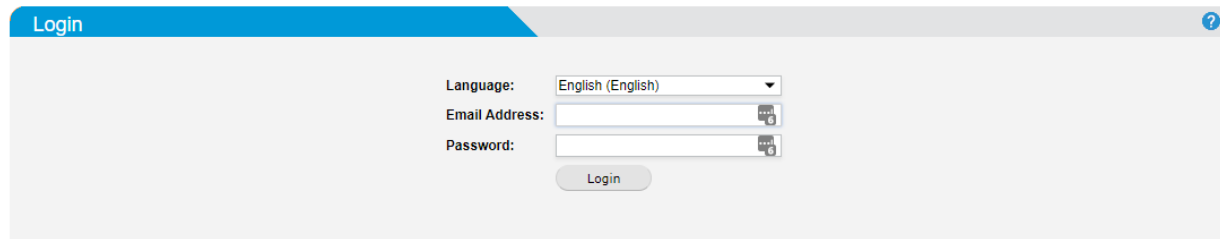


Spam Filter User Guide

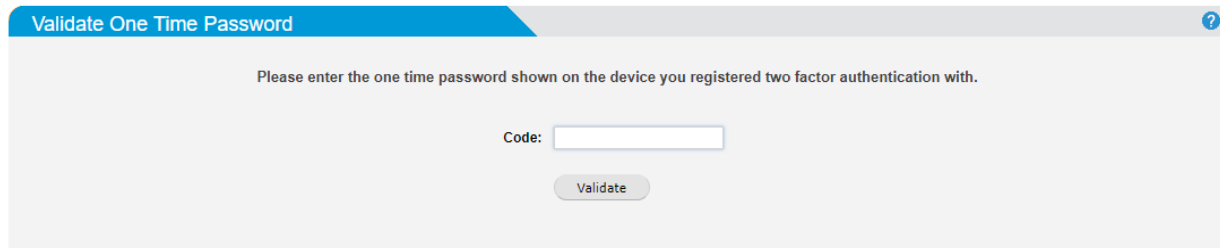
Ver. 2022.03.28

Login:

The login form is titled "Login" in a blue header bar. It contains three input fields: "Language:" with a dropdown menu set to "English (English)", "Email Address:" with a text box and a small icon, and "Password:" with a text box and a small icon. Below these fields is a "Login" button. A help icon (?) is in the top right corner.

To log in, enter your **full email address** and password and click Login button.

2-factor login:

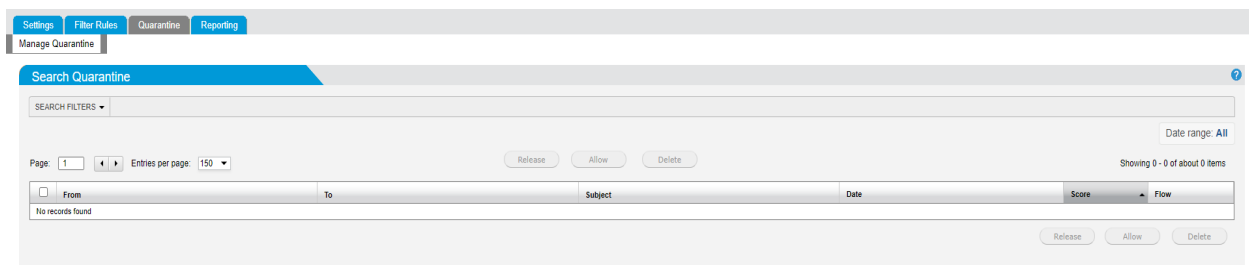
The form is titled "Validate One Time Password" in a blue header bar. It contains a text box for "Code:" and a "Validate" button. A message above the code box says: "Please enter the one time password shown on the device you registered two factor authentication with." A help icon (?) is in the top right corner.

If you have 2-factor authentication enabled, it will ask you for your code.

(On first login you will not have this prompt. How to setup 2-factor is listed below)

Managing Quarantine Email:

Go to Quarantine > Manage Quarantine. Use Search Filters and Display Settings to manage the list of emails in quarantine.

The interface shows a navigation bar with tabs: "Settings", "Filter Rules", "Quarantine", and "Reporting". Below is a "Manage Quarantine" section. It includes a "Search Filters" dropdown, a "Date range: All" selector, and a table with columns: "From", "To", "Subject", "Date", "Score", and "Flow". The table currently shows "No records found". There are "Release", "Allow", and "Delete" buttons at the bottom right.

