Allow/block domains and emails

Allowlists provide the ability to include known safe email sender addresses and domains that Coro can check if an *Email Security* event occurs. For instance, if an email is flagged by Coro's detection mechanisms as containing potentially malicious content or a possible phishing attack, Coro will continue to allow the email if the sender or sender's domain is listed in an allowlist.

Blocklists can be used to provide lists of known bad senders or domains where, regardless of content or authentication status, corresponding emails are blocked from being received by the named recipients. Coro raises tickets identifying the blocked event.

List types

Coro provides two primary allowlist and blocklist types applicable to your workspace (and optionally also to child workspaces generated by this workspace owner, where relevant):

Type	Description
Suspicious content	An allowlist and blocklist relating to checks on email content. Records added here (through ticket remediation or manual entry on this page) feed into remediation decisions concerning the content of emails sent to your protected and protectable users. Future remediation decisions based on positive detector tests take into account whether the sender or domain is in this list.
Authentication failure	An allowlist and blocklist for authentication failure conditions with the specified sender or sender's domain. Authentication is performed on the sender details to establish the legitimacy of their identity, primarily by checking message headers to determine the possibility of spoofing or impersonation. Records added here (through ticket remediation or manual entry on this page) feed into remediation decisions concerning detectors that are triggered by authentication failures.