GTS Email Security Admin Portal - High Level Overview

Jason Molaison - 2025-07-26 - General Support

This article will give you a high level overview of the GTS Email Security Admin Portal.

Within the Admin Center tab, some useful functions are below:

VIP List

- Here you can add the names and email addresses of high level executives within your organization that may be targeted in impersonation scams. For example, someone in accounting may receive an email from what looks like the COO requesting to pay an invoice or change wire details. With this feature enabled, those messages will be flagged.

Allow List

- Here you can enter company-wide entries, either individual email addresses, or domains to be excluded. Within the Result Type pull down menu, you can choose which filter should be bypassed, or you can select “Do not warn about any threats”. Use caution when adding entries here, as it can allow malicious messages to bypass the intended security checks. It is recommended that you always leave the check mark “Apply only to messages that pass DMARC authentication”. Note that this will be in addition to any user-level entries.

Block List

- Here you can enter company-wide entries, either individual email addresses, or domains to be blocked. Within the Result Type pull down menu, you can designate how the message will be classified. You can also utilize the “Apply only to messages that fail DMARC authentication” to target spoofed messages. Note that this will be in addition to any user-level entries.

Tools

- With the Link Decoder, you can paste a rewritten link to obtain the original URL.
- The Microsoft 365 Message Trace is useful when trying to locate a missing message. Not only will it show results of messages that have been quarantined, but will also display details of messages that were moved using a user level mail processing rule within the mail client.

Under the Analysis Pull Down, some useful functions are below:

Observations

- Within this section, you can view the details of all processed messages. By clicking the filter icon in the upper left corner, you can drill down into various aspects of the messages.

Threat Level

- This provides an overview of the messages received over a period of time (default is 10 days), and gives insight on how the messages were classified. You can click on the Threat Level to see the message details

Quarantine

- In this section, any messages that were quarantined will be listed. If the message was incorrectly quarantined, it can be released by clicking on the message, then click “Preview” and finally “Release From Quarantine”. Use extreme caution when releasing these messages