

Release Notes for Cisco Secure Email Encryption Service 10.0

Published: October 19, 2024
Revised: September 15, 2026

Contents

- What's New In This Release, page 2
- Changes in Behavior, page 6
- Supported Operating Systems and Certificate Authorities, page 10
- Known and Fixed Issues, page 11
- Related Documentation, page 15
- Service and Support, page 16
- Obtaining Documentation and Submitting a Service Request, page 17

Cisco Systems, Inc.
www.cisco.com

What's New In This Release

- What’s New in Release 10.0.0-418, page 2
- What’s New in Release 10.0.0-413, page 2
- What’s New in Release 10.0.0-392, page 2
- What’s New in Release 10.0.0-360, page 3
- What’s New in Release 10.0.0-355, page 3
- What’s New in Release 10.0.0-346, page 3
- What’s New in Release 10.0.0-328, page 3
- What’s New in Release 10.0.0-309, page 4
- What’s New in Release 10.0.0-293, page 4
- What’s New in Release 10.0.0-291, page 4
- What’s New in Release 10.0.0-262, page 4
- What’s New in Release 10.0.0-252, page 4
- What’s New in Release 10.0.0-233, page 4
- What’s New in Release 10.0.0-203, page 5
- What’s New in Release 10.0.0-190, page 5
- What’s New in Release 10.0.0-138, page 5
- What’s New in Release 10.0.0-114, page 5
- What’s New in Release 10.0.0-092, page 5
- What’s New in Release 10.0.0-069, page 5
- What’s New in Release 10.0.0-060, page 5
- What’s New in Release 10.0.0-058, page 6
- What’s New in Release 10.0.0-003, page 6

What’s New in Release 10.0.0-418

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

What’s New in Release 10.0.0-413

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

What’s New in Release 10.0.0-392

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

What's New in Release 10.0.0-360

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

What's New in Release 10.0.0-355

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

What's New in Release 10.0.0-346

Secure Messaging Restrictions for Non-Corporate Users	Non-corporate users (end users with email domains that are not registered with Cisco Secure Email Encryption Service) can no longer send new secure messages. They can only reply or reply all to the secure messages they receive. This measure is implemented to prevent platform abuse and protect systems from phishing attempts. To enable secure compose for a domain, contact Cisco Support and provide the list of domains to be registered for secure messaging. For more information, see https://www.cisco.com/c/en/us/support/docs/security/email-encryption/222286-understand-cres-secure-compose-restricti.html

What's New in Release 10.0.0-328

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues in Release 10.0.0-328, page 13

What's New in Release 10.0.0-309

Restoring Your Last Saved Email	Cisco Secure Email Encryption Service now allows you to recover the contents of an unsent message that was automatically saved. Secure Email Encryption Service automatically saves draft messages in the **Compose Message** page after two minutes, so that you do not loose your unsaved drafts even if you navigate to other pages. To recover the saved content, click **Restore last saved email** at the top-right corner of the **Compose Message** page.

What's New in Release 10.0.0-293

Support for Both SAML 2.0 and CRES Methods in Websafe and Add-In	Cisco Secure Email Encryption Service now allows administrators to enable both SAML 2.0 and CRES authentication methods for the websafe and add-in. When both methods are configured, users logging in with CRES for the first time must use the Forgot Password link to generate a new password before they can log in successfully.

What's New in Release 10.0.0-291

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues in Release 10.0.0-291, page 13

What's New in Release 10.0.0-262

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues in Release 10.0.0-262, page 14

What's New in Release 10.0.0-252

Support for Setting Email Signatures	Cisco Secure Email Encryption Service now includes the Email Signature feature, allowing you to create a personalized signature that automatically appears at the bottom of emails when composing a message.

What's New in Release 10.0.0-233

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues in Release 10.0.0-233, page 14

What's New in Release 10.0.0-203

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues in Release 10.0.0-203, page 14

What's New in Release 10.0.0-190

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues in Release 10.0.0-190, page 14

What's New in Release 10.0.0-138

There are no new features added in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues in Release 10.0.0-138, page 14.

What's New in Release 10.0.0-114

Password Change Notifications for Account Administrators and Corporate Users when account admin resets the password	If an account administrator changes the password of another account admin, the affected admin will receive a notification email indicating which admin has changed their password. Also, if an account administrator changes the password of any user within the account, the user will receive a message notifying them that their password has been changed by an account admin.
Password Reset Notification for Non-Corporate Users when System admin resets the password	If a non-corporate user resets their password by contacting Secure Email Encryption Service support, they will receive an email confirming that their password has been reset by the support team.

