email Security detect spam?	14
	How do I stop Cloud Email Security from blocking messages I want?	14
	Why didn't Cloud Email Security block the spam I received?	17
	Recommendations for handling spam	19
	How does Cloud Email Security help protect me from downloading malicious Web sites?	19

Using Cloud Email Security

Introduction

Welcome to the *Cloud Email Security User's Guide*. Your organization has subscribed to the Cloud Email Security service provided by Websense.

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 Cloud Email Security?

Cloud Email Security 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 Cloud Email Security 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 Cloud Email Security is being used. Your email is delivered normally, but you might notice a reduction in the volume of junk mail you receive.

Cloud Email Security 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. **End-user message report:** Cloud Email Security can send you a message 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?](#), page 3 for more details.

Will Cloud Email Security 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 Cloud Email Security handle spam?

All messages passing through Cloud Email Security 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 unless your administrator configures your organization's policy to do so. 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 Cloud Email Security 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?

Cloud Email Security 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, visit the Web page:

<http://www.websense.com/content/messagereport.aspx>

websense
ESSENTIAL INFORMATION PROTECTION™

MyWebsense Buy & Renew Search English (US) ▼

Products Solutions **Support** Partners About Us

Support Overview Support By Product Solution Center Technical Library Forums **Tools & Policies** Contact Support

Tools & Policies

- Overview
- SiteLookup Tool
- Support Videos
- Support Webinars
- Product Downloads
- 7.6 Upgrade Center
- Websense Hotfixes and Service Packs
- Surfcontrol Hotfixes and Service Packs
- Version Support and End of Life Policies
- Training & Certification
- Early Adopter Program
- Tech Alerts
- MX Record Checker
- My Message Report**
- Get the Most out of

My Message Report

End User Message Report

As a Websense Cloud Email Security customer, you can receive regular updates about messages addressed to you that Cloud Email Security has blocked. To receive this report, enter your email address below. This automatically generates a summary of your quarantined spam. From this email, you can view the messages themselves and configure other settings.

[Example of an End-user Message Report](#)

E-mail address:

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?

Many useful things are included in the message report. The example below shows the online version of the report, which you can access by clicking **Show Reports** in the email version.

Messages processed from: 2 Dec 2008 - 8 Dec 2008 A

Accounts: jcuevas@cuevas.com, jcuevas@cuevasout.com B

Please contact your administrator for further information: me@ppp.com

Suspicious: 97
Clean: 0 C

Show 7 days D Display

If you want to receive this report regularly by email, please click [here](#) E

[Change Subscription](#) [Manage White/Black Lists](#) G H

Suspicious mail

Select for action: All, Quarantined, Spam
Clear

Action to take F

	From	To	Date / Time	Status	
<input type="checkbox"/>	← ralph@catedra.com	jcuevas@cuevasout.com	03/12/2008 12:11	Spam (16.4)	
	WHY PAY MORE !!!! MORTGAGES 4.375 %			Quarantined	K Details Release Whitelist Blacklist
<input type="checkbox"/>	← ralph@catedra.com	jcuevas@cuevasout.com	03/12/2008 12:11	Spam (16.4)	
	WHY PAY MORE !!!! MORTGAGES 4.375 %			Quarantined	Details Release Whitelist Blacklist
<input type="checkbox"/>	← ralph@catedra.com	jcuevas@cuevasout.com	03/12/2008 11:56	Spam (16.4)	
	WHY PAY MORE !!!! MORTGAGES 4.375 %			Quarantined	Details Release Whitelist Blacklist
<input type="checkbox"/>	← ralph@catedra.com	jcuevas@cuevasout.com	03/12/2008 11:56	Spam (16.4)	
	WHY PAY MORE !!!! MORTGAGES 4.375 %			Quarantined	Details Release Whitelist Blacklist
<input type="checkbox"/>	← master@catedra.com	jcuevas@cuevasout.com	03/12/2008 10:29	Spam (18.6)	
	Free Golf Wedge - Best in the World!			Quarantined	Details Release Whitelist Blacklist

Contents

A	The date range for which the report was processed
B	Your email address. Note that if you have consolidated end-user message report data from multiple email accounts into one EUMR, you will see all the email addresses included in that subscription.
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 white lists and black lists
I	<p>A list of your email arranged in the following order (list depends on user and account configuration):</p> <ul style="list-style-type: none"> • Suspicious messages you received or sent • Clean messages you received or sent <p>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.</p>

	Contents
J	An indication of whether a message has been: <div style="display: flex; align-items: center; margin-left: 20px;"> ← received, or → sent. </div>
K	The actions you can take action on a message. (Select a message by clicking in the check box on the left.) Options include: <ul style="list-style-type: none"> • 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 white list. 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 black list. This tells the cloud service to never allow messages from this sender or domain.