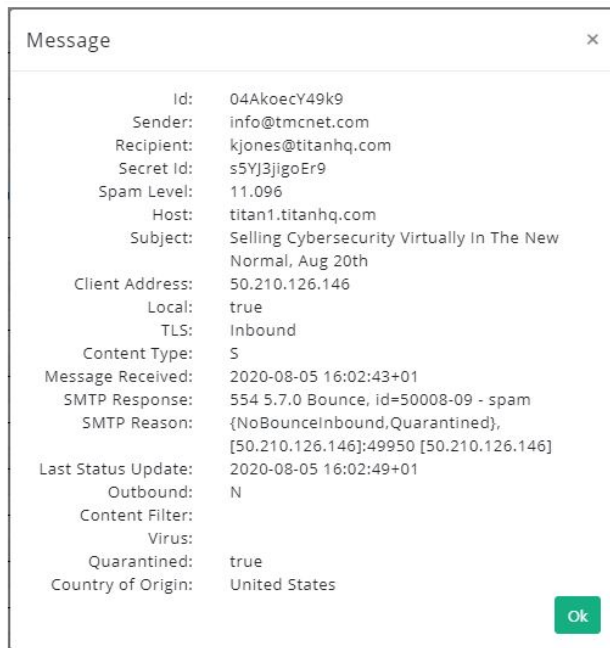
Messages will reside in quarantine for 30 days after that they are deleted from quarantine.

NOTE: The history tab will display in Mountain Time.

The following actions can be performed on email in quarantine:

View Message

Click any message in quarantine to view it in a separate window. Click on one of the four tabs to view more information on the quarantined email - Details, View Message, View Source, and Options.



All images are blocked in review to prevent possible inappropriate content. If a message is subsequently released and delivered then the original images will be present.

Release Message

On a rare occasion, an email in quarantine may have been incorrectly identified as spam. This is known as a 'false positive'. To release a message, click the checkbox to the left of the email address and click the Release button. This will automatically forward the email to the recipient.

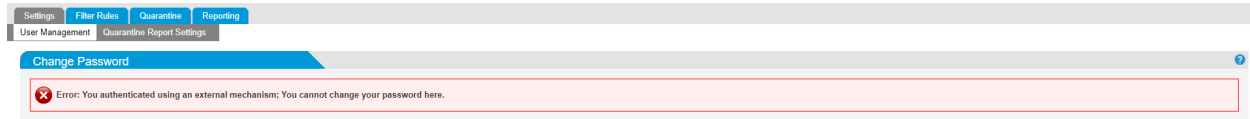
Allow a Sender

To add the email address of an email in quarantine to your Allow List, click the checkbox to the left of the email address and click the Allow button. The email address then is added to the email recipients allow list and the email is released from quarantine and delivered to the recipient.

Delete Message

To delete a message, click the checkbox to the left of the email address and click the Delete button. Delete multiple messages at the same time by selecting several email addresses at once before clicking Delete.

Change User Password:

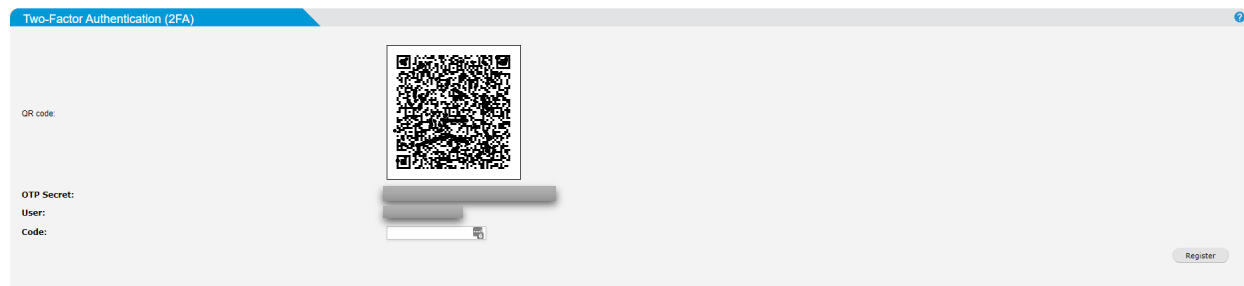


Your email credentials are synced with the filter so you will not be able to change your password from the filter.

Two factor authentication:

Two-factor authentication (2FA) is an additional layer of security used to protect your mail filter account from unauthorized access. If 2FA is enabled, a user provides their username and password on login and then must also provide an additional piece of information known only to them. This additional piece of information is a one-time password, regenerated every thirty seconds.

Go to Settings > User Management > Two-Factor Authentication (2FA) to manage 2FA settings.



Follow the steps below to set up two-factor authentication:

1. Before continuing, you must download and install an authenticator phone app, e.g., Google Authenticator or FreeOTP.
2. Scan the QR code using the authenticator app installed in step 1.



If you are unable to scan the QR code, manually enter the OTP (One Time Password) secret provided in the OTP Secret: field.

