

ESA FAQ: How to submit email messages to Cisco

Contents

[Introduction](#)

[What types of email messages can be submitted to Cisco?](#)

[Why submit email messages to Cisco?](#)

[How to submit email messages to Cisco](#)

[Cisco Email Security Plug-in](#)

[Cisco Email Submission and Tracking Portal](#)

[Direct Email Submission](#)

[Microsoft Outlook 2010, 2013, or 2016 for Windows](#)

[Microsoft Outlook Web App, Microsoft Office 365](#)

[Microsoft Outlook 2011 and Microsoft Outlook 2016 for Mac \(OS X, macOS\)](#)

[Mail \(OS X, macOS\)](#)

[Mozilla Thunderbird](#)

[Mobile Platforms \(iPhone, Android, etc\)](#)

[How to verify submissions to Cisco](#)

[Direct Email Submission](#)

[Email Submission and Tracking Portal](#)

[Related Information](#)

Introduction

This document describes how an end-user may submit email messages pertaining to Spam, Ham, or Marketing to Cisco for support, troubleshooting, or additional examination.

What types of email messages can be submitted to Cisco?

Generally speaking, Spam, Ham, and Marketing email messages are defined as:

- *Spam*: Irrelevant or inappropriate email message(s) to a recipient.
- *Ham*: An email message that is not Spam. Or, "non-spam", "good mail".
- *Marketing*: Directly marketing a commercial email message.

Cisco will accept submissions for any email that is classified incorrectly. This consists of the following:

- false negative (missed Spam)
- false positive (or "Ham")
- false negative marketing messages
- false positive marketing messages
- phish-suspected messages

Why submit email messages to Cisco?

Submitting missed Spam or incorrectly marked Spam email messages will assist Cisco confirm the content of email messages. This also assists in IronPort Anti-Spam (IPAS) efficacy and scoring.

How to submit email messages to Cisco

Supported methods for submitting email messages to Cisco are:

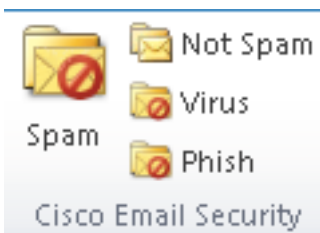
1. Cisco Email Security Plug-In
2. [Cisco Email Submission and Tracking Portal](#) (via the [Cisco SecurityHub](#))
3. Direct email submission from the end-user

Cisco Email Security Plug-in

Note: You may download the Cisco Email Security Plug-In from the [Cisco Email Security Appliance Download Software](#) page. This requires an active Cisco Connection Online (CCO) ID that is associated to an active contract.

The Cisco Email Security Plug-in is available ONLY for Microsoft Outlook on Windows. To check if you have installed a version of the Cisco Email Security Plug-in, with Microsoft Outlook open, click **File > Options > Add-Ins**. If you see Cisco IronPort Email Security Plug-In, or similar, then you have the Cisco Email Security Plug-in installed. If you do not, then please download the Plug-In from the URL provided above.

Example of the Cisco Email Security Plug-In installed, as seen from the Microsoft Outlook ribbon:



Note: Older versions of the Plug-in are named "IronPort Email Security Plug-in" or "Encryption Plug-in for Outlook". This would be seen in versions 7.6 and older for the Plug-in. This version of the Plug-in contained both Reporting and Encryption together. Starting in 2017, Cisco separated the services and released two new versions of the Plug-in, "Email Reporting Plugin for Outlook" and the "Email Encryption Plugin for Outlook". These were available with a 1.0.0.x version.

Cisco Email Submission and Tracking Portal

Please review the following articles to assist with the Cisco Email Submission and Tracking Portal:

- [ESA FAQ: How to work with Cisco Email Submission and Tracking Portal](#)
- [ESA FAQ: Troubleshooting Email Submission and Tracking Portal](#)

