Cisco Email Perimeter

Cisco Email Perimeter

The Cisco Email Perimeter is the mechanism DoIT uses to route and scan all email messages entering the State Enterprise email system. It is used to provide delivery of email correspondence from / to external sources; as well as, protect the security of the mail system for all our customers. The perimeter solution reviews all email for potential security threats such as Phishing, Spam, viruses, Denial of Service attacks. As it finds these threats it takes action according to the type and severity of the threat. For those with a lower threat it will place the message into the Quarantine Manager, which is fully explained below. Cisco Email Perimeter also allows users to send secure messages using its integrated CRES (Cisco Registered Envelope Service); more information on this is found near the below of this document or at this Secure Messaging FAQ Link.

Cisco Quarantine Manager

Cisco Email Perimeter uses an email quarantine manager to provide a central point for users to analyze and act upon emails that have been identified as potential Spam. This gives the user the ability to Release/Delete messages and Whitelist/Blacklist senders or sending domains. With Cisco Quarantine Manager, the user will be able to act upon the messages within the Spam Digest email or access a user Interface to perform these functions. User created blacklist/whitelists from our old system will not be brought over to the new email perimeter. Cisco uses a different reputation dictionary, so these may need to be set up again when the user receives their first quarantine notification. Instructions on how to set these blacklists/whitelists are explained in more detail below.

Cisco Quarantine Notification

From: noreply@illinois.gov <noreply@illinois.gov> **On Behalf Of** Cisco Quarantine Manager
Sent: Friday, March 15, 2019 4:01 PM
To: User, test <test.user@Illinois.gov>
Subject: Spam Quarantine Notification

Spam Quarantine Notification

The message(s) below have been blocked by your administrator as suspected spam.

There are 2 new messages in your Email Quarantine since you received your last Spam Quarantine Notification. If the messages below are spam, you do not need to take any action. Messages will be automatically removed from the quarantine after 17 day(s).

To see all quarantined messages view your email quarantine.

Quarantined Email			
	From	Subject	Date
Release	<External.User@gmail.com>	[External] [SUSPECTED SPAM] Test Spam Quarantine	15 Mar 2019
Release	<External.User@gmail.com>	[External] [SUSPECTED SPAM] Test Spam Quarantine	15 Mar 2019
			View All Quarantined Messages(4)

Note: This message has been sent by a notification only system. Please do not reply

If the above links do not work, please copy and paste the following URL into a Web browser:
https://quarantine.illinois.gov:4431/quarantine?h= b29b6frestc20694892arb5636e0bb33e2&email=test.user%40illinois.gov&action=search

In order to access spam quarantine in old portal, please copy and paste the following URL into a Web browser:
https://quarantine.illinois.gov/Search?h=b29b6frestc20694892arb5636e0bb33e2&email=test.user%40illinois.gov

If you have any questions please contact DoIT Service Desk 217-524-DoIT(3648) or 312-814-DoIT(3648).

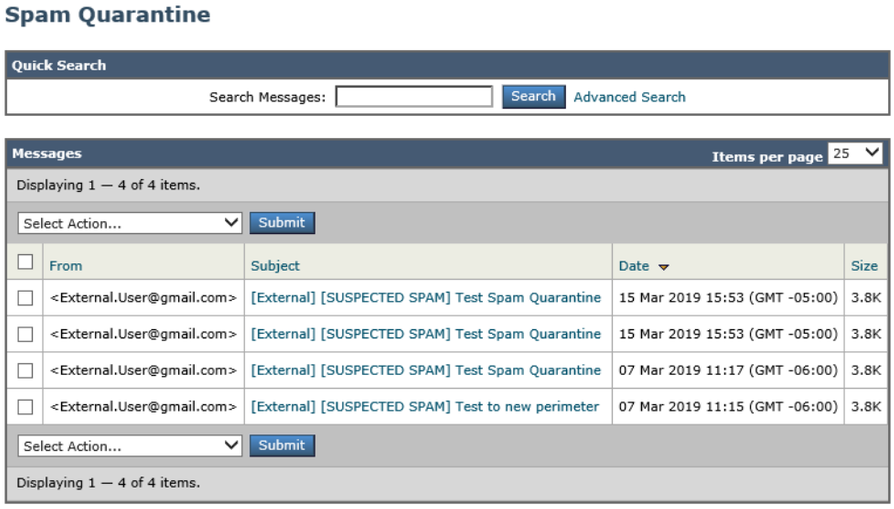
You can choose to **release** the message or view all the quarantine messages using the link provided in the email. If you choose to not take any actions on these messages the message(s) will automatically be purged from the system in 17 days.

