# List of Ciphers for AsyncOS 15.5 for Secure Web Appliance

**First Published:** 2025-04-21

## About Secure Web Appliance

The Cisco Secure Web Appliance intercepts and monitors Internet traffic and applies policies to help keep your internal network secure from malware, sensitive data loss, productivity loss, and other Internet-based threats.

## Supported Ciphers

This section contains the list of supported ciphers (SSL and SSH) for AsyncOS for Secure Web Appliance.

### Port 8443 (Management Interface)

| TLS 1.2 | TLS 1.3 |
|---|---|
| ECDHE-ECDSA-AES256-GCM-SHA384 | TLS_AES_256_GCM_SHA384 |
| ECDHE-RSA-AES256-GCM-SHA384 | TLS_AES_128_GCM_SHA256 |
| ECDHE-ECDSA-CHACHA20-POLY1305 | TLS_CHACHA20_POLY1305_SHA256 |
| ECDHE-RSA-CHACHA20-POLY1305 | |
| ECDHE-ECDSA-AES256-CCM | |
| ECDHE-ECDSA-AES128-GCM-SHA256 | |
| ECDHE-RSA-AES128-GCM-SHA256 | |
| ECDHE-ECDSA-AES128-CCM | |
| ECDHE-ECDSA-AES256-SHA384 | |
| ECDHE-RSA-AES256-SHA384 | |
| ECDHE-ECDSA-CAMELLIA256-SHA384 | |
| ECDHE-RSA-CAMELLIA256-SHA384 | |
| ECDHE-ECDSA-AES128-SHA256 | |
| ECDHE-RSA-AES128-SHA256 | |
| ECDHE-ECDSA-CAMELLIA128-SHA256 | |
| ECDHE-RSA-CAMELLIA128-SHA256 | |
| AES256-GCM-SHA384 | |

| TLS 1.2 | TLS 1.3 |
|---|---|
| AES256-CCM | |
| AES128-GCM-SHA256 | |
| AES128-CCM | |
| AES256-SHA256 | |
| CAMELLIA256-SHA256 | |
| AES128-SHA256 | |
| CAMELLIA128-SHA256 | |
| Default Mode:<br>ECDHE-RSA-AES256-GCM-SHA384<br>ECDHE-RSA-CHACHA20-POLY1305<br>ECDHE-RSA-AES128-GCM-SHA256<br>ECDHE-RSA-AES256-SHA384<br>ECDHE-RSA-CAMELLIA256-SHA384<br>ECDHE-RSA-AES128-SHA256<br>ECDHE-RSA-CAMELLIA128-SHA256<br>ECDHE-RSA-AES128-SHA<br>AES256-GCM-SHA384<br>AES256-CCM AES128-GCM-SHA256<br>AES128-CCM AES256-SHA256<br>CAMELLIA256-SHA256 AES128-SHA256<br>CAMELLIA128-SHA256<br>AES256-SHA AES128-SHA<br>CAMELLIA128-SHA | |
| **Note**<br>From AsyncOS 15.5, TLS 1.0 and TLS 1.1 is not supported on management interface (Port 8443). | |
| **Note**<br>Default mode represents the supported ciphers with the “SSL Cipher String” that is configured in the Secure Web Appliance.. | |

# Port 443 (SSL Port)

| TLS 1.0 | TLS 1.1 | TLS 1.2 | TLS 1.3 |
|---|---|---|---|
| ECDHE-ECDSA-AES128-SHA | ECDHE-ECDSA-AES128-SHA | ECDHE-ECDSA-AES256-GCM-SHA384 | TLS_AES_256_GCM_SHA384 |
| ECDHE-RSA-AES128-SHA | ECDHE-RSA-AES128-SHA | ECDHE-RSA-AES256-GCM-SHA384 | TLS_AES_128_GCM_SHA256 |
| AES256-SHA | AES256-SHA | ECDHE-ECDSA-CHACHA20-POLY1305 | TLS_CHACHA20_POLY1305_SHA256 |
| AES128-SHA | AES128-SHA | ECDHE-RSA-CHACHA20-POLY1305 | |

| TLS 1.0 | TLS 1.1 | TLS 1.2 | TLS 1.3 |
|---|---|---|---|
| | | ECDHE-ECDSA-AES256-CCM | |
| | | ECDHE-ECDSA-AES128-GCM-SHA256 | |
| | | ECDHE-RSA-AES128-GCM-SHA256 | |
| | | ECDHE-ECDSA-AES128-CCM | |
| | | ECDHE-ECDSA-AES256-SHA384 | |
| | | ECDHE-RSA-AES256-SHA384 | |
| | | ECDHE-ECDSA-CAMELLIA256-SHA384 | |
| | | ECDHE-RSA-CAMELLIA256-SHA384 | |
| | | ECDHE-ECDSA-AES128-SHA256 | |
| | | ECDHE-RSA-AES128-SHA256 | |
| | | ECDHE-ECDSA-CAMELLIA128-SHA256 | |
| | | ECDHE-RSA-CAMELLIA128-SHA256 | |
| | | AES256-GCM-SHA384 | |
| | | AES256-CCM | |
| | | AES128-GCM-SHA256 | |
| | | AES128-CCM | |
| | | AES256-SHA256 | |
| | | CAMELLIA256-SHA256 | |
| | | AES128-SHA256 | |
| | | CAMELLIA128-SHA256 | |

