



# User Guide for Cisco Secure Email Submission Add-In



**Published:** May 30, 2025

## **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](http://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)

© 2025 Cisco Systems, Inc. All rights reserved.

---

# Contents

<b>Chapter 1: Getting Started .....</b>	<b>4</b>
Supported Configurations.....	4
Related Documents .....	4
Cisco End User License Agreement.....	4
<b>Chapter 2: Installing and Managing the Cisco Secure Email Submission Add-In.....</b>	<b>5</b>
Installing the Cisco Secure Email Submission Add-In .....	5
Modifying the Cisco Secure Email Submission Add-In Settings .....	10
Uninstalling the Cisco Secure Email Submission Add-In .....	11
<b>Chapter 3: Submitting Messages Using the Cisco Secure Email Submission Add-In .....</b>	<b>13</b>
When to Submit a Message to Cisco .....	13
Submitting Messages Using the Cisco Secure Email Submission Add-In .....	14
Reporting Messages Using the Secure Email Submission Add-In .....	17
Submitting Simulated Phishing Messages Using the Cisco Secure Email Submission Add-In .....	18
Submitting Messages to Additional Email Addresses Using the Cisco Secure Email Submission Add-In .....	18
<b>Chapter 4: Customizing the Secure Email Service Submission Add-In Branding.....</b>	<b>20</b>
<b>Chapter 5: Troubleshooting the Cisco Secure Email Submission Add-In.....</b>	<b>22</b>
Email Submission Add-In becomes unresponsive when user tries to report messages .....	22
Unable to Change the Submission Message Format .....	23
Granting Consent Using Entra Admin Center.....	23

# 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](https://talosintelligence.com/email_status_portal)).

## Supported Configurations

Microsoft Office Variant	
Certified	Microsoft 365 Apps for Enterprise
	Outlook Web App (on the latest version of Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari.)

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

## 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](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.

## 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 (addin-10.0.0-100) from the Cisco Software Download page (<https://software.cisco.com/download/home>). If you are not able to download the manifest file, please contact Cisco Support to obtain the manifest file.
  - If you do not have a Cisco Account, please contact Cisco Support to obtain the manifest file.
- 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.
- For Centralized Deployment, you must remove the old manifest file before uploading the new one. For Standalone Deployment, upload the new manifest file directly to replace the old one.
- If you have an O365 Exchange Online account, you must provide consent using the admin consent URL before deployment to enable the Secure Email Submission Add-In to report incorrectly filtered messages. See [Providing consent using the admin URL](#) for more details.

The email administrator can install the Secure Email Submission Add-In in two ways:

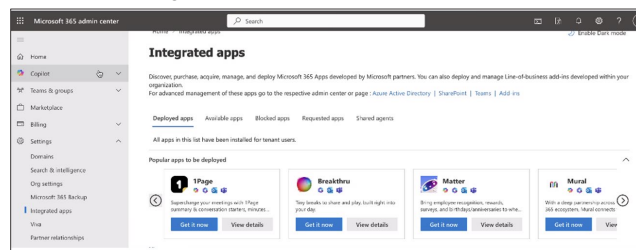
1. [Centralized Deployment](#) (through the Microsoft Admin Center)
2. [Standalone Deployment](#)

**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.

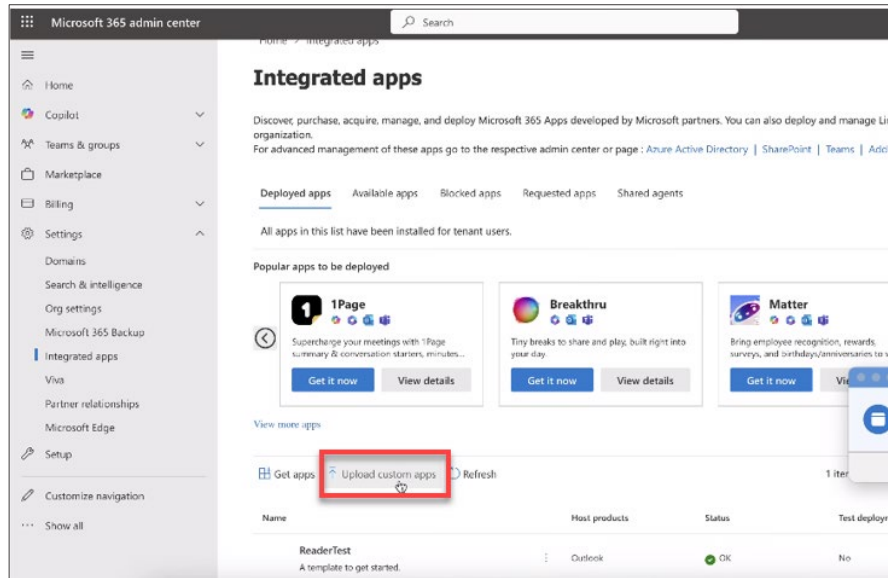
### *Centralized Deployment*

Step 1. Log in to <https://admin.microsoft.com/>.