What's New in Release 10.0.0-092

There are no new features added in this release. For the list of fixed issues for this release, see Known and Fixed Issues in Release 10.0.0-092, page 15.

What's New in Release 10.0.0-069

There are no new features added in this release. For the list of fixed issues for this release, see Fixed Issues in Release 10.0.0-069, page 15.

What's New in Release 10.0.0-060

There are no new features added in this release. For the list of fixed issues for this release, see Fixed Issues in Release 10.0.0-060, page 15.

What's New in Release 10.0.0-058

There are no new features added in this release. For the list of fixed issues for this release, see Fixed Issues in Release 10.0.0-058, page 15.

What's New in Release 10.0.0-003

Cisco Secure Email Encryption Service Infrastructure Migration to Amazon Web Services (AWS)	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 Encryption Service, Encryption Add-in, and 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.

Changes in Behavior

- Changes in Behavior in Release 10.0.0-418, page 7
- Changes in Behavior in Release 10.0.0-413, page 7
- Changes in Behavior in Release 10.0.0-392, page 7
- Changes in Behavior in Release 10.0.0-360, page 7
- Changes in Behavior in Release 10.0.0-355, page 7
- Changes in Behavior in Release 10.0.0-346, page 7
- Changes in Behavior in Release 10.0.0-328, page 7
- Changes in Behavior in Release 10.0.0-309, page 7
- Changes in Behavior in Release 10.0.0-293, page 8
- Changes in Behavior in Release 10.0.0-291, page 8
- Changes in Behavior in Release 10.0.0-262, page 8
- Changes in Behavior in Release 10.0.0-252, page 8
- Changes in Behavior in Release 10.0.0-233, page 8
- Changes in Behavior in Release 10.0.0-203, page 8
- Changes in Behavior in Release 10.0.0-190, page 8
- Changes in Behavior in Release 10.0.0-138, page 9
- Changes in Behavior in Release 10.0.0-114, page 9
- Changes in Behavior in Release 10.0.0-092, page 9
- Changes in Behavior in Release 10.0.0-069, page 9
- Changes in Behavior in Release 10.0.0-060, page 9
- Changes in Behavior in Release 10.0.0-058, page 9

- Changes in Behavior in Release 10.0.0-003, page 10

Changes in Behavior in Release 10.0.0-418

There are no behavior changes in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

Changes in Behavior in Release 10.0.0-413

There are no behavior changes in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

Changes in Behavior in Release 10.0.0-392

There are no behavior changes in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

Changes in Behavior in Release 10.0.0-360

There are no behavior changes in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

Changes in Behavior in Release 10.0.0-355

There are no behavior changes in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

Changes in Behavior in Release 10.0.0-346

There are no behavior changes in this release. For the list of known and fixed issues for this release, see Known and Fixed Issues, page 11

Changes in Behavior in Release 10.0.0-328

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 10.0.0-328, page 13

Changes in Behavior in Release 10.0.0-309

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 10.0.0-293, page 13

Changes in Behavior in Release 10.0.0-293

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 10.0.0-293, page 13

Changes in Behavior in Release 10.0.0-291

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 10.0.0-291, page 13

Changes in Behavior in Release 10.0.0-262

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 10.0.0-262, page 14

Changes in Behavior in Release 10.0.0-252

Feature	Description
Email address not listed option on the login page	From this release onwards, **Email address not listed** option appears directly on the login page. Recipients can manually enter their email address to open and read secure messages.

Changes in Behavior in Release 10.0.0-233

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 10.0.0-233, page 14

Changes in Behavior in Release 10.0.0-203

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 10.0.0-203, page 14

Changes in Behavior in Release 10.0.0-190

Feature	Description
Security Level Change Notification for end users if the account admin changes the security level from High to Medium or Low	The account admin will send an email notification to the end users asking them to update their configurations to update the existing security level settings and reflect the new changes on their side.

Changes in Behavior in Release 10.0.0-138

Feature	Description
Changes in Secure Compose Restrictions for non-corporate users.	If you have logged in using a non-corporate email address, you can send secure messages to both corporate and non-corporate recipients, except for some public domains, such as gmail.com, yahoo.com, aol.com, etc. For more information, see https://www.cisco.com/c/en/us/support/docs/security/email-encryption/222286-understand-cres-secure-compose-restricti.html

Changes in Behavior in Release 10.0.0-114

There are no behavior changes in this release. For the list of fixed issues for this release, see Known Issues in Release 10.0.0-114, page 15.

