



User Guide for Cisco Secure Email Submission Add-In



Published: March 24, 2022

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL:

<https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

Contents

Chapter 1: Getting Started	4
Supported Configurations.....	4
Related Documents	4
Cisco End User License Agreement.....	5
Chapter 2: Installing and Managing the Cisco Secure Email Submission Add-In.....	6
Installing the Cisco Secure Email Submission Add-In	6
Modifying the Cisco Secure Email Submission Add-In Settings	7
Uninstalling the Cisco Secure Email Submission Add-In	8
Chapter 3: Submitting Messages Using the Cisco Secure Email Submission Add-In	10
When to Submit a Message to Cisco	10
Submitting Messages Using the Cisco Secure Email Submission Add-In	11
Submitting Simulated Phishing Messages Using the Cisco Secure Email Submission Add-In	12
Submitting Messages to Additional Email Addresses Using the Cisco Secure Email Submission Add-In	12
Chapter 4: Troubleshooting the Cisco Secure Email Submission Add-In.....	14
Unable to Submit Large Messages	14
Unable to Change the Submission Message Format	14

Chapter 1: Getting Started

The Cisco Secure Email Submission add-in allows you to submit feedback to Cisco about unsolicited and unwanted messages such as spam/phish/virus, marketing messages, and legitimate messages that were incorrectly filtered out. We use this feedback to update our filters to stop unwanted messages from getting delivered to your mailbox. You can track your submissions by logging in to the Cisco Talos Email Status Portal (https://talosintelligence.com/email_status_portal).

Supported Configurations

Microsoft Office Variant		Supported Outlook Versions
Certified	Microsoft 365 Apps for Enterprise	1701 or later
	Office Professional Plus 2019 or Office Standard 2019	1808 or later
	Outlook Web App	The latest versions of Microsoft Edge (on Windows), Google Chrome, Mozilla Firefox, and Safari (on macOS)
Compatible	Office Professional Plus 2016 (MSI) or Office Standard 2016 (MSI)	16.0.4494.1000 or later
	Office 2016 for Mac	16.0.9318.1000 or later

Note: You can install the Cisco Secure Email Submission add-in only if you are using an Office 365/Microsoft 365 subscription.

Related Documents

If you are an email administrator, we recommend that you review the following resources:

Resource	Location
Cisco Talos Email Status Portal Help Center	https://talosintelligence.com/tickets/email_submissions/help
How to Submit Email Messages to Cisco	https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214133-how-to-submit-email-messages-to-cisco.html
Publish Office Add-Ins Using Centralized Deployment via the Microsoft 365 Admin Center	https://docs.microsoft.com/en-us/office/dev/add-ins/publish/centralized-deployment

Cisco End User License Agreement

For information about the Cisco End User License Agreement, see

https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html.

Chapter 2: Installing and Managing the Cisco Secure Email Submission Add-In

Install and configure the Cisco Secure Email Submission add-in on your Microsoft Outlook to submit incorrectly classified messages to Cisco.

Note: If your administrator uses Centralized Deployment to publish the Cisco Secure Email Submission add-in, you may already have the add-in in your Outlook. In this scenario, skip the installation process.

Installing the Cisco Secure Email Submission Add-In

Before You Begin

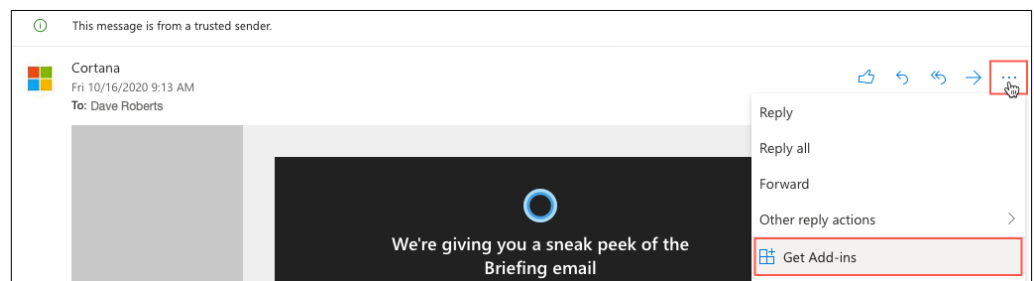
- Review the [Supported Configurations](#) topic.
- Obtain the add-in manifest file. Do one of the following:
 - If you have a Cisco Account, download the manifest file from the Cisco Software Download page (<https://software.cisco.com/download/home>).
 - If you do not have a Cisco Account, obtain the manifest file from your administrator.
- Check whether your Outlook client is installed using Microsoft Store. If you have installed the Outlook client using Microsoft Store, you may not find an option to install custom add-ins. Install the Cisco Secure Email Submission add-in using Outlook Web App in this scenario.