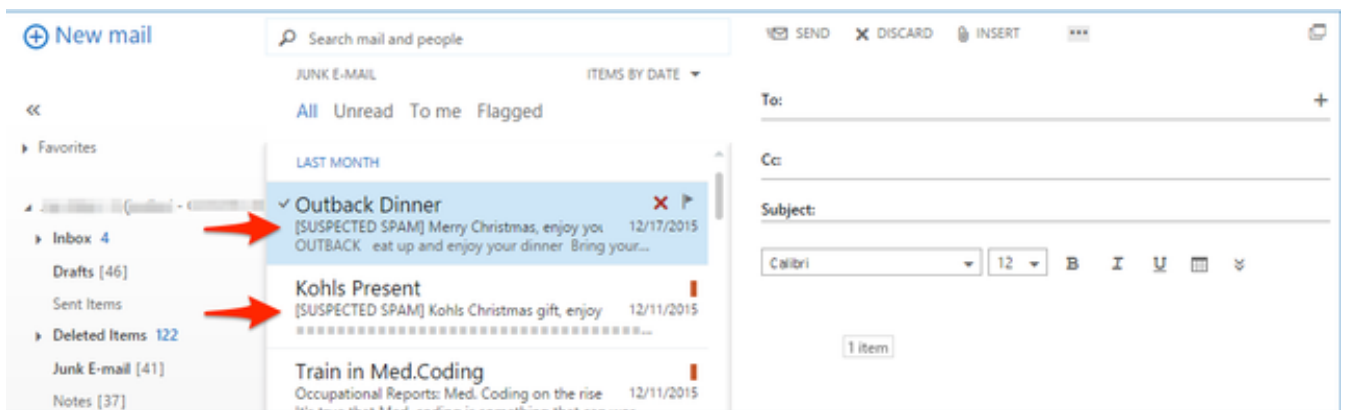
Direct Email Submission

Please follow the instructions for your email client below in order to attach the email as an [RFC 822](#) Multipurpose Internet Mail Extension (MIME)-encoded attachment. If your email client is not provided as an example below, please refer direct to the email client user guide or support help, and confirm that it will support "Forwarding as Attachment."

Submissions should be sent to the email address that is appropriate:

spam@access.ironport.com	Subject line may be pre-pended as [SUSPECTED SPAM], the end-user considers the email message spam.
ham@access.ironport.com	Subject line may be pre-pended as [SUSPECTED SPAM] or the subject line may also contain additional tagging, the end-user DOES NOT consider the email message as spam.
ads@access.ironport.com	Untagged subject line, the end-user may consider the email message to be marketing content.
not_ads@access.ironport.com	Subject line may be pre-pended as [MARKETING], the end-user DOES NOT consider the email message to be marketing.
phish@access.ironport.com	Untagged subject line, but the email message appears to be phishing (designed to acquire user name(s), passwords, credit card info, or other personally identifiable information), or the email message contains malware attachments.

Example of tagged subject lines:



Warning: Simply forwarding an email message does not retain the order of the mail routing headers, and also removes important mail routing headers which are required to attribute the origination of the email.

Email submissions can be made through any of the following clients:

- Microsoft Outlook 2010, 2013, or 2016 for Windows
- Microsoft Outlook Web App, Microsoft Office 365
- Microsoft Outlook 2011 and Microsoft Outlook 2016 for Mac (OS X, macOS)
- Mail (OS X, macOS)
- Mozilla Thunderbird
- Mobile Platforms (iPhone, Android, etc)

Microsoft Outlook 2010, 2013, or 2016 for Windows

- The preferred submission method from Microsoft Outlook on Windows is to use the [Cisco Email Security Plug-In](#). As noted, simply forwarding an email message does not retain the order of the mail routing headers, and also removes important mail routing headers which are required to attribute the origination of the email.

Note: If you prefer not to install the Cisco Email Security Plug-In, you can use the Microsoft Outlook Web App, Microsoft Office 365 instructions below (if your company provides use of Microsoft Office Online).

Microsoft Outlook Web App, Microsoft Office 365

1. Open your mailbox in Microsoft Outlook Web App.
2. Select the message that you want to submit.
3. Click "New mail" at the top left.
4. Drag the message you are submitting over, and drop as an attachment into the new message.
5. Send the email message to the respective address as described above.

Microsoft Outlook 2011 and Microsoft Outlook 2016 for Mac (OS X, macOS)

1. Select the message in the message pane.
2. Click the Attachment button.
3. Forward the message on to the respective address listed in the Outlook Web App instructions below.

Mail (OS X, macOS)

1. Right click on the email message itself and choose **Forward as Attachment**.
2. Forward the email message to the respective address as described above.

Mozilla Thunderbird

1. Right click on the email message itself and choose **Forward As > Attachment**.
2. Forward the email message to the respective address as described above.

Note: [MailSentry IronPort Spam Reporter](#) is a third-party plug-in that is available for Mozilla Thunderbird that takes the same action as described above, but does so by providing a "Spam/Ham" button. *This is not a supported plug-in from Cisco.

Mobile Platforms (iPhone, Android, etc)

- If your mobile platform does not have a method to forward the original email as an attachment, you will need to wait until you have access to one of the other methods above, prior to submitting.

How to verify submissions to Cisco

Direct Email Submission

No confirmation or notice of receipt for submissions will be provided to the end-user for direct email submissions to Cisco.

Email Submission and Tracking Portal

Once a submission is successfully completed on the Email Submission and Tracking Portal, an email confirmation is sent with a Submission ID and other details.

Example of email confirmation:

EMAIL SUBMISSION AND TRACKING PORTAL

New Spam Submission Processed

Submission ID: cidG50057a3fb1357395a7464ca4babc8ca0
Subject: カレンダー (は Centre d'aide sólo en inglés) ná o 法使用用
Submitter: SubmissionPortal@cisco.com

[Track on Portal →](#)

This email is typically received within 2 hours. If it is not received then it means that the submission was not done correctly. You may wish to recheck your Submissions tab on the portal for further information.

Related Information

- [Track your submissions using Email Submission and Tracking Portal](#)
- [Troubleshooting Email Submission and Tracking Portal](#)