Changes in Behavior in Release 10.0.0-092

Feature	Description
Secure Compose Restrictions Using Websafe.	Non-corporate email addresses cannot send or forward secure messages to other non-corporate accounts. For more details, see https://www.cisco.com/c/en/us/support/docs/security/email-encryption/222286-understand-cres-secure-compose-restricti.html

Changes in Behavior in Release 10.0.0-069

- There are no behavior changes in this release. For the list of fixed issues for this release, see Fixed Issues in Release 10.0.0-069, page 15.

Changes in Behavior in Release 10.0.0-060

There are no behavior changes in this release. For the list of fixed issues for this release, see Fixed Issues in Release 10.0.0-060, page 15.

Changes in Behavior in Release 10.0.0-058

There are no behavior changes in this release. For the list of fixed issues for this release, see Fixed Issues in Release 10.0.0-058, page 15.

Changes in Behavior in Release 10.0.0-003

Feature	Description
Removal of Microsoft OneDrive for storage of messages	From this release onwards, only Cisco Storage on AWS is available for storing secure messages. Support for Microsoft OneDrive is not available.
Configure key retention period up to five years	Admins can configure the time period up to which the encryption keys are stored. By default, the keys are stored for one year. You can configure the key retention period up to five years. End user cannot open a secure message if its encryption key has expired.
Configure Read Message link expiry duration	Admins can set the maximum storage duration for the Read Message link in secure messages to 30 days.
Secure messages sent from Websafe cannot be forwarded.	If a secure message is sent from Websafe, recipients cannot forward it further to anyone. The *Forward Message* functionality is not available if the original message is sent from Websafe.

Supported Operating Systems and Certificate Authorities

For information about the supported operating systems and certificate authorities in this release, see Compatibility Matrix for Cisco Secure Email Encryption Service.

Known and Fixed Issues

- Known and Fixed Issues in Release 10.0.0-418, page 12
- Known and Fixed Issues in Release 10.0.0-413, page 12
- Known and Fixed Issues in Release 10.0.0-392, page 12
- Known and Fixed Issues in Release 10.0.0-360, page 12
- Known and Fixed Issues in Release 10.0.0-355, page 11
- Known and Fixed Issues in Release 10.0.0-346, page 13
- Known and Fixed Issues in Release 10.0.0-328, page 13
- Known and Fixed Issues in Release 10.0.0-309, page 13
- Known and Fixed Issues in Release 10.0.0-293, page 13
- Known and Fixed Issues in Release 10.0.0-291, page 13
- Known and Fixed Issues in Release 10.0.0-262, page 14
- Known and Fixed Issues in Release 10.0.0-252, page 14
- Known and Fixed Issues in Release 10.0.0-233, page 14
- Known and Fixed Issues in Release 10.0.0-203, page 14
- Known and Fixed Issues in Release 10.0.0-190, page 14
- Known and Fixed Issues in Release 10.0.0-138, page 14
- Known Issues in Release 10.0.0-114, page 15
- Known and Fixed Issues in Release 10.0.0-092, page 15
- Fixed Issues in Release 10.0.0-069, page 15
- Fixed Issues in Release 10.0.0-060, page 15
- Fixed Issues in Release 10.0.0-058, page 15
- Known Issues in Release 10.0.0-058, page 15

Known and Fixed Issues in Release 10.0.0-418

Known Issues	There are no known issues for this release.
Fixed Issues	• CSCww17382 - CRES Admin Portal Add User form loses required fields and Save after validation error • CSCww19537 - Account Admin: Password mismatch validation message not shown while modifying user password

Known and Fixed Issues in Release 10.0.0-413

Known Issues	• CSCww17382 - CRES Admin Portal Add User form loses required fields and Save after validation error • CSCww19537 - Account Admin: Password mismatch validation message not shown while modifying user password
Fixed Issues	There are no fixed issues for this release.

Known and Fixed Issues in Release 10.0.0-392

Known Issues	There are no known issues for this release.
Fixed Issues	CSCwv10371 - CRES txt attachments execute directly to the browser breaking text encoding

Known and Fixed Issues in Release 10.0.0-360

Known Issues	There are no known issues for this release.
Fixed Issues	• CSCwt46653 - Sender Display Name Shows ???? for Non-Latin Characters in SecureDocs Mail From Field For more information, see User Action for CSCwt46653, page 12. • CSCwt39210 - Read Receipt from External Users Displays Two Different Email Addresses in MAIL FORM

User Action for CSCwt46653

To ensure the fix takes effect, user should perform the following steps:

- Log in to the Websafe.
- Navigate to the Edit Profile section.
- Re-enter the First Name and Last Name using the desired non-Latin characters.
- Click Save to apply the changes.

Following these steps will ensure that outgoing emails display the sender's name correctly.

