



Release Notes for Cisco Secure Email Submission Add-In 10.0

Published: April 17, 2024

Revised: July 29, 2025

Contents

- [Overview, page 1](#)
- [What's New In This Release, page 2](#)
- [Changes in Behavior, page 2](#)
- [Known and Fixed Issues, page 3](#)
- [Service and Support, page 4](#)
- [Obtaining Documentation and Submitting a Service Request, page 4](#)

Overview

Cisco Secure Email Submission add-in allows you to submit feedback to Cisco about unsolicited and unwanted messages such as spam, viruses, phishing, 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). You can add an additional email address to submit your messages to another email. However, this is optional.



What's New In This Release

- [What's New in Release 10.0.0-100 for Secure Email Submission Add-In, page 2](#)
- [What's New in Release 10.0.0-002 for Secure Email Submission Add-In, page 2](#)

What's New in Release 10.0.0-100 for Secure Email Submission Add-In

Feature	Description
Support for submitting messages up to 5 MB.	From this release onwards, Cisco Secure Email Submission Add-In allows submitting messages up to 5 MB.
Support for submitting emails to multiple addresses.	From this release onwards, Cisco Secure Email Submission Add-In supports submitting emails to multiple email addresses.

What's New in Release 10.0.0-002 for Secure Email Submission Add-In

Cisco Secure Email Encryption Service is transitioning to Amazon Web Services (AWS) infrastructure. The migration will be seamless, requiring no action on your part. Following the migration, you can continue to work on the Secure Email Submission Add-in. You will experience no downtime or disruption, and continue to access Secure Email Encryption Service as usual, with no changes to your user accounts or settings. This release of Secure Email Submission Add-In aligns with the transition of Cisco Secure Email Encryption Service infrastructure.

Changes in Behavior

[Changes in Behavior in Release 10.0.0-100, page 2](#)

Changes in Behavior in Release 10.0.0-100

There are no behavior changes in this release. For the list of known and fixed issues for this release, see [Known and Fixed Issues in Release 10.0.0-100, page 3](#)

Supported Configurations

See [Compatibility Matrix for Cisco Secure Email Services](#).

Outlook 2019 Support Removal for Cisco Secure Email Submission Add-In

Effective October 14, 2025, Cisco Secure Email Submission Add-In and Cisco Secure Email Submission Add-In are no longer supported on Microsoft Outlook 2019.

To continue using the Submission Add-in, customers should upgrade to Microsoft 365. Download and install the new manifest from the CCO portal and follow the instructions provided in the *Cisco Secure Email Submission Add-In User Guide*.

Known and Fixed Issues

[Known and Fixed Issues in Release 10.0.0-100, page 3](#)

[Known and Fixed Issues in Release 10.0.0-002, page 3](#)

Known and Fixed Issues in Release 10.0.0-100

Known Issues	There are no known issues for this release.
Fixed Issues	CSCwo53866 – Email submissions fail from Submission Add-In.

Known and Fixed Issues in Release 10.0.0-002

There are no known or fixed issues for this release of Secure Email Submission Add-In.

Installation Notes

If you are using Centralized Deployment, you must remove the old manifest file before uploading the new one. For Standalone Deployment, upload the new manifest file to replace the old one.

Related Documentation

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 Secure Email Gateway User Guide	https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html
Cisco Secure Email Encryption Service User Guide	https://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html

Service and Support

You can request support by phone, email, or online 24 hours a day, 7 days a week. Cisco Customer Support service level agreement details are available on the Support Portal. You can contact Cisco Customer Support using one of the following methods:

- Cisco Support Portal: <https://www.cisco.com/support>
- Phone support: Contact Cisco Technical Assistance Center (TAC) within U.S. /Canada at 800-553-2447 and at Worldwide Phone Numbers.
- Email: tac@cisco.com

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

To have a list of all new and revised Cisco technical documentation delivered directly to your desktop using a reader application, subscribe to *What's New in Cisco Product Documentation* as an RSS feed by clicking the RSS icon on the What's New page. The RSS feeds are a free service.

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)

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.

© 2022-2025 Cisco Systems, Inc. and/or its affiliates. All rights reserved.