SSL Settings

SSL Settings

Configure the SSL Settings at either of the following locations:

- **Configuration > Device Management > Advanced > SSL Settings**
- **Configuration > Remote Access VPN > Advanced > SSL Settings**

The ASA uses the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) to support secure message transmission for ASDM, Clientless SSL VPN, VPN, and browser-based sessions. In addition, DTLS is used for AnyConnect VPN client connections. The SSL Settings pane lets you configure SSL versions and encryption algorithms for clients and servers. It also lets you apply previously configured trustpoints to specific interfaces and configure a fallback trustpoint for interfaces that do not have an associated trustpoint.

Note For Release 9.3(2), SSLv3 has been deprecated. The default is now **tlsv1** instead of **any**. The **any** keyword has been deprecated. If you choose **any**, **sslv3**, or **sslv3-only**, the settings are accepted with a warning. Click **OK** to continue. In the next major ASA release, these keywords will be removed from the ASA.

For Version 9.4(1), all SSLv3 keywords have been removed from the ASA configuration, and SSLv3 support has been removed from the ASA. If you have SSLv3 enabled, a boot-time error will appear from the command with the SSLv3 option. The ASA will then revert to the default use of TLSv1.

The Citrix mobile receiver may not support TLS 1.1/1.2 protocols; see https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf for compatibility

Fields

- **Server SSL Version**—Specify the minimum SSL/TLS protocol version that the ASA uses when acting as a server from the drop-down list.

Any	Accepts SSLv2 client hellos and negotiates the highest common version.

SSL V3	Accepts SSLv2 client hellos and negotiates SSLv3 (or greater).
TLS V1	Accepts SSLv2 client hellos and negotiates TLSv1 (or greater).
TLSV1.1	Accepts SSLv2 client hellos and negotiates TLSv1.1 (or greater).
TLSV1.2	Accepts SSLv2 client hellos and negotiates TLSv1.2 (or greater).
DTLSv1	Accepts DTLSv1 client hellos and negotiates DTLSv1 (or greater)
DTLS1.2	Accepts DTLSv1.2 client hellos and negotiates DTLSv1.2 (or greater)

Note The configuration and use of DTLS applies to Cisco AnyConnect remote access connections only.

Ensure the TLS session is as secure, or more secure than the DTLS session by using an equal or higher version of TLS than DTLS. Given this, TLSV1.2 is the only acceptable TLS version when choosing DTLSV1.2; and any TLS version can be used with DTLS1 since they are all equal to or greater than DTLS 1.

- **Client SSL Version**—Specify the minimum SSL/TLS protocol version that the ASA uses when acting as a client from the drop-down list. (DTLS not available for SSL client role)

Any	Transmits SSLv3 client hellos and negotiates SSLv3 (or greater).
SSL V3	Transmits SSLv3 client hellos and negotiates SSLv3 (or greater).
TLS V1	Transmits TLSv1 client hellos and negotiates TLSv1 (or greater).
TLSV1.1	Transmits TLSv1.1 client hellos and negotiates TLSv1.1 (or greater).
TLSV1.2	Transmits TLSv1.2 client hellos and negotiates TLSv1.2 (or greater).

- **Diffie-Hellmann group to be used with SSL**—Choose a group from the drop-down list. Available options are Group1 - 768-bit modulus, Group2 - 1024-bit modulus, Group5 - 1536-bit modulus, Group14 - 2048-bit modulus, 224-bit prime order, and Group24 - 2048-bit modulus, 256-bit prime order. The default is Group2.
- **ECDH group to be used with SSL**—Choose a group from the drop-down list. Available options are Group19 - 256-bit EC, Group20 - 384-bit EC, and Group21 - 521-bit EC. The default value is Group19.

Note ECDSA and DHE ciphers are the highest priority.