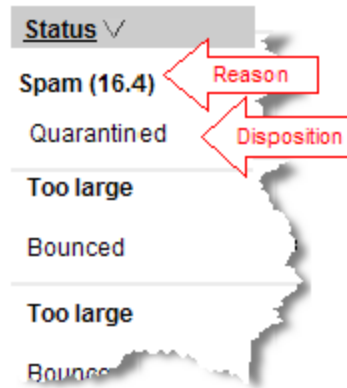
Information included on the message summary section:

- ◆ An indication of whether the message was inbound or outbound
- ◆ The message sender
- ◆ The message recipient
- ◆ The time and date that Cloud Email Security logged the email
- ◆ The status of the email. This includes a reason and a disposition. (See [What does the Status mean?](#), page 5 for more information.)
- ◆ The subject line of the message

What does the Status mean?

The **Status** column of the end-user message 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 black list or your policy's black list.
Clean	The message does not violate any of your policy settings.

Reason	Explanation
Dangerous content	<p>The message contains content that may be dangerous to your machine. This reason can have many sub-reasons:</p> <p>Double extension file - An attachment filename has a double file extension that can be used to mask the real function of the file.</p> <p>Empty archive - The message contains an empty archive file.</p> <p>Executable in service message - The message is a delivery status message that contains executable content.</p> <p>openrelay(block) - The message sender should not have been able to send mail via the sending mail server.</p> <p>Spoofed virus - The message contains a virus. The message sender appears to have been forged.</p> <p>Suspicious attachments - ThreatSeeker found a suspicious attachment \$1 in the message.</p> <p>Zero byte archive - The message contains an empty archive attachment. This is probably because a virus has been removed.</p> <p>Zero byte executable - The message contains an empty executable attachment. This is probably because a virus has been removed.</p>
Extension masked	<p>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.</p>

Reason	Explanation
Format	<p>The Format reason can have many sub-reasons:</p> <ul style="list-style-type: none"> • 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. • 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	<p>The message contains content that breaks a lexical rule set up in your policy.</p>

Reason	Explanation
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 white list or your policy's white list.

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.
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:

Message Details

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

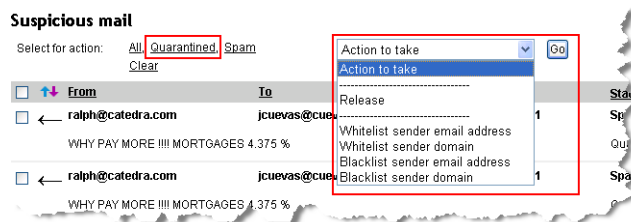
Subject **Free Golf Wedge - Best in the World!**
 From **admin@mailcontrol.com**
 To **jcuevas@cuevasout.com**
 Quarantined **15/12/2008 06:43**

Action to take

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

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 white list or black list. 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 an 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 Cloud Email Security keep a copy of my email?

By default, Cloud Email Security 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 Cloud Email Security.

Can Cloud Email Security 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 **Change Subscription** link. You are presented with a screen similar to the one shown below.

The screenshot shows the 'Change Subscription' form in the TRITON Cloud Security interface. The form is divided into two main sections: 'Manage Accounts' and 'Report Options'.

Manage Accounts: This section allows users to add or remove email addresses for the report. It includes a checkbox for 'jcuevas2@cust2.com' and an 'Add Address' button. A note states: 'After you save changes, the owner is emailed and asked to approve the subscription request.'

Report Options: This section allows users to configure the report details. It includes the following options:

- Reporting period:** 14 days (dropdown)
- Frequency sent:** weekly (dropdown)
- Maximum length:** 50 rows (dropdown)
- Email types to include:** A list of checkboxes for 'Quarantined email received', 'Quarantined email sent', 'Non-quarantined email received', 'Non-quarantined email sent', 'Clean email received', and 'Clean email sent'. All are checked.
- Sort by:** Status (dropdown) in ascending (dropdown) order. A note below states: 'Applies to quarantined and non-quarantined messages only.'
- Timezone:** GMT +00:00 (dropdown)
- Language:** English (British) (dropdown)

At the bottom of the form are 'Submit' and 'Close' buttons.

On the **Change Subscription** screen, you can specify the following subscription options:

- ◆ **Manage Accounts**
 - Do you want to consolidate the end user message report (EUMR) data for multiple aliases or email accounts into one EUMR?
- ◆ **Report Options**
 - 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, or monthly?
 - How many rows do you want on each page in the report: 20, 50, 100, 200, or 500?
 - What sections do you want included in the report: quarantined suspicious messages received or sent, non-quarantined suspicious messages received or sent, clean messages received or sent?
 - In what order do you want the information about quarantined and non-quarantined messages to appear: status, date/time, subject, from, or to? Ascending or descending? .



