CHAPTER 9

Configuring SSL Settings

SSL Settings

Configuration > Device Management > Advanced > SSL Settings

Configuration > Remote Access VPN > Advanced > SSL Settings

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

Fields

- **Server SSL Version**—Choose to specify the SSL/TLS protocol version the ASA uses to negotiate as a server. You can make only one selection.

Any	The ASA accepts SSL version 2 client hellos, and negotiates either SSL version 3 or TLS version 1.
Negotiate SSL V3	The ASA accepts SSL version 2 client hellos, and negotiates to SSL version 3.
Negotiate TLS V1	The ASA accepts SSL version 2 client hellos, and negotiates to TLS version 1.
SSL V3 Only	The security appliance accepts only SSL version 3 client hellos, and uses only SSL version 3.
TLS V1 Only	The security appliance accepts only TLSv1 client hellos, and uses only TLS version 1.

Note To use port forwarding for Clientless SSL VPN, you must select Any or Negotiate SSL V3. The issue is that JAVA only negotiates SSLv3 in the client Hello packet when you launch the Port Forwarding application.

- **Client SSL Version—**Choose to specify the SSL/TLS protocol version the ASA uses to negotiate as a client. You can make only one selection.

any	The ASA sends SSL version3 hellos, and negotiates either SSL version 3 or TLS version 1.
sslv3-only	The security appliance sends SSL version 3 hellos, and accepts only SSL version 3.
tlsv1-only	The security appliance sends TLSv1 client hellos, and accepts only TLS version 1.

- **Encryption**—Add the SSL encryption algorithms you want to support.
  - **Available Algorithms**—Lists the encryption algorithms the ASA supports that are not in use for SSL connections. To use, or make active, an available algorithm, highlight the algorithm and click **Add**.
  - **Active Algorithms**—Lists the encryption algorithms the security appliance supports and is currently using for SSL connections. To discontinue using, or change an active algorithm to available status, highlight the algorithm and click **Remove**.
  - **Add/Remove**—Click to change the status of encryption algorithms in either the Available or Active Algorithms columns.
  - **Move Up/Move Down**—Highlight an algorithm and click these buttons to change its priority. The ASA attempts to use an algorithm
- **Certificates—**Assign certificates to use for SSL authentication on each interface. Click **Edit** to define or modify the Trustpoint for each interface. Trustpoints are configured on Configuration
  - 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 select a certificate to use for interfaces that have no certificate associated with them. If you select **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 apply your changes.
- **Reset**—Click to remove changes you have made and reset SSL parameters to the values that they held when you opened the window.

SSL