3. In the Code: field, enter the code generated from the authenticator phone app.
4. Click Register.

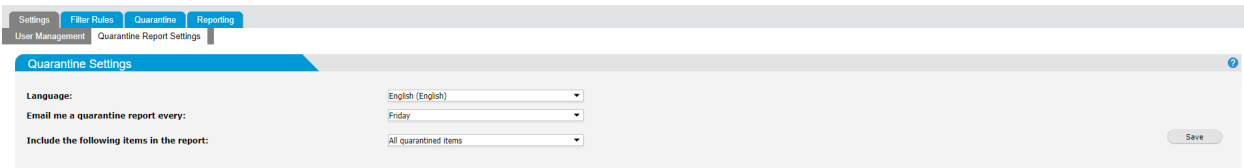
Recovery Codes

A set of recovery codes are generated when 2FA is enabled. Store these codes carefully as they are the only way to access your mail filter account if the device you registered 2FA on is lost.

The recovery codes are one-time use, and they must be used in sequential order.

Quarantine Report Settings:

This page allows you to manage the language, frequency, and content of your own Quarantine Report.

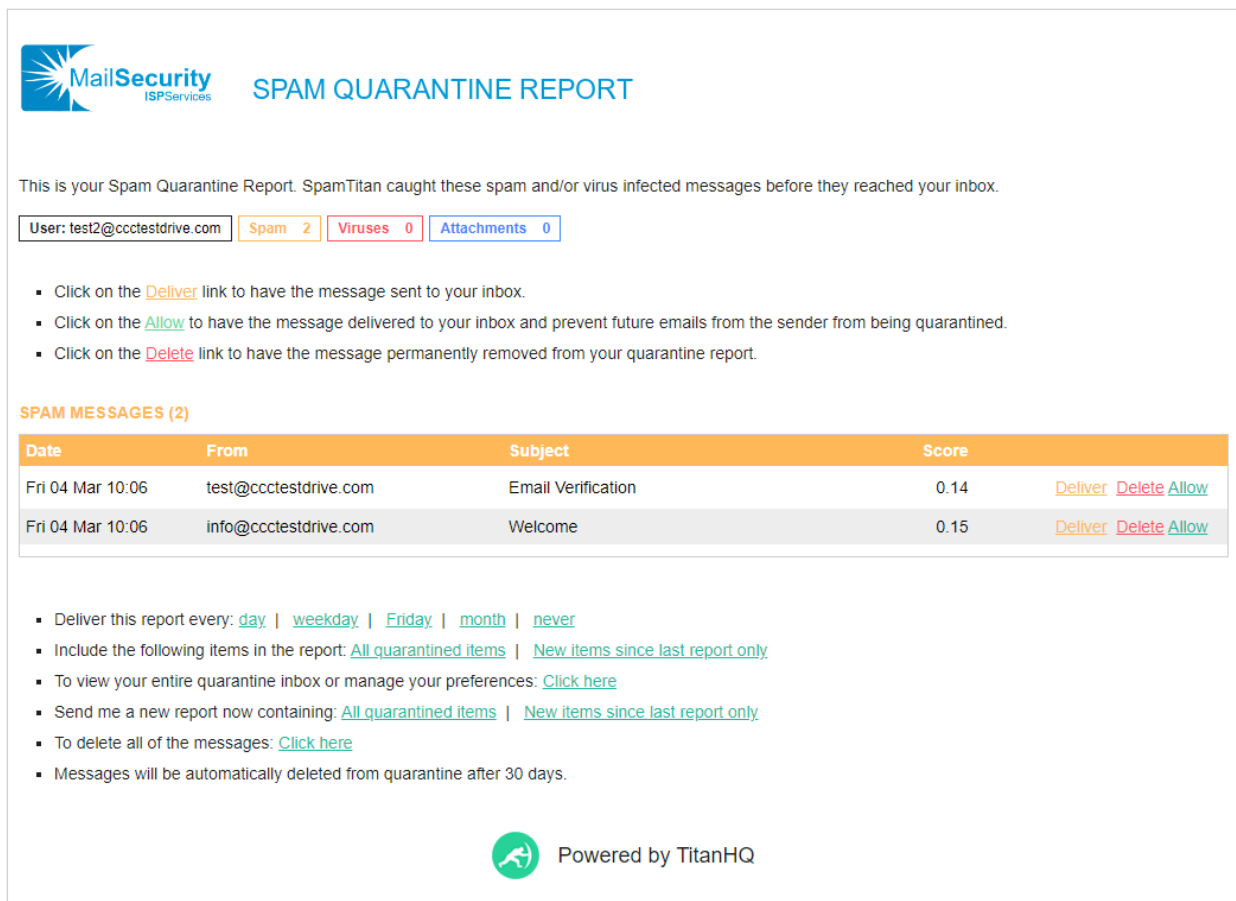


The screenshot shows the 'Quarantine Report Settings' page. At the top, there are tabs for 'Settings', 'Filter Rules', 'Quarantine', and 'Reporting'. Below these, there are sub-tabs for 'User Management' and 'Quarantine Report Settings'. The 'Quarantine Report Settings' tab is active. The settings include: 'Language' set to 'English (English)', 'Email me a quarantine report every:' set to 'Friday', and 'Include the following items in the report:' set to 'All quarantined items'. A 'Save' button is located at the bottom right.