| TLS 1.0 | TLS 1.1 | TLS 1.2 | TLS 1.3 |
|---|---|---|---|
| Default Mode:<br>ECDHE-RSA-AES128-SHA<br>ECDHE-ECDSA-AES128-SHA<br>AES128-SHA<br>DHE-RSA-AES128-SHA | Default Mode:<br>ECDHE-RSA-AES128-SHA<br>ECDHE-ECDSA-AES128-SHA<br>AES128-SHA<br>DHE-RSA-AES128-SHA<br>ECDHE-PSK-AES128-CBC-SHA256<br>ECDHE-PSK-AES128-CBC-SHA<br>DHE-PSK-AES128-CBC-SHA256 | Default Mode:<br>ECDHE-ECDSA-AES256-GCM-SHA384<br>ECDHE-RSA-AES256-GCM-SHA384<br>ECDHE-ECDSA-AES128-GCM-SHA256<br>ECDHE-RSA-AES128-GCM-SHA256<br>ECDHE-ECDSA-AES256-SHA384<br>ECDHE-RSA-AES256-SHA384<br>ECDHE-ECDSA-AES128-SHA256<br>ECDHE-RSA-AES128-SHA256<br>ECDHE-ECDSA-AES128-SHA<br>ECDHE-RSA-AES128-SHA<br>AES256-GCM-SHA384<br>AES128-GCM-SHA256<br>AES256-SHA256<br>AES128-SHA256<br>AES128-SHA<br>DHE-RSA-AES128-SHA<br>DHE-PSK-AES256-GCM-SHA384<br>ECDHE-PSK-CHACHA20-POLY1305<br>DHE-PSK-AES128-GCM-SHA256 | Default Mode:<br>TLS_AES_256_GCM_SHA384<br>TLS_AES_128_GCM_SHA256<br>TLS_CHACHA20_POLY1305_SHA256 |

**Note**
Default mode represents the supported ciphers with the “SSL Cipher String” that is configured in the Secure Web Appliance.

# Port 22 (SSH Port)

**ssh2-enum-algos:**

| 1. kex_algorithms (8): | 2. encryption_algorithms (7): | 3. server_host_key_algorithms (4): |
|---|---|---|
| • diffie-hellman-group14-sha1<br>• ecdh-sha2-nistp256<br>• ecdh-sha2-nistp384<br>• ecdh-sha2-nistp521<br>• diffie-hellman-group14-sha256<br>• curve25519-sha256<br>• curve25519-sha256@libssh.org<br>• diffie-hellman-group16-sha512 | • aes192-cbc<br>• aes256-cbc<br>• aes128-ctr<br>• aes192-ctr<br>• aes256-ctr<br>• aes128-cbc<br>• chacha20-poly1305@openssh.com | • rsa-sha2-256<br>• ssh-rsa<br>• ssh-dss<br>• ssh-ed25519<br>• ecdsa-sha2-nistp256<br>• rsa-sha2-512 |

| 4. mac_algorithms (3): | 5. compression_algorithms (2): | |
|---|---|---|
| • hmac-sha2-256<br>• hmac-sha1<br>• hmac-sha2-512 | • none<br>• zlib@openssh.com | |

# Unsupported Ciphers

The following ciphers are not supported from the release SWA15.5 onwards with OpenSSL-1.1.1y.

| |
|---|
| DHE-RSA-AES256-GCM-SHA384 |
| DHE-RSA-CHACHA20-POLY1305 |
| DHE-RSA-AES128-GCM-SHA256 |
| DHE-RSA-AES256-SHA256 |
| DHE-RSA-AES128-SHA256 |
| DHE-RSA-AES128-SHA |
| RSA-PSK-AES256-GCM-SHA384 |
| DHE-PSK-AES256-GCM-SHA384 |
| RSA-PSK-CHACHA20-POLY1305 |
| DHE-PSK-CHACHA20-POLY1305 |
| ECDHE-PSK-CHACHA20-POLY1305 |
| PSK-AES256-GCM-SHA384 |
| PSK-CHACHA20-POLY1305 |
| RSA-PSK-AES128-GCM-SHA256 |
| DHE-PSK-AES128-GCM-SHA256 |
| PSK-AES128-GCM-SHA256 |
| ECDHE-PSK-AES256-CBC-SHA384 |
| RSA-PSK-AES256-CBC-SHA384 |
| DHE-PSK-AES256-CBC-SHA384 |
| PSK-AES256-CBC-SHA384 |
| ECDHE-PSK-AES128-CBC-SHA256 |
| ECDHE-PSK-AES128-CBC-SHA |
| RSA-PSK-AES128-CBC-SHA256 |
| DHE-PSK-AES128-CBC-SHA256 |
| RSA-PSK-AES128-CBC-SHA |

| |
|---|
| DHE-PSK-AES128-CBC-SHA |
| PSK-AES128-CBC-SHA256 |
| PSK-AES128-CBC-SHA |

## Port 8443 (Management Interface)

| SSL V 3.0 | TLS 1.0 |
|---|---|
| RC4-MD5 | RC4-MD5 |
| RC4-SHA | RC4-SHA |

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)

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.

© 2025 Cisco Systems, Inc. All rights reserved.