Step 2. Search for Integrated apps.



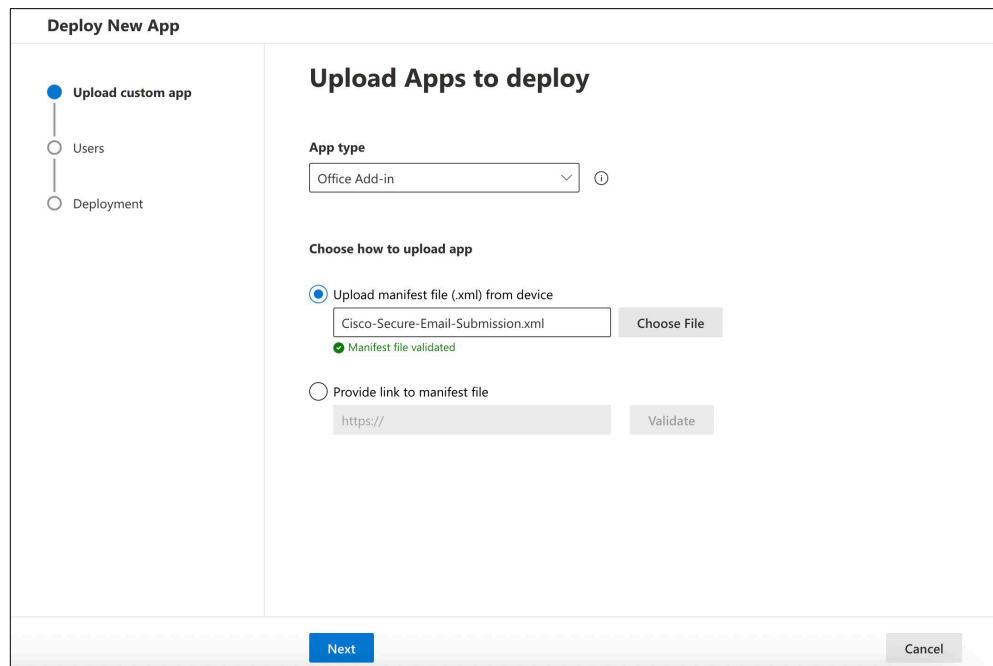
Step 3. Select **Upload custom app** in the Integrated apps page.



Step 4. Select Office Add-in from the **App type** drop-down list.

Step 5. Select **Upload manifest file (.xml) from device** option and upload a manifest file by clicking the **Choose File** button.

Step 6. Click **Next**.



Step 7. Select an option under **Assign users** to add a user.

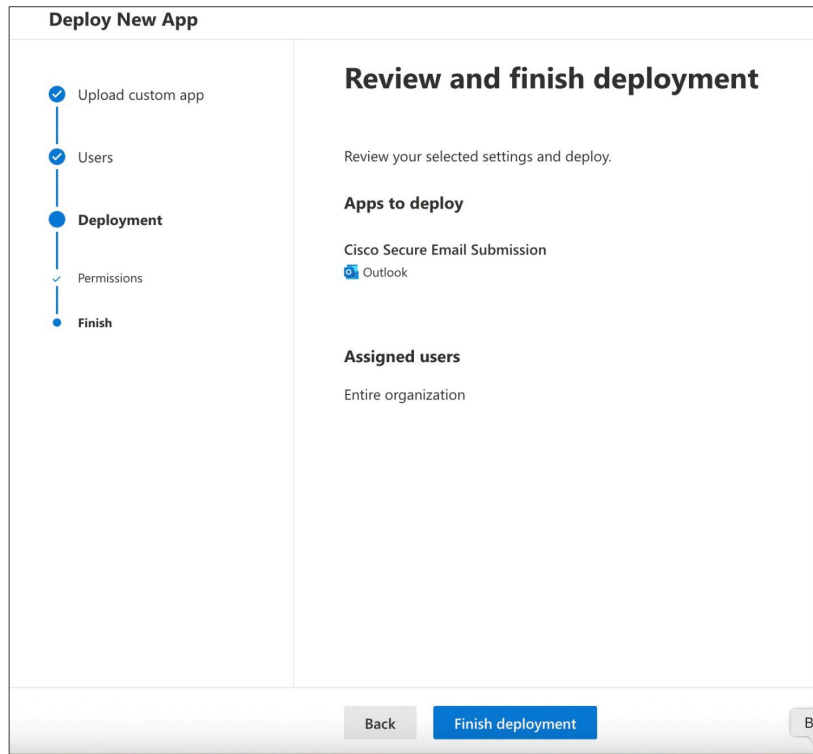
The screenshot shows the 'Deploy New App' wizard in the 'Add users' step. On the left, a progress bar indicates the current step: 'Upload custom app' (checked), 'Users' (checked), 'Deployment' (selected), and 'Permissions' (unchecked). The main content area is titled 'Add users' and features the app icon 'Cisco Secure Email Submission'. Under the 'Assign users' section, there are three radio button options: 'Just me (a.onmicrosoft.com)' (unchecked), 'Entire organization' (checked), and 'Specific users/groups' (unchecked). Below these options is a search input field labeled 'Search for users or grou...'. At the bottom of the wizard, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

Step 8. Click **Next**.