Spam Quarantine Report:

A quarantine report contains a list of emails that have been caught and quarantined. Users can directly manage their quarantined mail through these reports, which are emailed to them on a periodic basis.

A quarantine report provides links for a user to manage their quarantined emails directly from the report. See a sample quarantine report below.



The sample report is titled 'SPAM QUARANTINE REPORT' and is from MailSecurity ISPServices. It states: 'This is your Spam Quarantine Report. SpamTitan caught these spam and/or virus infected messages before they reached your inbox.' Below this, it shows the user 'test2@ccctestdrive.com' with 2 Spam, 0 Viruses, and 0 Attachments. A list of instructions follows: 'Click on the [Deliver](#) link to have the message sent to your inbox.', 'Click on the [Allow](#) to have the message delivered to your inbox and prevent future emails from the sender from being quarantined.', and 'Click on the [Delete](#) link to have the message permanently removed from your quarantine report.'

SPAM MESSAGES (2)

Date	From	Subject	Score	
Fri 04 Mar 10:06	test@ccctestdrive.com	Email Verification	0.14	Deliver Delete Allow
Fri 04 Mar 10:06	info@ccctestdrive.com	Welcome	0.15	Deliver Delete Allow

Below the table, there are more instructions: 'Deliver this report every: [day](#) | [weekday](#) | [Friday](#) | [month](#) | [never](#)', 'Include the following items in the report: [All quarantined items](#) | [New items since last report only](#)', 'To view your entire quarantine inbox or manage your preferences: [Click here](#)', 'Send me a new report now containing: [All quarantined items](#) | [New items since last report only](#)', 'To delete all of the messages: [Click here](#)', and 'Messages will be automatically deleted from quarantine after 30 days.'

At the bottom, there is a logo for TitanHQ and the text 'Powered by TitanHQ'.

User Block List:

Go to Filter Rules > User Block List to manage block list entries.



The screenshot shows the 'User Block List' interface. At the top, there are tabs for 'Settings', 'Filter Rules', 'Quarantine', and 'Reporting'. Below these, there are sub-tabs for 'User Block List', 'User Allow List', and 'Geoblocking'. The main content area is divided into two sections: 'Blocked Email Addresses' and 'Blocked Domains'. Each section has a search bar, a 'Page' selector, and an 'Entries per page' dropdown. The 'Blocked Email Addresses' section shows a table with columns for 'Sender Email', 'Comment', 'Last Modified', and 'Options'. The 'Blocked Domains' section shows a table with columns for 'Sender Domain', 'Include Subdomains', 'Comment', 'Last Modified', and 'Options'. Both sections show 'No records found' and have buttons for 'Edit...', 'Delete', 'Import...', and 'Add...'.

If you Block an address or domain, then mail from that address or domain to your account will be blocked before it reaches your inbox.

Adding a Block List Entry

1. Go to Filter Rules > Block List > Blocked Email Addresses to add an email address to the block list or go to Filter Rules > Block List > Blocked Domains to add a domain.
2. Click Add... and the Add window displays.
3. Enter the Sender Email: in the form of user@example.com or Sender Domain: in the form of example.com.
4. For a domain entry, check Include Subdomains: for subdomains to also be blocked.
5. Enter any optional comments in the Comments: field.
6. Click Save.

Deleting a Block List Entry

1. To delete an individual email address or domain, click the delete  icon in the Options column to the right of the listing. To delete multiple entries at once, check the box  to the left of the listings you want to delete.
2. Click Delete... under Blocked Email Addresses or Blocked Domains.

Importing Block List Entries

1. Create a single text file containing the entries to import. Both email addresses and domains can be imported together from the same text file. The file must have one email address or domain (preceded by the '@' sign) per line. For example:
 - john@example.com
 - @example.com
2. Click Import... and select the text file to import. Click Open.
3. Email addresses will be imported to the Blocked Email Addresses and domains will be imported to the Blocked Domains.

User Allow List:

No spam checking is performed for domains or email addresses that are added to an allow list, they are automatically forwarded to the recipient.

Go to Filter Rules > Allow List to manage allow list entries.


The screenshot displays the 'User Allow List' management interface. At the top, there are tabs for 'Settings', 'Filter Rules', 'Quarantine', and 'Reporting'. Below these, a sub-menu shows 'User Block List', 'User Allow List' (which is selected), and 'Global Blocking'. The main content area is divided into two sections: 'Allowed Email Addresses' and 'Allowed Domains'. Each section has a search bar, a table with columns for 'Sender Email' or 'Sender Domain', 'Comment', 'Last Modified', and 'Options'. Both sections currently show 'No records found'. At the bottom of each section are buttons for 'Edit...', 'Delete', 'Import...', and 'Add...'.

