



# Customer Notification for AsyncOS 15.5.1 for Cisco Secure Email and Web Manager - New Features and Behavior Changes

---

Published: March 13, 2024

## Contents

- [Release Date, page 1](#)
- [New Features, page 2](#)
- [Changes in Behavior, page 3](#)
- [Service and Support, page 5](#)

## Release Date

Release Date: March 20, 2024




---

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

# New Features

Feature	Description
TLS 1.3 Support for Web Interface and API Server	<p>You can use TLS 1.3 for TLS communication across the legacy or new web interfaces of your Secure Email and Web Manager and the API services.</p> <p>For more information, see "Secure Communication Protocol" section in the "Common Administrative Tasks" chapter of the user guide.</p>
Search Filter Enhancement	<p>To enhance your search, two new filters, Contains and Does Not Contain, are added to the drop-down list on the Search ribbon at the bottom of the reporting pages.</p> <p>For more information, see "Searching and the Interactive Email Report Pages" section in the "Using Centralized Email Security Reporting" chapter of the userguide.</p>

# Changes in Behavior

SSH Server Configuration Changes	<p><b>New Install Scenario</b></p> <p>The following SSH server configuration changes are applicable when you install AsyncOS 15.5 for Cisco Secure Email and Web Manager for the first time.</p> <p><b>[Non-FIPS Mode]</b></p> <p>The following cipher algorithms, MAC method, Host key algorithms, and Kex algorithms are supported in your Secure Email and Web Manager:</p> <ul style="list-style-type: none"> <li>• Cipher algorithms - aes128-gcm@openssh.com and chacha20-poly1305@openssh.com</li> <li>• MAC method- hmac-sha2-256</li> <li>• Host key algorithms - ecdsa-sha2-nistp256, and ssh-ed25519</li> <li>• Kex algorithms - curve25519-sha256 , diffie-hellman-group14-sha256, and curve25519-sha256@libssh.org</li> </ul> <p><b>[FIPS Mode]</b></p> <p>The following cipher algorithm, MAC method, and Host key algorithm are supported in your Secure Email and Web Manager:</p> <ul style="list-style-type: none"> <li>• Cipher algorithm - aes128-gcm@openssh.com</li> <li>• MAC method - hmac-sha2-256</li> <li>• Host key algorithm - ecdsa-sha2-nistp256</li> </ul> <p> <b>Note</b> When you upgrade your Secure Email and Web Manager from a lower AsyncOS version to AsyncOS 15.5 version and later, all the must-supported algorithms are added to the SSH Server.</p>
Log Message Changes for TLS Connection Status	<p>The log message for TLS connection status is modified to include details about the validity check along with the date and time of certificate expiry or certificate validity commencement for the following services:</p> <ul style="list-style-type: none"> <li>• LDAP</li> <li>• Updater</li> <li>• Syslog</li> <li>• Alert Over TLS</li> <li>• SMTP Outbound (EUQ)</li> </ul>

Application SSH Client Algorithm Support	<p>The application SSH client algorithms are supported for the following connections:</p> <ul style="list-style-type: none"> <li>• When you connect Secure Email Gateway to Secure Email and Web Manager.</li> <li>• When you back up the configuration from Secure Email and Web Manager.</li> <li>• When you add a secondary Secure Email and Web Manager to a primary Secure Email and Web Manager.</li> </ul> <p><b>[Non-FIPS Mode]</b></p> <p>The following cipher algorithm, MAC method, and KEX algorithm are added to your Secure Email and Web Manager by default in addition to the existing algorithms:</p> <ul style="list-style-type: none"> <li>• Cipher algorithms - aes128-ctr</li> <li>• MAC methods - hmac-sha2-256</li> <li>• KEX algorithms - diffie-hellman-group14-sha256</li> </ul> <p><b>[FIPS Mode]</b></p> <p>The following cipher algorithm and MAC method are added to your Secure Email and Web Manager by default in addition to the existing algorithms:</p> <ul style="list-style-type: none"> <li>• Cipher algorithms - aes128-ctr</li> <li>• MAC methods - hmac-sha2-256</li> </ul>
Removal of Splunk Database Files	<p>Before this release, the Secure Email and Web Manager retained Splunk database files after the upgrade process.</p> <p>After you upgrade to this release, if the Splunk database files were present before the upgrade process, the Secure Email and Web Manager removes all the Splunk database files.</p>
Accepting Substrings of Passwords	<p>Before this release, when you added a user with a password that contains a substring (three or more characters) of the string "password," the system would not accept any substrings such as "pas," "wor," or "ord."</p> <p>After you upgrade to this release, when you add a user with a password that contains a substring (3 or more characters) of the string "password," the system accepts substrings such as "pas," "wor," or "ord," ensuring more comprehensive detection of substrings.</p>
Deleting Files from <code>/data/db/syslogs</code> Directory	<p>Before this release, you could not delete files in the <code>/data/db/syslogs</code> directory.</p> <p>From this release onwards, you can use the <code>wipedata</code> CLI command to delete files in the <code>/data/db/syslogs</code> directory. When you delete files from the <code>/data/db/syslogs</code> directory using the <code>wipedata</code> command, you will also receive a notification message informing you to modify the log subscription to <b>Manual</b> and configure it back to <b>Syslog</b> if you want to retrieve the log files using Syslog Push.</p>

# Service and Support

**Note**

To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.

Cisco TAC: [http://www.cisco.com/en/US/support/tsd\\_cisco\\_worldwide\\_contacts.html](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)

Support site for legacy IronPort: Visit <http://www.cisco.com/web/services/acquisitions/ironport.html>

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.

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)

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.

© 2024 Cisco Systems, Inc. All rights reserved.