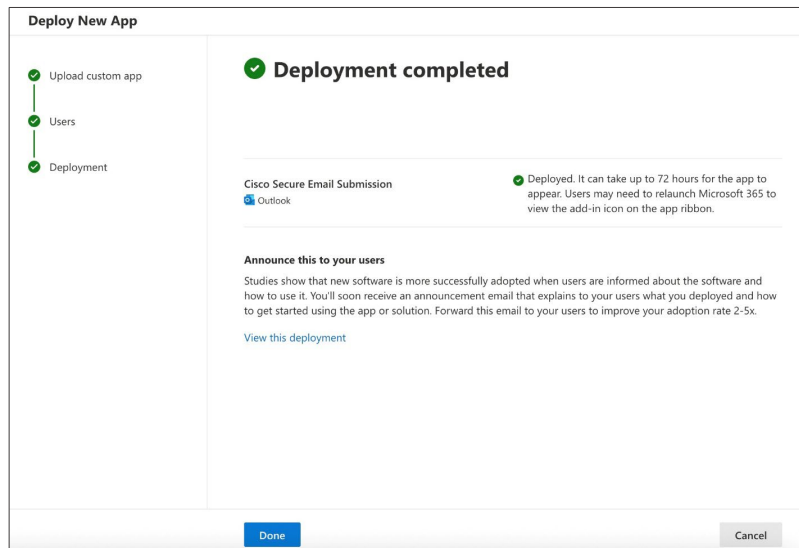
Step 9. Accept Permissions.

The screenshot shows the 'Accept permissions requests' screen. On the left, the progress bar is updated: 'Upload custom app' (checked), 'Users' (checked), 'Deployment' (checked), 'Permissions' (selected), and 'Finish' (unchecked). The main content area is titled 'Accept permissions requests' and includes the instruction 'Read the app permissions and capabilities carefully before proceeding'. Below this is the section 'App Permissions and Capabilities', which lists the app 'Cisco Secure Email Submission' and the provider 'Outlook'. Under 'App capabilities:', there is a bulleted list: 'ReadWriteMailbox' and 'SendReceiveData'. The screen has a clean, white background with blue accents.

Step 10. Click **Finish Deployment**.



Step 11. Click **Done**.

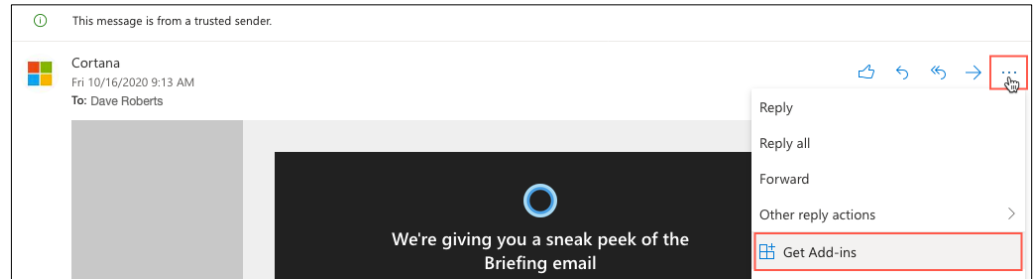


## Standalone Deployment

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.

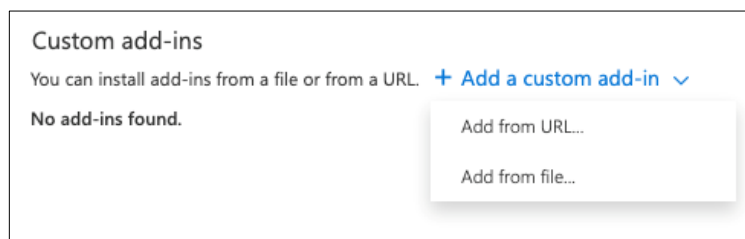
**Note:** If the **Get Add-ins** button is not available on your Outlook, log in to the Outlook Web App and complete the following steps:

1. Log in to <https://aka.ms/olksideload>.
2. In the left pane, select **My add-ins**.
3. Select Add a custom add-in, and then click **Add from File...**

For detailed instructions about adding the **Get Add-ins** button, see the Microsoft Office documentation.

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.