If you Allow a particular email address or domain then all mail from that user, or that domain to your account will be passed through by the Spam Filter with no questions - even if the message were recognized as spam. In effect it will bypass the spam filters.

Adding an Allow List Entry

1. Go to Filter Rules > Allow List > Allowed Email Addresses to add an email address to the allow list or go to Filter Rules > Allow List > Allowed Domains to add a domain.
2. Enter a Sender Email: in the form of user@example.com or Sender Domain: in the form of example.com.
3. Enter Comments: as required.
4. Click Save.

Deleting an Allow List Entry

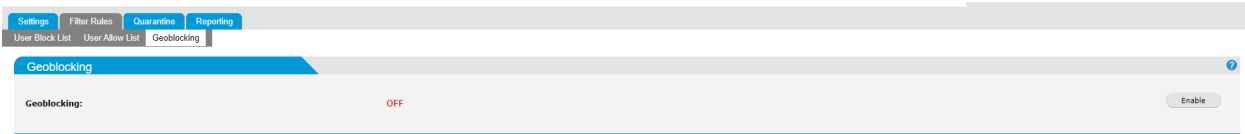
1. To delete an individual email address or domain, click the  icon in the Options column to the right of the listing. To delete multiple entries at once, check the box ☒ to the left of the listings you want to delete.
2. Click Delete... under Allowed Email Addresses or Allowed Domains.

Importing Allow List Entries

1. Create a single text file with all the entries to import. Both email addresses and domains can be imported together from the same text file. The file must have one email address or domain (preceded by the '@' sign) per line. For example:
 - o john@example.com
 - o @example.com
2. Click Import... to select the text file. Click Open.

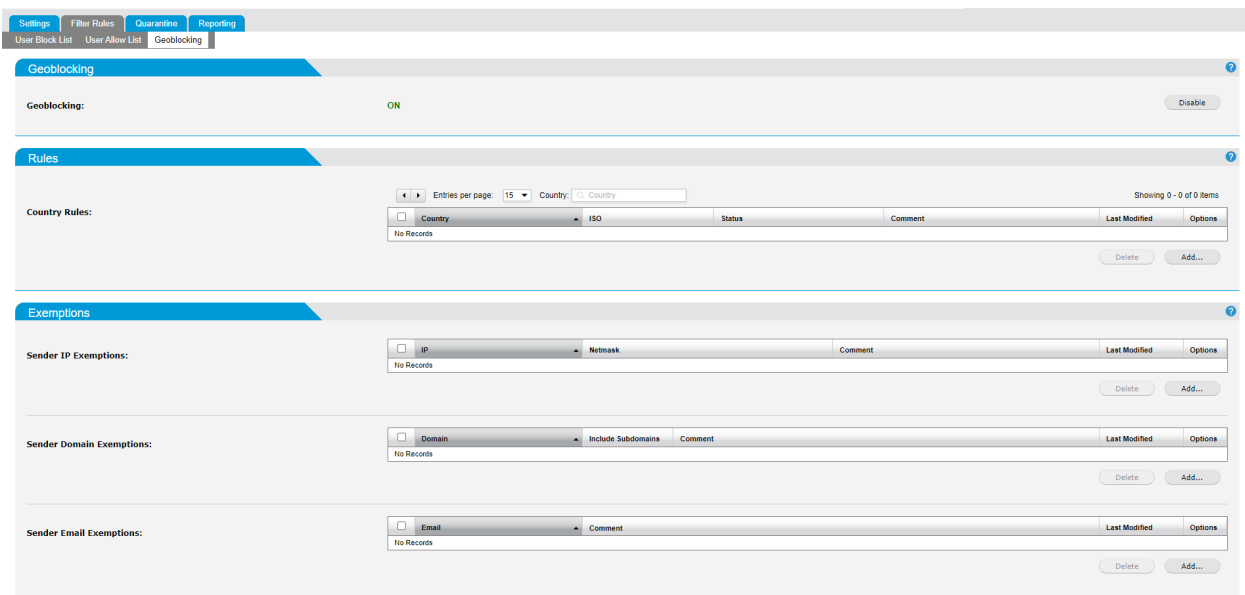
Geoblocking:

Geoblocking restricts email based on a sender's geographic location, which is identified by the sending server's IP address.





Geoblocking is off by default to turn it on click “Enable”.

Go to Filter Rules > Geoblocking and follow the steps below to add a geoblocking rule for a country.