Note

Subscriptions to the Cloud Email Security message report lapse after 93 days. 62 days after subscribing, each time users receive a report, they are reminded that they should renew their subscription.

- What time zone should the report assume?
- In what language do you want the report delivered? Cloud Email Security supports 14 languages:
 - Czech
 - Dutch
 - English (U.K. and U.S.)
 - French
 - German
 - Greek
 - Italian
 - Polish
 - Portuguese (Brazilian)
 - Romanian
 - Slovak
 - Spanish
 - Swedish

Click **Submit** to submit your settings. You can change this configuration at any time.

Regardless of the settings for the scheduled report, you can also request a report on-demand by filling out the report request form at <http://www.websense.com/content/messagereport.aspx>.

How do I consolidate end-user message report data from multiple addresses into one report?

If you are allowed to modify settings in your end-user message report (EUMR), you have the option to consolidate EUMR data from your other email accounts or aliases into one EUMR. Reviewing and managing one report versus several reports may help save time.

Note that if LDAP synchronization is enabled, all aliases associated with you will be automatically listed on the Change subscription screen under Add subscription addresses. You can then add one or more of them into one consolidated report.

To consolidate addresses, do the following:

- ◆ From the EUMR, click **Change Subscription**.
- ◆ Under **Manage Accounts**, check the box for the email address or addresses that you want to add if a list is given, or enter the email address.
- ◆ Click **Add Address**.
- ◆ If you want to add a new email address, you must receive approval from the owner of that address. Clicking **Add Address** sends an email request to the address owner requesting approval. Until the owner approves the request, the email will be marked “pending approval by owner.” If the owner approves the request, you are notified by email and the “pending” status is removed. The owner may choose to decline the request in which case you may not add the email address to the EUMR report.
- ◆ To remove an address from the report, uncheck the checkbox next to the email address that you want to remove. Unchecking the box reveals a **Remove** link. If you click on this link, you are asked if you’re sure you want to remove the address.

Note that after you create a consolidated EUMR, if you then order a message report, or are set up to automatically receive a report, the report that you receive is the consolidated report. If you wish to receive reports from more than one subscription (for example, an individual and a consolidated subscription), your administrator must create these subscriptions for you in the Cloud Security portal.

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**.

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 Cloud Email Security detect spam?

Cloud Email Security uses a highly advanced spam detection engine that is constantly updated to identify new types of junk mail. Because spam is continuously evolving, Cloud Email Security 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.

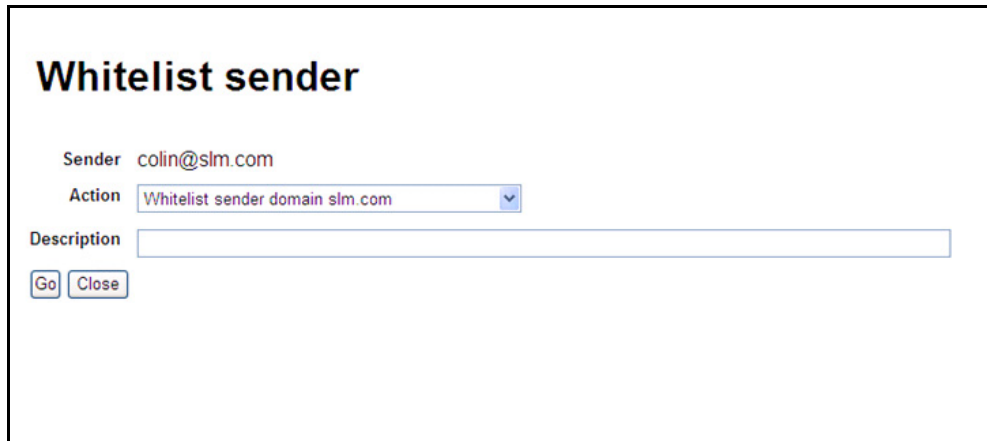
How do I stop Cloud Email Security from blocking messages I want?

The definition of spam is subjective; one user's spam is another user's valid email. Because of this, it is possible for Cloud Email Security to occasionally block email that you want to receive. This typically occurs with newsletters and mail blasts that have spam characteristics.

To stop Cloud Email Security from blocking these messages in future, you can add the sender to your personal white list (if your administrator has given you this option). Email originating from someone in your white list is never classified as spam. To add a sender to your white list, 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**.