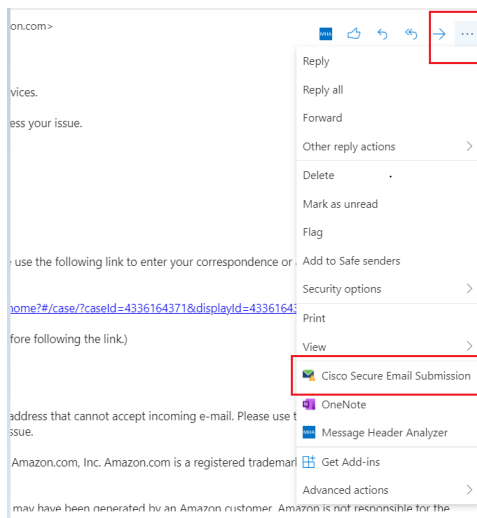
For detailed instructions about installing add-ins, see the Microsoft Office documentation.

# Modifying the Cisco Secure Email Submission Add-In Settings

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"> <li>Encrypted – the report is encrypted before sending.</li> <li>Plain – the report is sent without encryption.</li> </ul> <p><b>Note:</b> Currently, only the plain format is supported.</p>
Message Subject	Modify the message subject of your submission.

Step 4. Click **Apply**.

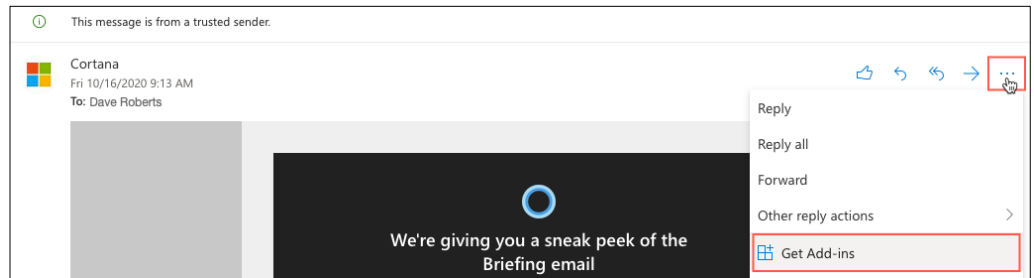
**Note:** Click **Reset** to change the settings to the default settings.

## Uninstalling the Cisco Secure Email Submission Add-In

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**.

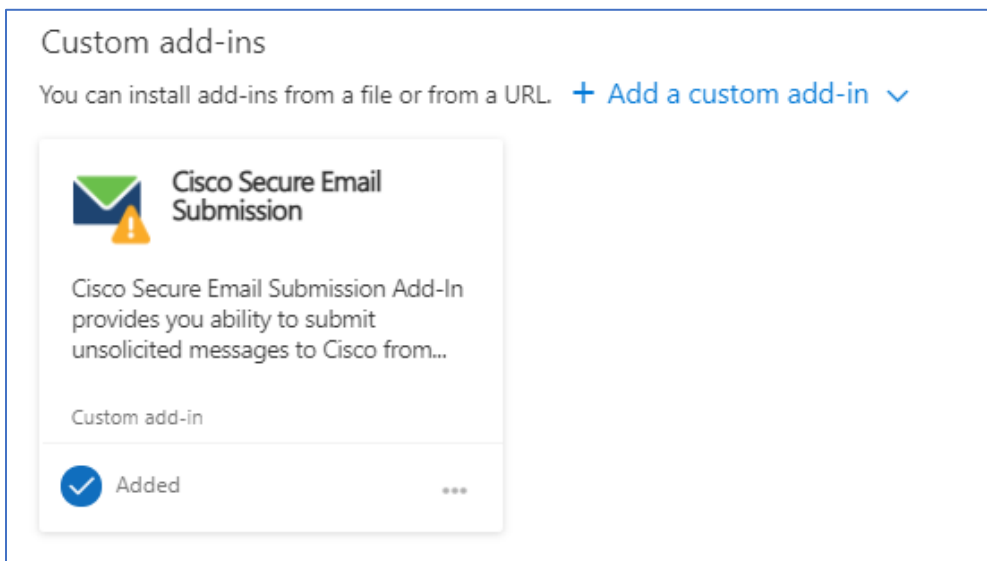


- On Outlook for Windows or macOS, click **Get Add-ins** from the Ribbon.

**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**.

Step 3. Under **Custom add-ins**, click the ellipsis icon in the Cisco Secure Email Submission add-in, and click **Remove**.



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

## Prerequisites

1. Install the new manifest file. See [Installing the Cisco Secure Email Submission Add-In](#) for more details.
2. O365 Exchange Online account users are required to provide consent for the Secure Email Submission Add-In to report incorrectly filtered messages.

Account administrators can provide the consent using one of the following ways:

- [Providing consent using the admin URL](#) (Recommended to be performed before deployment)
- [Providing consent using the Report button](#)

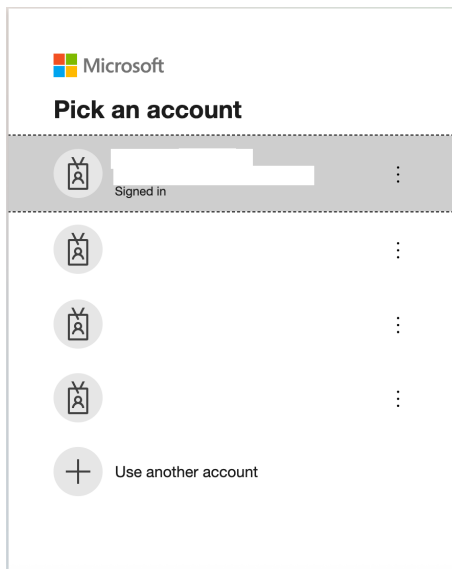
## Providing consent using the admin URL

Use the admin consent URL to grant consent for your organization. To grant consent, perform the following steps:

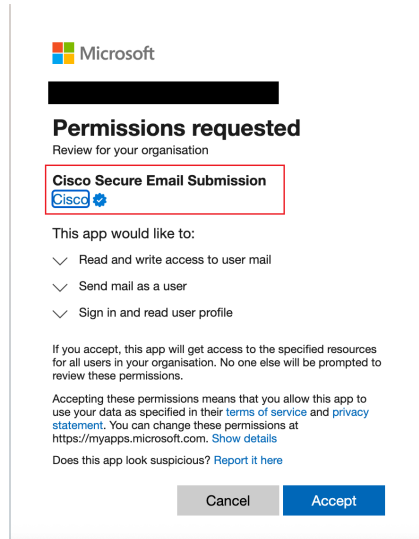
Step 1. Open this URL in a web browser:

[https://login.microsoftonline.com/common/adminconsent?client\\_id=ec007a11-e3ed-4943-b3da-3c79c960c4ca&redirect\\_uri=https://res.cisco.com/admin-consent-redirect.html](https://login.microsoftonline.com/common/adminconsent?client_id=ec007a11-e3ed-4943-b3da-3c79c960c4ca&redirect_uri=https://res.cisco.com/admin-consent-redirect.html)

The **Pick an account** pop-up opens if you have signed in using multiple accounts.



Step 2. Select the account that you are logged in to Outlook using which you are providing the consent.



**Note:** Make sure that you see **Cisco Secure Email Submission**, Cisco and the blue tick mark as shown.

Step 3. Click **Accept**.

A success message appears after the consent is granted.

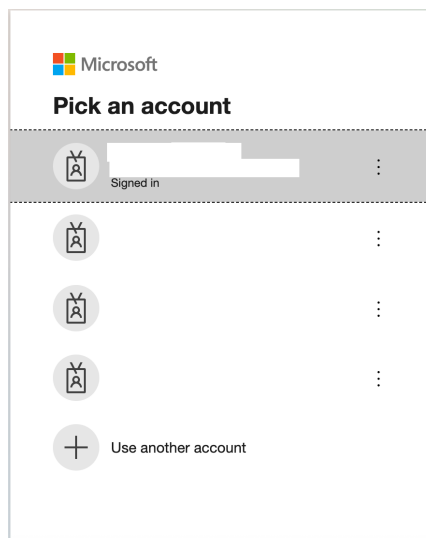
## Providing consent using the Report button

Account administrators can also grant consent for their organization by using one of the report options on the Cisco Secure Email Submission Add-In. To grant consent, perform the following steps:

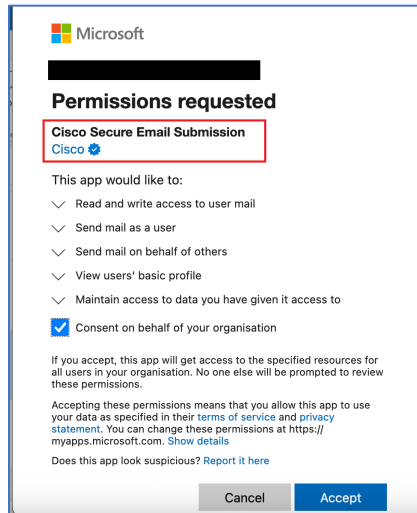
Step 1. Select an email and click the **Report Email** button on the Ribbon.

Step 2. Click any one of the report buttons.

The **Pick an account** pop-up opens if you have signed in using multiple accounts.



Step 3. Select the account that you are logged in to Outlook using which you are providing the consent.



**Note:** Make sure that you see **Cisco Secure Email Submission**, Cisco and the blue tick mark as shown.

Step 4. Select the **Consent on behalf of your organization** checkbox.