1. Click Enable to turn Policy Based Geoblocking: ON (default: disabled).
2. Click Add... and the Add Geoblocking Rule window displays.
 - Country: Select a country to allow or block. This field auto-populates as you type.
 - Status: Select Allow or Block to allow/block the country you selected.
 - Comment: Enter an optional description of this geoblocking rule.
3. Click Save to save this geoblocking rule or cancel to discard.

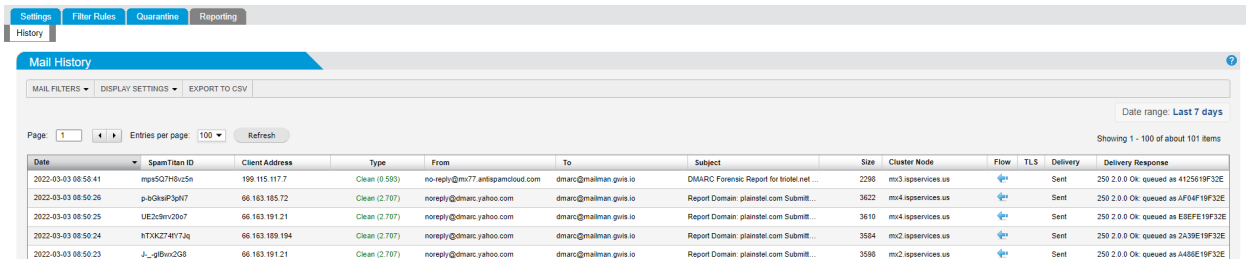
Once a geoblocking rule has been added, it can be edited or deleted. Click the edit  icon to edit a rule or click the  delete icon to delete a rule.

Mail History:

The mail filter keeps a record of all mail that it processes. This information is available in Reporting > History.

Click the Refresh button to refresh the history list.

To view mail history by date, click the Date Range button and select from the list of available options. Choose Custom Date range... to set your own date range.



The screenshot shows the 'Mail History' section of a web interface. It includes tabs for 'Settings', 'Filter Rules', 'Quarantine', and 'Reporting', with 'Reporting' selected. Below the tabs is a 'History' sub-tab. The main area displays a table of email records with columns: Date, SpamTitan ID, Client Address, Type, From, To, Subject, Size, Cluster Node, Flow, TLS, Delivery, and Delivery Response. The table shows five rows of data, all with a 'Clean' type. A 'Date range: Last 7 days' filter is applied. At the bottom, it says 'Showing 1 - 100 of about 101 items'.

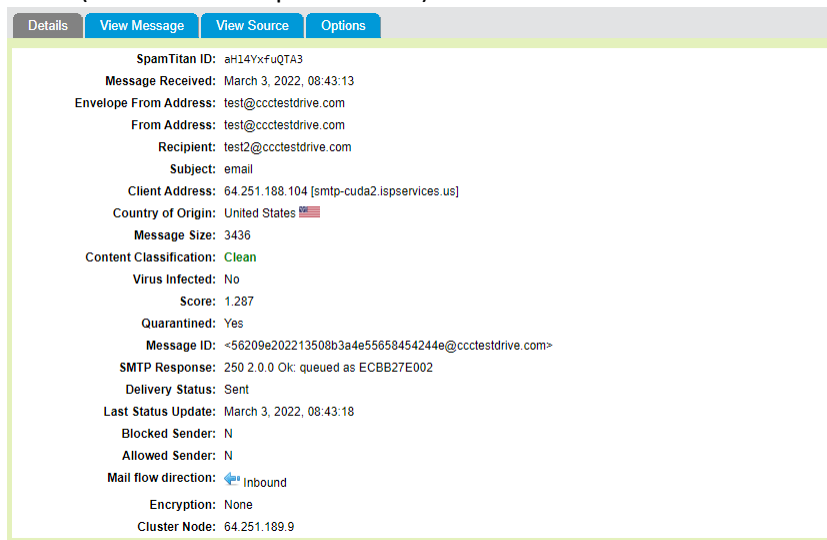
Date	SpamTitan ID	Client Address	Type	From	To	Subject	Size	Cluster Node	Flow	TLS	Delivery	Delivery Response
2022-03-03 08:50:41	mpa507H0vz5n	199.115.117.7	Clean (0.593)	no-reply@mv77.antispamcloud.com	dmarc@mailman.gvix.io	DMARC Forensic Report for biotet.net...	2298	ms3.ipservices.us	+		Sent	250 2.0.0 Ok: queued as 4125619F32E
2022-03-03 08:50:26	p-bGkaP3pA7	66.163.185.72	Clean (2.707)	noreply@dmarc.yahoo.com	dmarc@mailman.gvix.io	Report Domain: planettel.com Submitt...	3622	ms4.ipservices.us	+		Sent	250 2.0.0 Ok: queued as AF04F19F32E
2022-03-03 08:50:25	UE2c8v20o7	66.163.191.21	Clean (2.707)	noreply@dmarc.yahoo.com	dmarc@mailman.gvix.io	Report Domain: planettel.com Submitt...	3610	ms4.ipservices.us	+		Sent	250 2.0.0 Ok: queued as E8EF419F32E
2022-03-03 08:50:24	NTXKZ74Y7a	66.163.189.194	Clean (2.707)	noreply@dmarc.yahoo.com	dmarc@mailman.gvix.io	Report Domain: planettel.com Submitt...	3584	ms2.ipservices.us	+		Sent	250 2.0.0 Ok: queued as 2A39E19F32E
2022-03-03 08:50:23	J_-g8wv208	66.163.191.21	Clean (2.707)	noreply@dmarc.yahoo.com	dmarc@mailman.gvix.io	Report Domain: planettel.com Submitt...	3598	ms2.ipservices.us	+		Sent	250 2.0.0 Ok: queued as A486E19F32E

