List of Ciphers for AsyncOS 16.0 for Secure Web Appliance

First Published: 2026-06-09

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

Port 443 (SSL Port)

TLS 1.2	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	

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 1.2	TLS 1.3
Default Mode: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-RSA-AES128-SHA AES256-GCM-SHA384 AES128-GCM-SHA256 AES256-SHA256 AES128-SHA256 AES128-SHA DHE-RSA-AES128-SHA	Default Mode: TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256 TLS_CHACHA20_POLY1305_SHA256
Note Starting with AsyncOS 16.0, SWA uses two different versions of the CiscoSSL library: • HTTPS proxy traffic: Uses the CiscoSSL_PQC 3.3.3.8.3.39 library (based on OpenSSL 3.3.3). • All other services: Continue to use Ciscossl-fom-7.3a (based on OpenSSL_1.1.1y).	
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): • diffie-hellman-group14-sha1 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • diffie-hellman-group16-sha512	**2. encryption_algorithms (7):** • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr • aes256-ctr • aes128-cbc • chacha20-poly1305@openssh.com • aes128-gcm@openssh.com	**3. server_host_key_algorithms (4):** • rsa-sha2-256 • ssh-rsa • ssh-dss • ssh-ed25519 • ecdsa-sha2-nistp256 • rsa-sha2-512
4. mac_algorithms (3): • hmac-sha2-256 • hmac-sha1 • hmac-sha2-512	**5. compression_algorithms (2):** • none • zlib@openssh.com	

Unsupported Ciphers

The following ciphers are not supported from the release SWA16.0 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