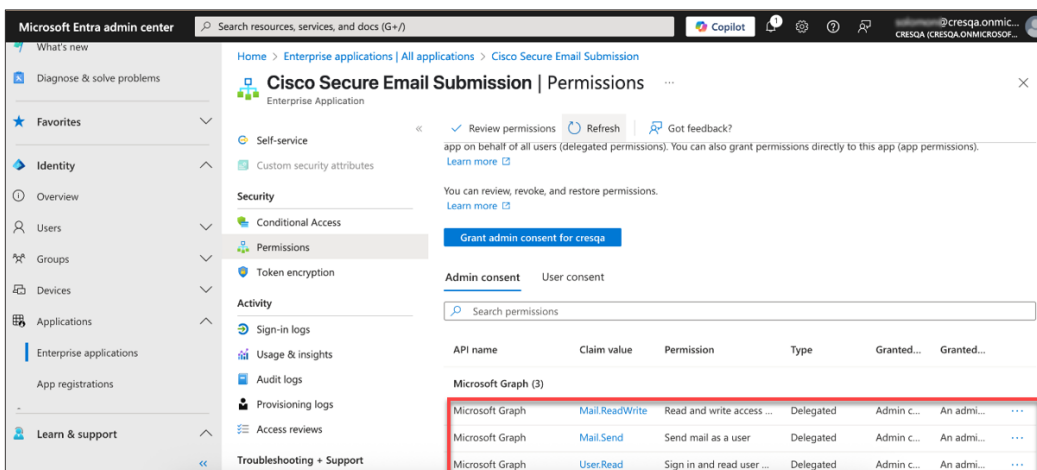
Step 5. Click **Accept**.

## Why Permission is Required

Permissions to sign in, read profiles, Read and write access, Send mails as a user, and delegate actions on your behalf are required to submit emails to global threat intelligence research for further processing.

This is already in use; however, consent is requested due to Microsoft's enhancements with Outlook Add-Ins. There are no changes to how the Secure Email Submission Add-In works.

The example below shows a list of granted permissions.

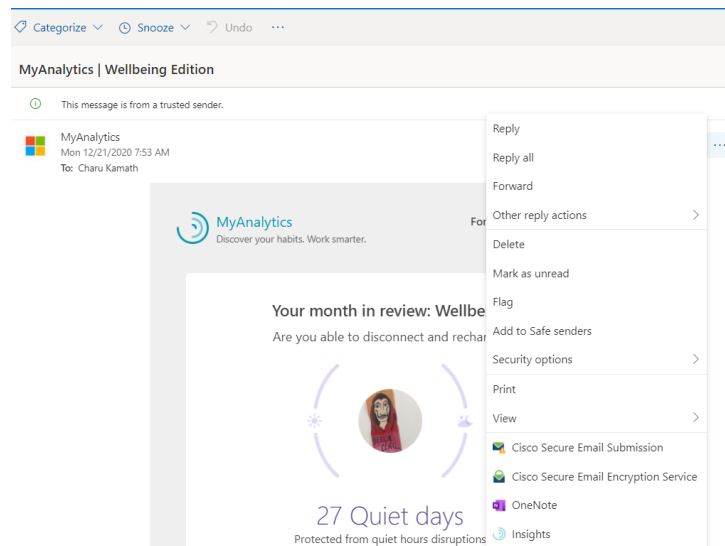


## Reporting Messages Using the Secure Email Submission Add-In

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](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.

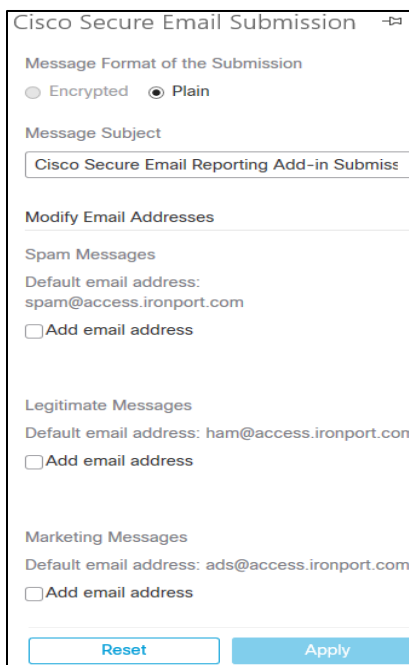
To submit a simulated phishing message, follow the procedure described in the previous section.

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.

- 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.



The screenshot shows the 'Cisco Secure Email Submission' settings pane. It includes the following sections:

- Message Format of the Submission:** Radio buttons for 'Encrypted' and 'Plain' (selected).
- Message Subject:** A text input field containing 'Cisco Secure Email Reporting Add-in Submit'.
- Modify Email Addresses:** A section with three sub-sections:
  - Spam Messages:** Default email address: spam@access.ironport.com. Includes an 'Add email address' checkbox.
  - Legitimate Messages:** Default email address: ham@access.ironport.com. Includes an 'Add email address' checkbox.
  - Marketing Messages:** Default email address: ads@access.ironport.com. Includes an 'Add email address' checkbox.
- Buttons:** 'Reset' and 'Apply' buttons at the bottom.

