



SSL VPN Wizard

SSL VPN Feature

Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. Users have no direct access to resources on the internal network.

The Cisco AnyConnect VPN client provides secure SSL connections to the security appliance for remote users with full VPN tunneling to corporate resources. Without a previously-installed client, remote users enter the IP address in their browser of an interface configured to accept clientless SSL VPN connections. The security appliance downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates. In the case of a previously installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

Fields

- **Clientless SSL VPN Access**—Enables clientless, browser-based connections for specific, supported internal resources through a portal page.
- **Cisco SSL VPN Client (AnyConnect VPN Client)**—Enables SSL VPN client connections for full network access. Enables the security appliance to download the AnyConnect client to remote users.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

SSL VPN Interface

Provide a Connection name (previously called *tunnel group*), enable an interface for SSL VPN connections, and provide digital certificate information in this window.

Fields

- Connection Name—Provide a connection name for this group of connection-oriented attributes.
- SSL VPN Interface—Specify the interface to allow SSL VPN connections.
- Digital Certificate—Specify a certificate, if any, that the security appliance sends to the remote PC.
 - Certificate—Specify the name of the certificate.
- Connection Group Settings—You can enable the security appliance to display a group alias for this connection on the login page.
 - Connection Group Alias—Specify an alias name for the connection.
 - Display Group Alias list at the login page—Enable to display the group alias.
- Information—Displays information remote users need for establishing SSL VPN connections and ASDM connections.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

User Authentication

Specify authentication information on this screen.

Fields

- Authenticate using a AAA server group—Enable to let the security appliance contact a remote AAA server group to authenticate the user.
- AAA Server Group Name—Select a AAA server group from the list of pre-configured groups, or click **New** to create a new group.
- Authenticate using the local user database—Add new users to the local database stored on the security appliance.
 - Username—Create a username for the user.
 - Password—Create a password for the user.
 - Confirm Password—Re-type the same password to confirm.
 - Add/Delete—Add or delete the user from the local database.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Group Policy

Group policies configure common attributes for groups of users. Create a new group policy or select an existing one to modify.

Fields

- Create new group policy—Enable to create a new group policy. Provide a name for the new policy.
- Modify existing group policy—Select an existing group policy to modify.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Bookmark List

Bookmark lists appear on the portal page for Clientless, browser-based connections. SSL VPN client users do not see these bookmarks. Create a new bookmark list on this window.

Fields

- Bookmark List—Select an existing list or click **Manage** to create a new list, or import or export bookmark lists.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

IP Address Pools and Client Image

Provide a range of IP addresses to remote SSL VPN users and identify SSL VPN client images to the security appliance in this window.

Fields

- IP Address Pool—SSL VPN clients receive new IP addresses when they connect to the security appliance. Clientless connections do not require new IP addresses. Address Pools define a range of addresses that remote clients can receive.
- IP Address Pool—Select an existing IP Address Pool, or click **New** to create a new pool.
- AnyConnect VPN Client Image Location—Identify to the security appliance files in flash memory that are SSL VPN client images. Click **Browse** to locate images on your local PC.
 - Location—Provide the path and filename of a valid SSL VPN client image located in flash memory.
 - Download Latest AnyConnect VPN Client form CCO—Click this link to go to the Software Download page for the latest client image.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Summary

Provides a summary of your selections from the previous wizard windows.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