Personalized Cisco Quarantine Manager Link

Each user who accesses Cisco Quarantine Manager, will have a personalized link in which they can manage their quarantined emails and manage blacklisting/whitelisting email addresses or domains. The link is contained within your spam digest and can be added to your favorites for future access. **The links in the spam digest are unique to each user and should not be shared with any other person**

Releasing or Deleting Quarantined Messages

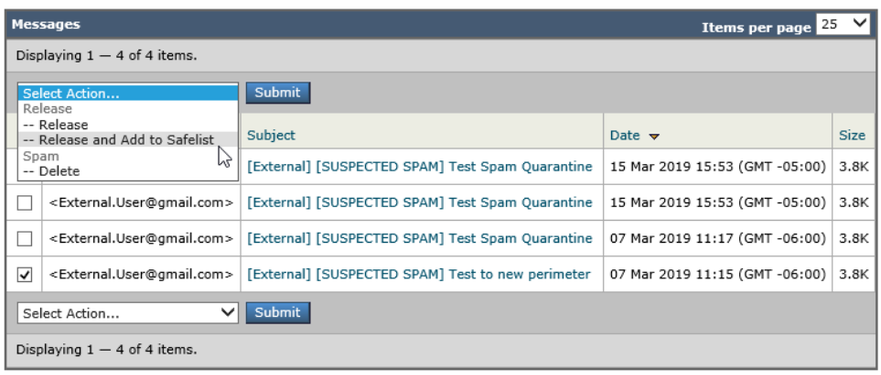
After accessing the Cisco Quarantine Manager, you can check the message you want to perform an action on. In this case, you may want to release the message or release and add the sender to your safelist for future messages. You can also choose to delete the message.



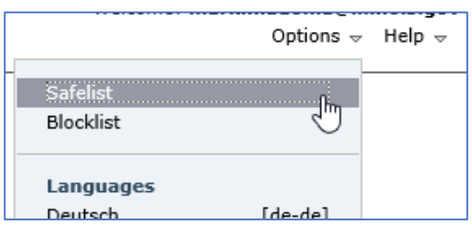
Hover over truncated fields to see the complete text.

Blacklist/Whitelist

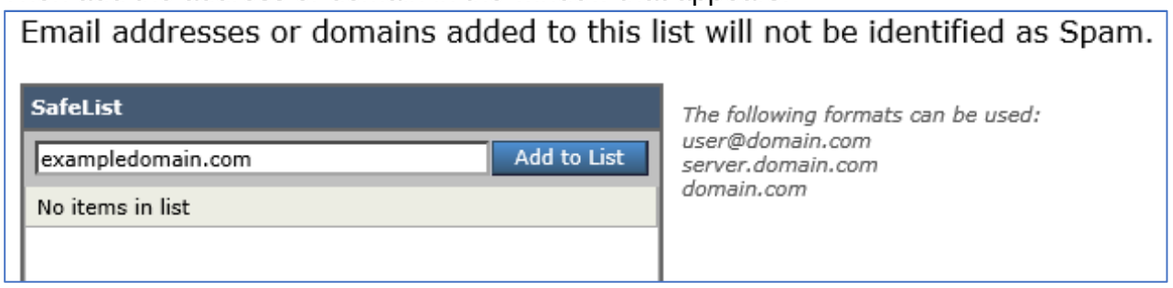
To perform other actions such as manually whitelisting & blacklisting you can click **Select Action** then **Release and Add to Safelist**



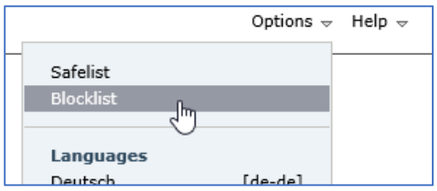
Another way to whitelist an email address or domain is to select **Options** in the right corner and click **Safelist.**



Then add the address or domain in the window that appears.