---

Step 4. (Optional) Check the **Add email address** checkbox.

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: Customizing the Secure Email Service Submission Add-In Branding

You can customize the Add-In Name, Description, Tooltip, and icons using the Manifest XML file downloaded from Cisco Software Central.

**Note:** Do not make any additional changes in the manifest XML file other than the ones mentioned in the section. Making additional changes will affect the deployment of the add-in and its functionality.

### To customize the add-in properties:

1. Login to <http://software.cisco.com/> and click *Access Downloads* under **Manage Downloads**.
2. Type *Secure Email Virtual Gateway* in the search box and click the search result.
3. In the Software Type, click **Email Submission AddIn**.
4. Click the download icon or *manifest-email-submission-1.0.0-006.xml* to download the file.
5. Click **Accept Cisco General Terms** if *Cisco's General Terms Agreement* pop-up appears. The manifest file gets downloaded to your system.
6. Open the *manifest-email-submission-1.0.0-006.xml* file on your system using any text editor.

You can customize the following items:

Item	Parameter Name	Default Value
Add-In Name	DisplayName DefaultValue	Cisco Secure Email Submission
Description	Description DefaultValue	Cisco Secure Email Submission Add-In provides you ability to submit unsolicited messages to Cisco from Outlook client.
Encryption Add-In Icon (Image)	IconUrl DefaultValue	<a href="https://static.cres-aws.com/add-in/report-message-80x80.png">https://static.cres-aws.com/add-in/report-message-80x80.png</a>
Icon (Image,, High-Resolution)	HighResolutionIconUrl DefaultValue	<a href="https://static.cres-aws.com/add-in/report-message-80x80.png">https://static.cres-aws.com/add-in/report-message-80x80.png</a>
Submission Add-In icons in Different resolutions	bt:Image id="Icon.16x16"  bt:Image id="Icon.32x32"  bt:Image id="Icon.80x80"	<a href="https://static.cres-aws.com/add-in/report-message-16x16.png">https://static.cres-aws.com/add-in/report-message-16x16.png</a>  <a href="https://static.cres-aws.com/add-in/report-message-32x32.png">https://static.cres-aws.com/add-in/report-message-32x32.png</a>  <a href="https://static.cres-aws.com/add-in/report-message-80x80.png">https://static.cres-aws.com/add-in/report-message-80x80.png</a>

---

Tooltip text for Submission Add-In	t:String id="TaskpaneButton.Tooltip"	Submit feedback to Cisco about unsolicited and unwanted messages such as spam, viruses, phishing, and marketing emails.
Tooltip text for Submission Add-In on reading window	bt:String id="ActionButton.Tooltip"	Submit feedback to Cisco about unsolicited and unwanted messages such as spam, viruses, phishing, and marketing emails.

After making the required changes, install the updated manifest file as described in [Installing the Cisco Secure Email Submission Add-In](#).

## Chapter 5: Troubleshooting the Cisco Secure Email Submission Add-In

### Email Submission Add-In becomes unresponsive when user tries to report messages

You are unable to report messages using the Cisco Secure Email Submission Add-In.

#### Reason

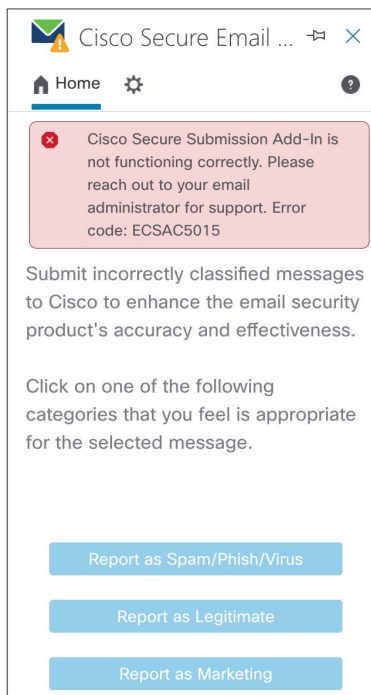
Microsoft has disabled legacy Exchange tokens for your organization, so the Cisco Secure Email Submission Add-In may require an update.

#### Solution

Contact your email administrator and provide the error code ECSAC5015 and screenshot.

**Note:** For Outlook users on Windows, the Submission Add-In may become unresponsive without displaying any error message, and no submissions will be processed. In this case, contact your email administrator.

**Note:** If the administrator encounters this error or a user reports this issue in O365 Exchange Online account, the administrator must remove the old manifest file before uploading the new one for Centralized Deployment. For Standalone Deployment in O365 Exchange Online account, upload the new manifest file directly to replace the old one. See [Installing the Cisco Secure Email Submission Add-In](#) for more details.



# 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

# Granting Consent Using Entra Admin Center

This is applicable only for users with an O365 Exchange Online account.