- **Encryption**—Specify the version, security level, and SSL encryption algorithms that you want to support. Click **Edit** to define or modify a table entry using the Configure Cipher Algorithms/Custom String dialog box. Choose the SSL cipher security level, then click **OK**.
  - **Cipher Version**—Lists the cipher version that the ASA supports and uses for SSL connections.
  - **Cipher Security Level**—Lists the cipher security levels that the ASA supports and uses for SSL connections. Choose one of the following options:

    All includes all ciphers, including NULL-SHA.

    Low includes all ciphers, except NULL-SHA.

    Medium includes all ciphers, except NULL-SHA, DES-CBC-SHA, RC4-MD5 (this is the default), RC4-SHA, and DES-CBC3-SHA.

    Fips includes all FIPS-compliant ciphers, except NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, and DES-CBC3-SHA.

    High includes only AES-256 with SHA-2 ciphers and applies only to TLS version 1.2.

    Custom includes one or more ciphers that you specify in the Cipher algorithms/custom string box. This option provides you with full control of the cipher suite using OpenSSL cipher definition strings.
  - **Cipher Algorithms/Custom String**—Lists the cipher algorithms that the ASA supports and uses for SSL connections. For more information about ciphers using OpenSSL, see https://www.openssl.org/docs/manmaster/man1/ciphers.html.

    The ASA specifies the order of priority for supported ciphers as: Ciphers supported by TLSv1.2 only then ciphers not supported by TLSv1.1 or TLSv1.2

  The following ciphers are supported as noted:

- **Server Name Indication (SNI)**—Specifies the domain name and to associate with that domain. Click **Add** or **Edit** to define or modify a domain and trustpoint for each interface using the Add/Edit Server Name Indication (SNI) dialog box.

Cipher	TLSv1.1 / DTLS V1	TLSV1.2
AES128-GCM-SHA256	no	yes
AES128-SHA	yes	yes
AES128-SHA256	no	yes
AES256-GCM-SHA384	no	yes
AES256-SHA	yes	yes
AES256-SHA256	no	yes
DERS-CBC-SHA	no	no
DES-CBC-SHA	yes	yes

Cipher	TLSv1.1 / DTLS V1	TLSV1.2
DHE-RSA-AES128-GCM-SHA256	no	yes
DHE-RSA-AES128-SHA	yes	yes
DHE-RSA-AES128-SHA256	no	yes
DHE-RSA-AES256-GCM-SHA384	no	l
DHE-RSA-AES256-SHA	yes	yes
ECDHE-ECDSA-AES128-GCM-SHA256	no	yes
ECDHE-ECDSA-AES128-SHA256	no	yes
ECDHE-ECDSA-AES256-GCM-SHA384	no	yes
ECDHE-ECDSA-AES256-SHA384	no	yes
ECDHE-RSA-AES128-GCM-SHA256	yes	yes
ECDHE-RSA-AES128-SHA256	no	yes
ECDHE-RSA-AES256-GCM-SHA384	no	yes
ECDHE-RSA-AES256-SHA384	no	yes
NULL-SHA	no	no
RC4-MD5	no	no
RC4-SHA	no	no

    - Specify domain—Enter the domain name.
    - Select trustpoint to associate with domain—Choose the trustpoint from the drop-down list.

- **Certificates—**Assign certificates to use for SSL authentication on each interface. Click **Edit** to define or modify the trustpoint for each interface using the Select SSL Certificate dialog box.
    - Primary Enrolled Certificate—Select the trustpoint to use for certificates on this interface.
    - Load Balancing Enrolled Certificate—Select a trustpoint to be used for certificates when VPN load balancing is configured.
- **Fallback Certificate**—Click to choose a certificate to use for interfaces that have no certificate associated with them. If you choose **None**, the ASA uses the default RSA key-pair and certificate.
- **Forced Certification Authentication Timeout**—Configure the number of minutes to wait before timing out certificate authentication.
- **Apply—**Click to save your changes.
- **Reset**—Click to remove changes you have made and reset SSL parameters to the previously defined values.