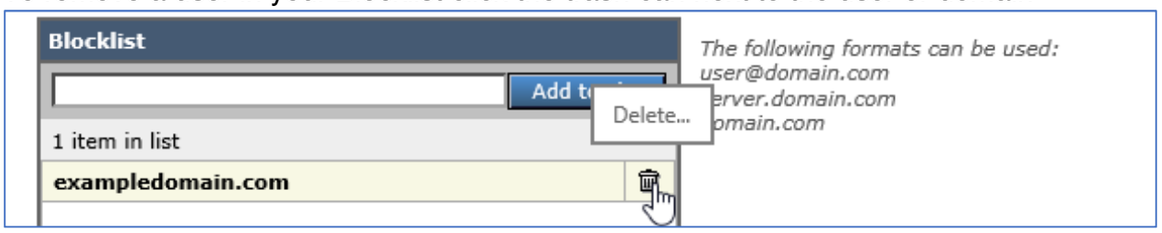


To **blacklist** senders, you can click on **Options** in the upper right corner and select "**Blocklist**".



Then add the address or domain

To remove a user in your Blocklist click the trash can next to the user or domain



Secure Message Delivery - CRES
Secure message delivery is a service that guarantees secure delivery of email by either delivering Transport Layer Security (TLS) or by storing the email within the Cisco Registered Envelope Services (CRES) and providing a secure link to the recipient to retrieve the email. For information about Secure Message Delivery you can click on the following link. Link to Secure Message Delivery FAQ.

Cisco Outbreak Filter (New Feature)
Cisco Outbreak Filters protects our network from large-scale virus outbreaks and smaller, non-viral attacks, such as phishing scams and malware distribution, as they occur. Cisco gathers data on outbreaks as they spread and sends updated information to our Email Security appliance in real-time to prevent these messages from reaching our users. Cisco uses global traffic patterns to develop rules that determine if an incoming message is safe or part of an outbreak.

Messages that may be part of an outbreak are quarantined until they're determined to be safe based on updated outbreak information from Cisco. Outbreak Filters analyze a message's content and searches for URL links to detect this type of non-viral attack. Outbreak Filters can rewrite URLs to

redirect traffic from potentially harmful websites through a web security proxy, which either warns users that the website they are attempting to access may be malicious or blocks the website completely. Messages which are identified using the Cisco Outbreak Filter and are determined to be clean are marked with "Suspicious Message" in the subject line when delivered to the user. Users should be aware of this and proceed with caution when opening these messages.

Graymail (Coming Soon!!!!)
Graymail messages are messages that do not fit the definition of spam. Examples of graymail would be, newsletters, mailing list, subscriptions, social media notifications, and so on. These messages were of use at some point in time but have subsequently diminished in value to the point where the end user no longer wants to receive them. The difference between graymail and spam is that the end user intentionally provided an email address at some point (for example, the end user subscribed to a newsletter on an e-commerce website or provided contact details to an organization during a conference) as opposed to spam, messages that the end user did not sign up for.

The graymail engine classifies each graymail message into one of the following categories:

- **Marketing Email**. Advertising messages sent by professional marketing groups, for example, bulletins from Amazon.com with details about their newly launched products.
- **Social Network Email**. Notification messages from social networks, dating websites, forums, and so on. Examples include alerts from:
    - LinkedIn, for jobs that you may be interested in
    - CNET forums, when a user responds to your post.
- **Bulk Email**. Advertising messages sent by unrecognized marketing groups, for example, newsletters from TechTarget, a technology media company.

How the Cisco Graymail unsubscribe function works

- End user receives an email with graymail banner and they no longer want to receive messages from this sender.
- End user clicks on the unsubscribe button which is presented to them in the Cisco format.
- Cisco Graymail Unsubscribe then extracts and checks the reputation of the unsubscribe link.
- If the link is malicious, it will block page to the end user.
- If the link is legitimate, Cisco will execute the unsubscribe process on the user's behalf.
- The unsubscribe status will then be displayed to the end user – it may take up to four hours for the unsubscribe to take effect.

Cisco URL Filtering and URL Re-Write (Coming Soon!!!)
Cisco URL Filtering allows control and protection against malicious or undesirable links that are introduced into our system within emails. Cisco URL Filtering will scan all URL's contained in an email and determine if the URL is safe to access. Filtering will re-write the URL if needed so the link takes the user to a Cisco Security Proxy first. This allows URLs to be scanned/checked by Cisco to determine the safety of the web-sites. If the site is determined to be unsafe, Cisco will block access.

If you are having issues, please contact the DoIT Help Desk at 217-524-3648 (Springfield) or 312-814-3648 (Chicago).