Procedure

Step 1. Open the Add-Ins for Outlook page from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:

- On Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Get Add-ins**.

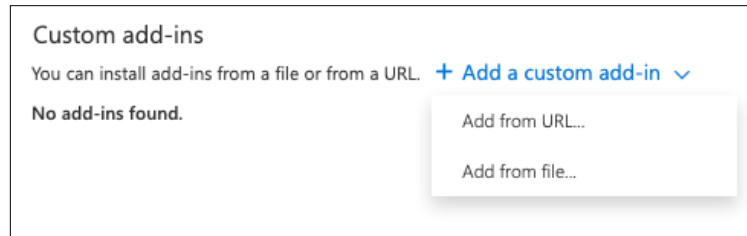


- On Outlook for Windows or macOS, click **Get Add-ins** from the Ribbon.

Note: If the **Get Add-ins** button is not available on your Outlook for macOS, log in to the Outlook Web App to complete this task.

Step 2. Click **My add-ins**.

Step 3. Under **Custom add-ins**, install the Cisco Secure Email Submission add-in from a manifest file or a URL.



Step 4. Follow the on-screen instructions to complete the installation process.

Step 5. (Optional) If you cannot view the add-in after performing Step 4, relaunch Outlook for Office 365/Microsoft 365 or Outlook Web App.

For detailed instructions about installing add-ins, see the Microsoft Office documentation.

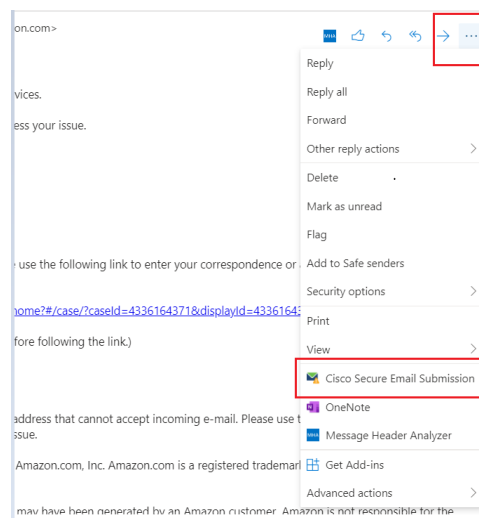
Modifying the Cisco Secure Email Submission Add-In Settings

Procedure

Step 1. Open the Cisco Secure Email Submission add-in from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:

- On Outlook Web App, after you select a message, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Submission**.



- On Outlook for Windows or macOS, click **Submit Messages** from the Ribbon.

Step 2. Click the settings (⚙️) icon.

Step 3. Adjust the following options as needed:

Option	Description
Keep a Copy of the Submission	Select this option to retain a copy of your submission in your Sent folder.
Message Format of the Submission	Select one of the following message formats: <ul style="list-style-type: none"> Encrypted – the report is encrypted before sending. Plain – the report is sent without encryption. Note: Currently, only the plain format is supported.
Message Subject	Modify the message subject of your submission.

Step 4. Click **Apply**.

Note: Click **Reset** to change the settings to the default settings.

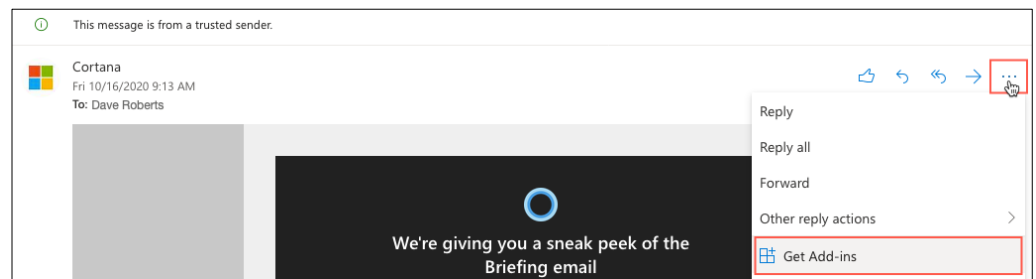
Uninstalling the Cisco Secure Email Submission Add-In

Procedure

Step 1. Open the Add-Ins for Outlook page from your Outlook for Office 365/Microsoft 365 or Outlook Web App.

Do one of the following:

- On Outlook Web App, after selecting a message, click the ellipsis icon in the Reading pane, and click **Get Add-ins**.




- On Outlook for Windows or macOS, click **Get Add-ins** from the Ribbon.

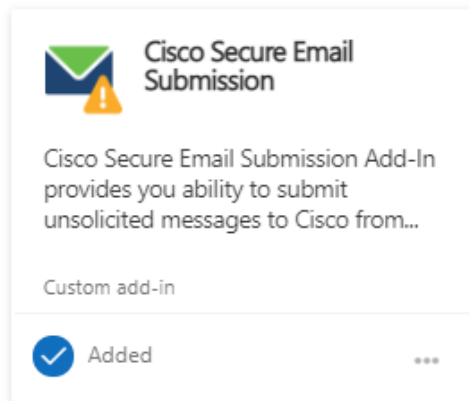
Note: If the **Get Add-ins** button is not available on your Outlook for macOS, log in to the Outlook Web App to complete this task.

Step 2. Click **My add-ins**.

Under **Custom add-ins**, click the ellipsis icon in the Cisco Secure Email Submission add-in, and click **Remove**.

Custom add-ins

You can install add-ins from a file or from a URL. [+ Add a custom add-in](#) 



For detailed instructions about uninstalling add-ins, see the Microsoft Office documentation.

Note: The Cisco Secure Email Submission add-in settings are stored in your Office 365/Microsoft 365 account and are retained for as long as your account is active. These settings are not deleted when you uninstall the add-in. Therefore, the old settings are applied again when you reinstall the Cisco Secure Email Submission add-in for the same Office 365/Microsoft 365 account.

Chapter 3: Submitting Messages Using the Cisco Secure Email Submission Add-In

We recommend that you submit unsolicited and unwanted messages such as spam, viruses, phishing, marketing messages, and legitimate messages that were incorrectly filtered out.

When to Submit a Message to Cisco

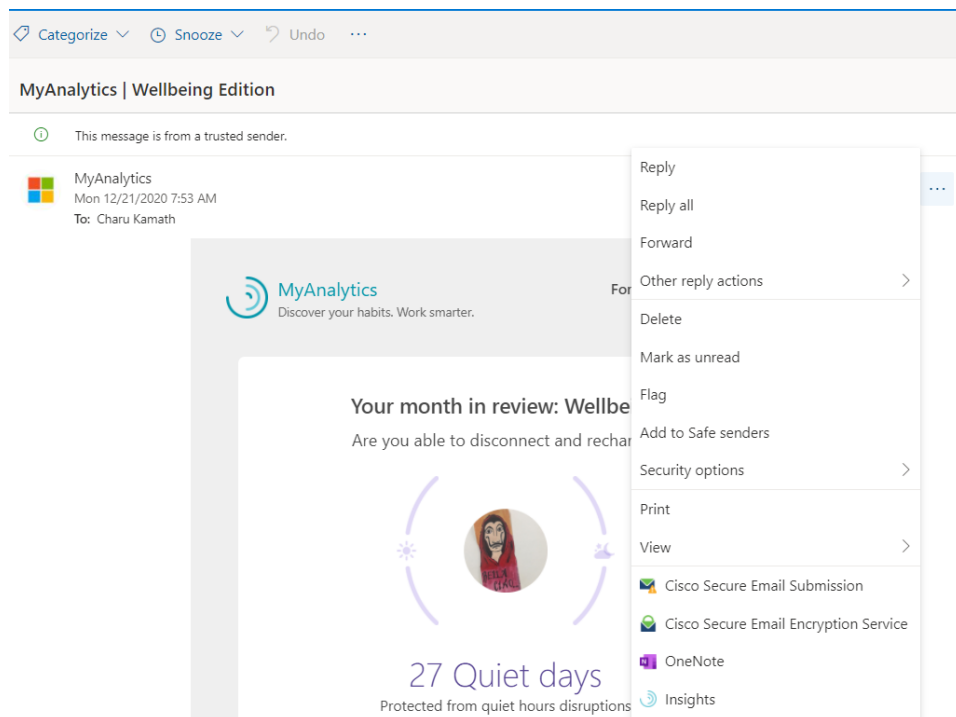
The following table shows various categories of messages and when to submit such messages to Cisco:

Category	Definition	When to Submit a Message
Spam/Phish/Virus	Messages that are unsolicited and undesired and are often sent out in bulk to an indiscriminate recipient list. Typically, spam is sent for commercial purposes. Messages that are unsolicited and undesired and may be malicious (virus, malware, scams, and so on). Messages and/or attachments that contain virus.	Delivered to your Inbox, but you consider the message as spam/phish/virus.
Marketing	Advertising messages that are sent by professional marketing groups. These messages were of use at some point in time but have diminished in value to the point where you no longer want to receive them.	Delivered to your Inbox, and not detected as marketing.
Legitimate	Legitimate (good) message, not spam. Also known as 'Ham.'	Detected as spam, but you consider the message as legitimate.

Submitting Messages Using the Cisco Secure Email Submission Add-In

Procedure

- Step 1. On your Outlook for Office 365/Microsoft 365 or Outlook Web App, select the message that you want to submit to Cisco.
- Step 2. Open the Cisco Secure Email Submission add-in.
Do one of the following:
 - On Outlook Web App, click the ellipsis icon in the Reading pane, and click **Cisco Secure Email Submission**.



- On Outlook for Windows or macOS, click the **Submit Messages** icon in the Ribbon.
- Step 3. On the Cisco Secure Email Submission add-in pane, click one of the following categories that is appropriate for the selected message:
 - Report as Spam/Phish/Virus
 - Report as Legitimate
 - Report as Marketing

Note: Keep in mind that:

- When you submit a message as spam or marketing, that message is automatically moved to the Junk folder.

- When you submit a message as legitimate, that message is automatically moved to Inbox.

After you submit a message, track the status of your submission by logging in to the Cisco Talos Email Status Portal (https://talosintelligence.com/email_status_portal). For more information, see [How to Submit Email Messages to Cisco](#).

Note: After you submit a message, the add-in pane closes automatically. To keep the add-in pane open, pin the add-in pane by clicking the pin (📌) icon.

Submitting Simulated Phishing Messages Using the Cisco Secure Email Submission Add-In

Cisco Secure Email Submission Add-In supports submission of simulated phishing messages sent through the Cisco Secure Awareness (CSA) cloud service portal. You can now submit the simulated phishing messages using the Secure Email Submission Add-In itself.

To submit a simulated phishing message, follow the procedure described in the previous section.


Tracking the message after you submit it aligns with the existing behavior of the CSAT portal. Only the CSA admin has access to that information.

Submitting Messages to Additional Email Addresses Using the Cisco Secure Email Submission Add-In

You can add an additional email address to submit your messages to another email address. However, this is optional.

Procedure

- Step 1. On your Outlook for Office 365/Microsoft 365 or Outlook Web App, select the message that you want to submit to Cisco.
- Step 2. Open the Cisco Secure Email Submission add-in.
- Step 3. Click the **Settings** (⚙️) icon.
- Step 4. (Optional) Check the **Add email address** checkbox.

Cisco Secure Email Submission 

Message Format of the Submission

☐ Encrypted ☒ Plain

Message Subject

Modify Email Addresses

Spam Messages

Default email address: spam@access.ironport.com

☐ Add email address

Legitimate Messages

Default email address: ham@access.ironport.com

☐ Add email address

Marketing Messages

Default email address: ads@access.ironport.com

☐ Add email address

Step 5. Enter the email address of the user you want to receive the email in the text box.

Step 6. Click **Apply**.

Chapter 4: Troubleshooting the Cisco Secure Email Submission Add-In

Unable to Submit Large Messages

You are unable to submit messages that are larger than 1 MB.

Reason

You cannot submit messages that are larger than 1 MB. This is a known limitation (Defect ID: CSCvv40345).

Solution

If you have large attachments in your message, consider removing them before submitting the message.

Unable to Change the Submission Message Format

You are unable to change the format of the submission message in the Settings tab.

Reason

In this release, you cannot change the format of the submission message. This is a known limitation (Defect ID: CSCvw30701).

Solution

None



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)