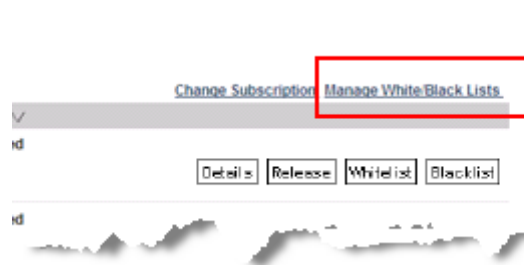
Whitelist sender

Sender: colin@slm.com

Action: Whitelist sender domain slm.com

Description:

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



On the resulting screen, you can search for email addresses or domains in your white list.

If you have created an end-user message report (EUMR) subscription that consolidates EUMR data from multiple email accounts into one report, a column of the accounts associated with the consolidated EUMR displays on this page. In a consolidated subscription, any action taken applies to all email accounts in the subscription. See [How do I consolidate end-user message report data from multiple addresses into one report?](#), page 13 for details on how to create a consolidated subscription.

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.

TRITON Cloud Security

View black and/or white lists by search criteria

Search criteria

Email address or domain contains:

Show whitelisted: ☒

Show blacklisted: ☒

Sort results by: Address ascending

Description contains:

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: Please select action:

Email address or domain	Account	Status	Description
<input type="checkbox"/> spammer1@cust2.com	alias_00174_1@cust1.5.test.blackspider.com	Blacklisted	
<input type="checkbox"/> spammer1@cust2.com	alias_00174_2@cust1.5.test.blackspider.com	Blacklisted	
<input type="checkbox"/> spammer1@cust2.com	alias_00174_3@cust1.5.test.blackspider.com	Blacklisted	
<input type="checkbox"/> spammer2@cust2.com	alias_00174_1@cust1.5.test.blackspider.com	Blacklisted	
<input type="checkbox"/> spammer2@cust2.com	alias_00174_2@cust1.5.test.blackspider.com	Blacklisted	
<input type="checkbox"/> spammer2@cust2.com	alias_00174_3@cust1.5.test.blackspider.com	Blacklisted	

If you do not see an address in your white list but you want to white list it, click the link [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](#)

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

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

Why didn't Cloud Email Security block the spam I received?

Websense is constantly updating the spam-filtering engine to detect new forms of spam. Cloud Email Security 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 Cloud Email Security from delivering messages from a particular sender in the future, you can add the sender to your black list (assuming your administrator has given you this option). Email originating from someone in your black list is always classified as spam.

To add a sender to your black list, 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**.

Blacklist sender

Sender: mqbftv@ckaof2wvt4k5.lsmorcossin.com

Action: Blacklist sender domain ckaof2wvt4k5.lsmorcossin.com

Description:

Go

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



On the resulting screen, you can search for email addresses or domains in your black list. 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.

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 Please select action

<input type="checkbox"/> Email address or domain	Status	Description	
<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 do not see an address in your black list but you want to black list it, click the link [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 button 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](#)

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

If you believe Cloud Email Security incorrectly classified the message, please inform Websense if you are given the option. This helps us to tune Cloud Email Security. 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, Websense 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 black list.

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 black list. (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 white list. (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 black list 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.)	

How does Cloud Email Security help protect me from downloading malicious Web sites?

Cloud Email Security offers URL sandboxing, a feature that helps protect end users from downloading malicious Web sites. It inspects uncategorized URLs in email by tagging them for additional real-time advanced security analysis. Your administrator may configure email policies that use this feature.

With URL sandboxing, if you click on a link within an email and that link or elements associated with that link are suspicious, you receive a warning that “The link may not be safe.” The notification includes:

- ◆ The domain you are trying to access.

- ◆ The reasons the link is considered suspicious, such as the sender email address may be unknown to our service or the sending mail server may have a suspicious reputation.
- ◆ The option to analyze the page further.



If you answer **NO** to **Analyze the page?**, the suspicious link is not analyzed. You can then close the notification window. For your protection, you cannot access the page.

If you answer **YES**, the page is analyzed using Cloud Email Security real-time advanced security analysis. You then receive one of four possible messages:

Notification	Description
The link appears to be safe	No malicious threats found. The notification lists the URL and category or categories of the page. You can proceed to view the page if you choose to do so.
Access denied	Malicious threats detected in the page. The notification lists any matched categories along with the sites suspected of being infected with a malicious link. You cannot access the page.
Access denied	You may also receive an Access denied notification if your organization does not permit you to browse uncategorized Web pages. Contact your administrator for more information.
Unable to access page	The Web server may be down or the link may be incorrect. You may want to try again later, or contact your administrator for more information.