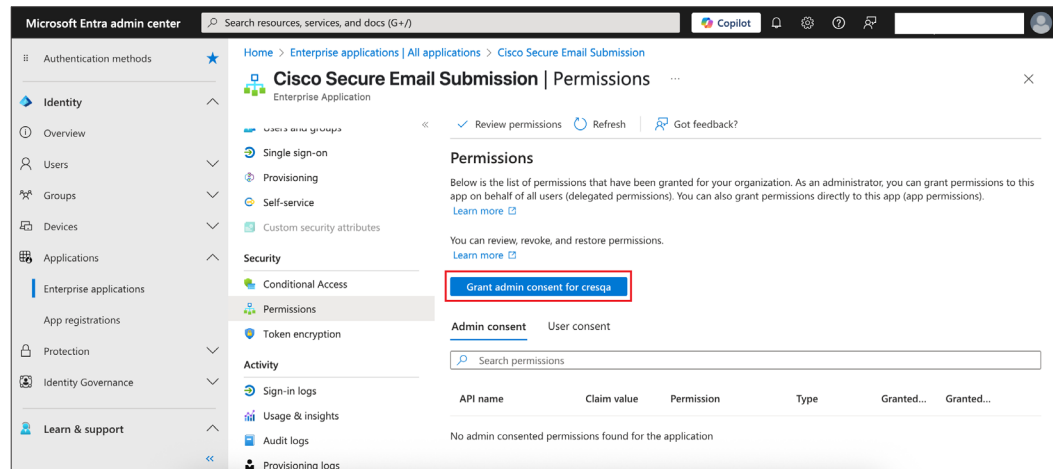
## Reason

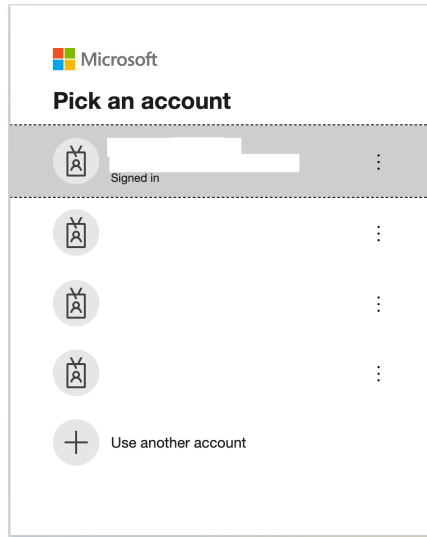
The account administrator did not provide consent using the recommended methods [here](#).

## Solution

The account administrator can grant consent on behalf of their organization by logging in to the Microsoft Entra admin center.

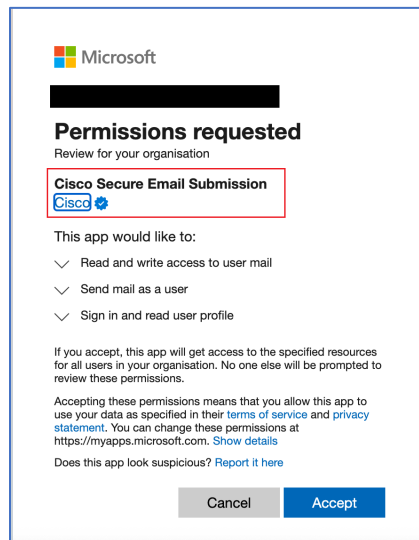
- Step 1. Log in to your **Microsoft Entra admin center**. (<https://admin.microsoft.com/>)
- Step 2. In the left pane, select **Identity > Applications > Enterprise Applications**.
- Step 3. Under **Enterprise Applications**, select **Cisco Secure Email Submission**, and then click **Permissions**.
- Step 4. Click the **Grant admin consent for <your organization name>** button.





The **Pick an account** pop-up opens if you have signed in using multiple accounts.

Step 5. Select the account that you are logged in to Outlook using which you are providing the consent.



**Note:** Make sure that you see **Cisco Secure Email Submission**, Cisco and the blue tick mark as shown.

Step 6. Click **Accept**.

The page reloads and shows the list of permissions granted for your organization.

Microsoft Entra admin center

Home > Enterprise applications | All applications > Cisco Secure Email Submission

### Cisco Secure Email Submission | Permissions

Enterprise Application

Review permissions Refresh Got feedback?

app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions).  
[Learn more](#)

You can review, revoke, and restore permissions.  
[Learn more](#)

[Grant admin consent for cresa](#)

Admin consent User consent

Search permissions

API name	Claim value	Permission	Type	Granted...	Granted...
Microsoft Graph (3)					
Microsoft Graph	Mail.ReadWrite	Read and write access ...	Delegated	Admin c...	An admi...
Microsoft Graph	Mail.Send	Send mail as a user	Delegated	Admin c...	An admi...
Microsoft Graph	User.Read	Sign in and read user ...	Delegated	Admin c...	An admi...



---

**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](http://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](http://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)