Known and Fixed Issues in Release 10.0.0-355

Known Issues	There are no known issues for this release.
Fixed Issues	• CSCws32757 - FROM header incorrectly contains two email addresses for Websafe ? TLS and related flows • CSCws39665 - Non Latin Characters Display as ? in CRES Websafe Manage Message View and in read recipients

Known and Fixed Issues in Release 10.0.0-346

Known Issues	There are no known issues for this release.
Fixed Issues	CSCws03397 - DKIM verification fails for emails sent from Websafe

Known and Fixed Issues in Release 10.0.0-328

Known Issues	There are no known issues for this release.
Fixed Issues	CSCws15386 - Non-ASCII characters transform to unreadable symbols in CRES emails

Known and Fixed Issues in Release 10.0.0-309

Known Issues	There are no known issues for this release.
Fixed Issues	There are no fixed issues for this release.

Known and Fixed Issues in Release 10.0.0-293

Known Issues	There are no known issues for this release.
Fixed Issues	There are no fixed issues for this release.

Known and Fixed Issues in Release 10.0.0-291

Known Issues	There are no known issues for this release.
Fixed Issues	CSCwq66677- TLS delivery from CRES can fail to verify some certificates, leading to delays

Known and Fixed Issues in Release 10.0.0-262

Known Issues	There are no known issues for this release.
Fixed Issues	CSCwq15434 - "CRES Websafe" created email may be treated as suspicious or junk due to formatting of the From header

Known and Fixed Issues in Release 10.0.0-252

Known Issues	There are no known issues for this release.
Fixed Issues	There are no fixed issues for this release.

Known and Fixed Issues in Release 10.0.0-233

Known Issues	There are no known issues for this release.
Fixed Issues	CSCwj88837 – Secure Email composed in Websafe incorrectly rendered in Microsoft Outlook on Windows.

Known and Fixed Issues in Release 10.0.0-203

Known Issues	There are no known issues for this release.
Fixed Issues	CSCwn80716 – Special character in Display name splits the email address using CRES.

Known and Fixed Issues in Release 10.0.0-190

Known Issues	CSCwn91656 – Message Expiry Fails in Websafe for Non-English Locales.
Fixed Issues	CSCwj69455 – Bounce emails for external users are sent to res.cisco.com instead of actual senders.

Known and Fixed Issues in Release 10.0.0-138

Known Issues	There are no known issues for this release.
Fixed Issues	CSCwm97862 – Users are unable to unblock themselves if admin blocks or they give wrong passwords for 5 times.

Known Issues in Release 10.0.0-114

- CSCwm85145 - Password Reset Notification is sent When User Status is Changed to Blocked/Locked/Suspended
- CSCwm77343 - Secure Forward gives success message even with no recipients.

Known and Fixed Issues in Release 10.0.0-092

- There are no known and fixed issues for this release.

Fixed Issues in Release 10.0.0-069

- CSCwk62092 - Link Greyed Out (Activation & Password Reset)
- CSCwm00383 - Secure message email contains invisible "Read Message" link when displayed in some Web Clients.

Fixed Issues in Release 10.0.0-060

- CSCwj69455: Bounce emails for external users are sent to res.cisco.com instead of the actual senders.

Fixed Issues in Release 10.0.0-058

- CSCwh56746: Language change option does not affect customer support page.

  Customer support page https://res.cisco.com/websafe/help?topic=ContactSupport now displays the languages correctly.

Known Issues in Release 10.0.0-058

- There are no known issues for this release.

Related Documentation

Document	Location
Account Administrator Guide	https://www.cisco.com/c/en/us/support/security/email-encryption/products-user-guide-list.html
Recipient User Guide	
Compatibility Matrix	

Open Source Documentation	https://www.cisco.com/c/en/us/support/security/email-encryption/products-release-notes-list.html
Release Notes	

Service and Support

Use the following steps to resolve support cases:

Step 1 Use the 'Frequently Asked Questions' web page—most issues with registration and Secure Message opening can be quickly resolved by seeing if your question is answered on the following web page: http://res.cisco.com/websafe/help?topic=FAQ.

Step 2 Recipients can obtain support by clicking the Chat Online icon and speaking with the Live Agent 24 hours a day, seven days a week. The web chat is available at: https://res.cisco.com/websafe/help?topic=ContactSupport.



Note The Email and Web Chat Support is now available in English and French. The French Support is available between the hours of 8:00 AM to 5:00 PM, Eastern Time, on weekdays.

Step 3 Contact Cisco Secure Email Encryption Service support through email—any issue that is not resolved by the FAQ page must be emailed to the Cisco Secure Email Encryption Service support (support@res.cisco.com). An end-user can expect a response within 24 business hours after submitting the email.

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.

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved.