List of Ciphers for AsyncOS 11.8 for Web Security Appliance

First Published: 2021-10-01

About Web Security Appliance

The Cisco Web Security 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 Web Security Appliance.

Port 8443 (Management Interface)

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA384
DHE-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA	ECDHE-RSA-AES256-SHA
AES256-SHA	AES256-SHA	AES256-SHA	DHE-RSA-AES256-GCM-SHA384
CAMELLIA256-SHA	CAMELLIA256-SHA	CAMELLIA256-SHA	DHE-RSA-AES256-SHA256
ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	DHE-RSA-AES256-SHA
DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA	DHE-RSA-CAMELLIA256-SHA
DHE-RSA-SEED-SHA	DHE-RSA-SEED-SHA	DHE-RSA-SEED-SHA	AES256-GCM-SHA384
DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA	AES256-SHA256
AES128-SHA	AES128-SHA	AES128-SHA	AES256-SHA
SEED-SHA	SEED-SHA	SEED-SHA	CAMELLIA256-SHA
CAMELLIA128-SHA	CAMELLIA128-SHA	CAMELLIA128-SHA	ECDHE-RSA-AES128-GCM-SHA256
			ECDHE-RSA-AES128-SHA256
			ECDHE-RSA-AES128-SHA
			DHE-RSA-AES128-GCM-SHA256
			DHE-RSA-AES128-SHA
			DHE-RSA-SEED-SHA

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
			DHE-RSA-CAMELLIA128-SHA
			AES128-GCM-SHA256
			AES128-SHA256
			AES128-SHA
			SEED-SHA
			CAMELLIA128-SHA

Port 443 (HTTPS Proxy Service)

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA	DHE-RSA-AES256-SHA	DHE-RSA-AES256-GCM-SHA384
DHE-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA	DHE-RSA-CAMELLIA256-SHA	DHE-RSA-AES256-SHA256
AES256-SHA	AES256-SHA	AES256-SHA	DHE-RSA-AES256-SHA
CAMELLIA256-SHA	CAMELLIA256-SHA	CAMELLIA256-SHA	DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA	DHE-RSA-AES128-SHA
DHE-RSA-SEED-SHA	DHE-RSA-SEED-SHA	DHE-RSA-SEED-SHA	DHE-RSA-CAMELLIA256-SHA
DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA	DHE-RSA-CAMELLIA128-SHA	DHE-RSA-AES128-SHA256
AES128-SHA	AES128-SHA	AES128-SHA	SEED-SHA
SEED-SHA	SEED-SHA	SEED-SHA	CAMELLIA128-SHA
CAMELLIA128-SHA	CAMELLIA128-SHA	CAMELLIA128-SHA	CAMELLIA256-SHA
DHE-DSS-AES256-SHA	DHE-DSS-AES256-SHA	DHE-DSS-AES256-SHA	AES256-SHA
DHE-DSS-CAMELLIA256-SHA	DHE-DSS-CAMELLIA256-SHA	DHE-DSS-CAMELLIA256-SHA	AES128-SHA256
DHE-DSS-AES128-SHA	DHE-DSS-AES128-SHA	DHE-DSS-AES128-SHA	AES128-GCM-SHA256
DHE-DSS-SEED-SHA	DHE-DSS-SEED-SHA	DHE-DSS-SEED-SHA	AES256-SHA256
DHE-DSS-CAMELLIA128-SHA	DHE-DSS-CAMELLIA128-SHA	DHE-DSS-CAMELLIA128-SHA	AES256-GCM-SHA384
DES-CBC3-SHA	DES-CBC3-SHA	DES-CBC3-SHA	AES128-SHA
EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	DHE-RSA-AES128-SHA
IDEA-CBC-SHA	IDEA-CBC-SHA	IDEA-CBC-SHA	DHE-RSA-SEED-SHA
ADH-AES128-SHA	ADH-AES128-SHA	ADH-AES128-SHA	DHE-RSA-CAMELLIA128-SHA
ADH-SEED-SHA	ADH-SEED-SHA	ADH-SEED-SHA	DES-CBC3-SHA
ADH-CAMELLIA128-SHA	ADH-CAMELLIA128-SHA	ADH-CAMELLIA128-SHA	EDH-RSA-DES-CBC3-SHA
ADH-AES256-SHA	ADH-AES256-SHA	ADH-AES256-SHA	IDEA-CBC-SHA

SSL V 3.0	TLS 1.0	TLS 1.1	TLS 1.2
ADH-CAMELLIA256-SHA	ADH-CAMELLIA256-SHA	ADH-CAMELLIA256-SHA	ADH-AES256-GCM-SHA384
ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	ADH-AES256-SHA256
			ADH-AES256-SHA
			ADH-CAMELLIA256-SHA
			ADH-AES128-GCM-SHA256
			ADH-AES128-SHA256
			ADH-AES128-SHA
			ADH-SEED-SHA
			ADH-DES-CBC3-SHA
			ADH-CAMELLIA128-SHA
			DHE-DSS-AES256-GCM-SHA384
			DHE-DSS-AES256-SHA256
			DHE-DSS-AES256-SHA
			DHE-DSS-CAMELLIA256-SHA
			DHE-DSS-AES128-GCM-SHA256
			DHE-DSS-AES128-SHA256
			DHE-DSS-AES128-SHA
			DHE-DSS-SEED-SHA
			DHE-DSS-CAMELLIA128-SHA
Default Mode: AES128-SHA DHE-RSA-AES128-SHA	Default Mode: AES128-SHA DHE-RSA-AES128-SHA	Default Mode: AES128-SHA DHE-RSA-AES128-SHA	Default Mode: AES128-SHA256 AES128-GCM-SHA256 AES256-SHA256 AES256-GCM-SHA384 AES128-SHA DHE-RSA-AES128-SHA
Note Default mode represents the supported ciphers with the “SSL Cipher String” that is configured in the Web Security Appliance.			
Note AsyncOS 12.0.1 and later versions support ECDHE related ciphers for TLS 1.0, TLS 1.1, and TLS 1.2.			

Port 22 (SSH Port)

OpenSSH_7.3p1:

1. key_algorithm (7):

- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

2. encryption_algorithm (8):

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- rijndael-cbc@lysator.liu.se
- aes128-ctr
- aes192-ctr
- aes256-ctr

3.mac_algorithms (4):

- hmac-sha1
- hmac-ripemd160
- hmac-ripemd160@openssh.com
- umac-64@openssh.com

Unsupported Ciphers

This section contains the list of unsupported ciphers.

Port 8443 (Management Interface)

SSL V 3.0	TLS 1.0
RC2-CBC-MD5	RC2-CBC-MD5
RC4-MD5	RC4-MD5
IDEA-CBC-MD5	IDEA-CBC-MD5
DES-CBC3-MD5	DES-CBC3-MD5