History contains the following information about each email. Click an email in the list to show more.



If a message type is clean this mail can be redelivered to the user's mailbox for a period of 30 days. This will allow the user to "restore" an email they have deleted from their inbox.

Details




- Date: date and time the email was received.
- Msg ID: a unique internal message identification number that the mail filter assigns to each email (also known as SpamTitan ID). Click to view extended details on an email:



The screenshot shows the 'Details' view of an email. It includes tabs for 'Details', 'View Message', 'View Source', and 'Options', with 'Details' selected. The details are as follows:

- SpamTitan ID: aH14YxfuQTa3
- Message Received: March 3, 2022, 08:43:13
- Envelope From Address: test@ccctestdrive.com
- From Address: test@ccctestdrive.com
- Recipient: test2@ccctestdrive.com
- Subject: email
- Client Address: 64.251.188.104 [smtp-cuda2.ipservices.us]
- Country of Origin: United States 
- Message Size: 3436
- Content Classification: Clean
- Virus Infected: No
- Score: 1.287
- Quarantined: Yes
- Message ID: <56209e202213508b3a4e55658454244e@ccctestdrive.com>
- SMTP Response: 250 2.0.0 Ok: queued as ECBB27E002
- Delivery Status: Sent
- Last Status Update: March 3, 2022, 08:43:18
- Blocked Sender: N
- Allowed Sender: N
- Mail flow direction:  Inbound
- Encryption: None
- Cluster Node: 64.251.189.9

- Client Address: source IP address a mail was received from.
- Type: message type as classified by the mail filter, e.g., Clean, Spam, RBL Reject, SPF Reject, etc.
- From: sender email address.
- To: recipient email address.
- Subject: subject header of the received message.
- Size: size of the message.

- Flow: The direction of the message (Inbound , Outbound  or Internal ).
- TLS: indicates if TLS (Transport Layer Security) was applied to the message.
- Delivery: Indicates the delivery status of a message (Sent/Deferred/Bounced).
- Delivery Response: This shows the SMTP response from the destination server. This can be useful to indicate, for example, why a remote server rejected a message.

View Message

This will show the contents of the email.

Details	View Message	View Source	Options
Date: Thu, 03 Mar 2022 08:42:01 -0700 From: test@ccctestdrive.com To: Test2 <test2@ccctestdrive.com> Subject: email Headers: Show all Headers			
1: unnamed [text/plain] 7 bytes			
sending			
2: unnamed [text/html] 202 bytes			
sending			

View Source

This shows specific header information for the email. (Useful for troubleshooting mail issues).

