Downloading suspicious emails for further inspection

Several email phishing type tickets have an additional action enabling you to download the suspicious email (in .eml format). This allows you to directly examine potentially malicious emails before taking any further action. This download action applies to both open and closed tickets.

> **Warning**
>
> Make sure that you download suspicious .eml files to a secure and isolated network segment to prevent any disruption to your other services.

A .eml file is an email message saved by an email application, such as Microsoft Outlook or Apple Mail. It contains the content of the message, along with the subject, sender, recipient(s), and date of the message. .eml files may also store one or more email attachments, which are files sent with the message.

You can open .eml files with:

- Email programs, such as Microsoft Outlook, Apple Mail, and Mozilla Thunderbird.
- Web browsers, including Google Chrome, Microsoft Edge, and Internet Explorer.
- Plain text editor, such as Microsoft Notepad, and Apple TextEdit.
- Word processors such as Microsoft Word.

Downloading suspicious emails in .eml format

To download a potentially malicious email in .eml format:

1. **Log into the Coro console** and select **Ticket Log** from the toolbar:

2. From the **Type** filter, select any one of the **Email Security** ticket types pertaining to phishing detectors. For a complete list of ticket types and outcomes, see **Email Security ticket types**.