Details	View Message	View Source	Options
Return-Path: <test@ccctestdrive.com> Delivered-To: clean-quarantine X-Envelope-From: <test@ccctestdrive.com> X-Envelope-To: <test2@ccctestdrive.com> X-Envelope-To-Blocked: X-Quarantine-ID: <ah14YxfuQTA3> X-Span-Flag: NO X-Span-Score: 1.287 X-Span-Level: * X-Span-Status: No, score=1.287 tag=999 tag2=5 kill=5 tests=[HTML_MESSAGE=0.001, KAM_DMARC_STATUS=0.01, PYZOR_CHECK=1.085, RCVD_IN_DNSWL_LOH=0.7, SPF_HELO_NONE=0.001, SPF_PASS=0.001, TVQ_SPACE_RATIO=0.001, T_SCC_BODY_TEXT_LINE=-0.01] autolearn=no autolearn_force=no Received: from mx3.ispservices.us ([IPv6:::1]) by localhost (mx3.ispservices.us [IPv6:::1]) (amavisd-new, port 10024) with ESMTP id ah14YxfuQTA3 for <test2@ccctestdrive.com>; Thu, 3 Mar 2022 08:43:13 -0700 (HST) Received: from mx3.ispservices.us (localhost [127.0.0.1]) by mx3.ispservices.us (Postfix) with ESMTP id 38500E63C98 for <test2@ccctestdrive.com>; Thu, 3 Mar 2022 08:43:13 -0700 (HST) Authentication-Results: mx3.ispservices.us; spf=pass smtp.mailfrom=test@ccctestdrive.com smtp.helo=smtp-cuda2.ispservices.us Received-SPF: pass (ccctestdrive.com: Sender is authorized to use 'test@ccctestdrive.com' in 'mfrom' identity (mechanism 'include:_spf.ig receiver=mx3.ispservices.us; identity=mailfrom; envelope-from='test@ccctestdrive.com'; helo=smtp-cuda2.ispservices.us; client-ip=64.251.188.104 Received: from smtp-cuda2.ispservices.us (smtp-cuda2.ispservices.us [64.251.188.104]) by mx3.ispservices.us (Postfix) with ESMTPS id 8B434E63C8E for <test2@ccctestdrive.com>; Thu, 3 Mar 2022 08:43:12 -0700 (HST) X-ASG-Debug-ID: 164632122-13e521172e141700001-qa4y9f Received: from smtpfarm-node2.gwis.io (smtpfarm-node2.gwis.io [64.251.188.97]) by smtp-cuda2.ispservices.us with ESMTP id e0E X-Barracuda-Envelope-From: test@ccctestdrive.com X-Barracuda-Effective-Source-IP: smtpfarm-node2.gwis.io[64.251.188.97] X-Barracuda-Apparent-Source-IP: 64.251.188.97 Received: from webmail.ccctestdrive.com (webmail-node1.gwis.io [64.251.188.194]) (Authenticated sender: test@ccctestdrive.com) by smtpfarm-node2.gwis.io (Postfix) with ESMTPA id 00DA78012B for <test2@ccctestdrive.com>; Thu, 3 Mar 2022 08:42:02 -0700 (HST) MIME-Version: 1.0 Date: Thu, 03 Mar 2022 08:42:01 -0700 From: test@ccctestdrive.com To: Test2 <test2@ccctestdrive.com>			

Options

Details

View Message

View Source

Options

[Release](#) message to recipient (test2@ccctestdrive.com)
[Allow](#) envelope Sender (test@ccctestdrive.com) and Release Message to recipient (test2@ccctestdrive.com)
[Delete](#) message
[Mark message as Spam](#)

- Release: Delivers the mail to the inbox, mail can be redelivered to the user's mailbox for a period of 30 days.
- Allow: Adds the email sender to you allow list and delivers the mail to the inbox.
- Delete: Removes the message from the filter.
- Mark message as spam: Marks the message in the filter as spam.

Modifying Mail History Display Settings

Go to Reporting > History > Display Settings to control what columns are displayed in your Mail History.

MAIL FILTERS ▾	DISPLAY SETTINGS ▾	EXPORT TO CSV
<input checked="" type="checkbox"/> Show Message Subject	<input checked="" type="checkbox"/> Show Virus name for Virus Messages	<input checked="" type="checkbox"/> Show TLS encryption status
<input checked="" type="checkbox"/> Show Score for Clean Messages	<input checked="" type="checkbox"/> Show Scanner that detected Virus	<input checked="" type="checkbox"/> Show delivery status
<input checked="" type="checkbox"/> Show Score for Spam Messages	<input checked="" type="checkbox"/> Show Message Flow	<input checked="" type="checkbox"/> Show delivery response
		<input type="checkbox"/> Show RBL name
		<input type="checkbox"/> Only show messages for local cluster node
		<input type="checkbox"/> Show Cluster node column

Important

As the mail filter runs over multiple systems, it is recommended to un-check 'only show messages from local cluster node'. Otherwise, you may only see 30% of your mail reported.

- The following Display Settings can be checked or unchecked:
- Show Message Subject: Display the subject of the message.
- Show Score for Clean Messages: If enabled, the score assigned by the mail filter will be displayed in the Type column of the history view for messages classified as Clean.
- Show Score for Spam Messages: If enabled, the score assigned by the mail filter will be displayed in the Type column of the history view for messages classified as Spam.
- Show Virus name for Virus Messages: If enabled, then the name of the virus that the virus scanner detected will be displayed in the Type column of the history view for virus messages.
- Show Scanner that detected Virus: If enabled, then the name(s) of the virus scanner(s) that detected the virus will be display in the Type column of the history view for virus messages.
- Show Message Flow: Show in which direction the Message is coming from and going to.

- Show TLS encryption status: Show the status of the Transport Layer Security (TLS).
- Show delivery status: Show Delivery Status of the message.
- Show delivery response: Show SMTP response from destination server.
- Show RBL name: Show the name of the RBL that blocked the message.
- Only show messages for local cluster node: Clicking this option will mean that only messages for the local cluster node are displayed (see Important note above).
- Show Cluster node column: This will enable the user to see a cluster node column on the table displayed.