



Configuring the Security Appliance to Deploy the AnyConnect Client

This chapter describes how to use ASDM to configure the security appliance to deploy the AnyConnect client. To use CLI to configure the security appliance, see the *Cisco 5500 Series Adaptive Security Appliance CLI Configuration Guide*.

This chapter includes the following sections:

- How the Security Appliance Deploys the AnyConnect Client, page 2-1
- Before You Install the AnyConnect Client, page 2-2
- Configuring the Security Appliance to Download the AnyConnect Client, page 2-5
- Prompting Remote Users for AnyConnect Client Download, page 2-9
- Enabling Modules for Additional AnyConnect Features, page 2-10
- Configuring Certificate-only Authentication, page 2-11

How the Security Appliance Deploys the AnyConnect Client

The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. Without a previously-installed client, remote users enter the IP address or DNS name in their browser of an interface configured to accept clientless SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.

A security appliance uses data that is stored in filtering tables to evaluate and match URL request attributes such as domain names and IP address path segments with locally maintained database records. If a match occurs, access policy settings determine an action to block or monitor the traffic. If no match occurs, processing continues.

After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it 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 version of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it attempts to connect using Datagram Transport Layer Security (DTLS). DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. If it cannot establish a DTLS connection, it falls back to Transport Layer Security (TLS).

The security appliance downloads the client based on the group policy or username attributes of the user establishing the connection. You can configure the security appliance to automatically download the client, or you can configure it to prompt the remote user, asking them if they want to download the client. In the latter case, if the user does not respond, you can configure the security appliance to either download the client after a timeout period or present the login page.

Before You Install the AnyConnect Client

The following sections contain recommendations to ensure successful AnyConnect client installation, as well as tips about certificates, Cisco Security Agent (CSA), adding trusted sites, and responding to browser alerts:

- Ensuring Automatic Installation of AnyConnect Clients, page 2-2
- Adding a Security Appliance to the List of Trusted Sites (IE), page 2-3
- Adding a Security Certificate in Response to Browser Alert Windows, page 2-4

Ensuring Automatic Installation of AnyConnect Clients

The following recommendations and caveats apply to the automatic installation of AnyConnect client software on client PCs:

- To minimize user prompts during AnyConnect client setup, make sure certificate data on client PCs and on the security appliance match:
 - If you are using a Certificate Authority (CA) for certificates on the security appliance, choose one that is already configured as a trusted CA on client machines.
 - If you are using a self-signed certificate on the security appliance, be sure to install it as a trusted root certificate on clients.

The procedure varies by browser. See the procedures that follow this section.

 Make sure the Common Name (CN) in security appliance certificates matches the name clients use to connect to it. By default, the security appliance certificate CN field is its IP address. If clients use a DNS name, change the CN field on the security appliance certificate to that name.

If the certificate has a SAN (Subject Alternate Name) then the browser will ignore the CN value in the Subject field and look for a DNS Name entry in the SAN field.

If users connect to the ASA using its hostname, the SAN should contain the hostname and domain name of the ASA. For example, the SAN field would contain DNS Name=hostname.domain.com.

If users connect to the ASA using its IP address, the SAN should contain the IP address of the ASA. For example, the SAN field would contain DNS Name=209.165.200.254.

• The Cisco Security Agent (CSA) might display warnings during the AnyConnect client installation.

Current shipping versions of CSA do not have a built-in rule that is compatible with the AnyConnect client. You can create the following rule using CSA version 5.0 or later by following these steps:

Step 1 In Rule Module: "Cisco Secure Tunneling Client Module", add a FACL:

Priority Allow, no Log, Description: "Cisco Secure Tunneling Browsers, read/write vpnweb.ocx" Applications in the following class: "Cisco Secure Tunneling Client - Controlled Web Browsers" Attempt: Read file, Write File

On any of these files: @SYSTEM\vpnweb.ocx

Step 2 Application Class: "Cisco Secure Tunneling Client - Installation Applications" add the following process names:

```
**\vpndownloader.exe
@program_files\**\Cisco\Cisco AnyConnect VPN Client\vpndownloader.exe
```

We recommend that Microsoft Internet Explorer (MSIE) users add the security appliance to the list of trusted sites, or install Java. The latter enables the ActiveX control to install with minimal interaction from the user. This is particularly important for users of Windows XP SP2 with enhanced security. Windows Vista users *must* add the security appliance to the list of trusted sites in order to use the dynamic deployment feature. For more information, see Adding a Security Appliance to the List of Trusted Sites (IE), page 2-3.

Adding a Security Appliance to the List of Trusted Sites (IE)

To add a security appliance to the list of trusted sites, use Microsoft Internet Explorer and do the following steps.

This is required on Windows Vista to use WebLaunch.
Go to Tools Internet Options.
The Internet Options window opens.
Click the Security tab.
Click the Trusted Sites icon.
Click Sites.
The Trusted Sites window opens.
Type the host name or IP address of the security appliance. Use a wildcard such as https://*.yourcompany.com to allow all ASA 5500s within the yourcompany.com domain to be used to support multiple sites.
Click Add.
Click OK.
The Trusted Sites window closes.
Click OK in the Internet Options window.

Adding a Security Certificate in Response to Browser Alert Windows

This section explains how to install a self-signed certificate as a trusted root certificate on a client in response to the browser alert windows.

In Response to a Microsoft Internet Explorer "Security Alert" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a Microsoft Internet Explorer Security Alert window. This window opens when you establish a Microsoft Internet Explorer connection to a security appliance that is not recognized as a trusted site. The upper half of the Security Alert window shows the following text:

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate. The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

Install the certificate as a trusted root certificate as follows:

Step 1 Click View Certificate in the Security Alert window. The Certificate window opens. Click Install Certificate. Step 2 The Certificate Import Wizard Welcome opens. Click Next. Step 3 The Certificate Import Wizard - Certificate Store window opens. Step 4 Select "Automatically select the certificate store based on the type of certificate." Step 5 Click Next. The Certificate Import Wizard - Completing window opens. Click Finish. Step 6 Step 7 Another Security Warning window prompts "Do you want to install this certificate?" Click Yes. The Certificate Import Wizard window indicates the import is successful. Step 8 Click OK to close this window. Click OK to close the Certificate window. Step 9 Click Yes to close the Security Alert window. Step 10

The security appliance window opens, signifying the certificate is trusted.

In Response to a Netscape, Mozilla, or Firefox "Certified by an Unknown Authority" Window

The following procedure explains how to install a self-signed certificate as a trusted root certificate on a client in response to a "Web Site Certified by an Unknown Authority" window. This window opens when you establish a Netscape, Mozilla, or Firefox connection to a security appliance that is not recognized as a trusted site. This window shows the following text:

Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.

Install the certificate as a trusted root certificate as follows:

- Step 1 Click the Examine Certificate button in the "Web Site Certified by an Unknown Authority" window. The Certificate Viewer window opens.
- **Step 2** Click the "Accept this certificate permanently" option.
- Step 3 Click OK.

The security appliance window opens, signifying the certificate is trusted.

Ensuring Fast Connection Time when Loading Multiple AnyConnect Client Images

When you load multiple AnyConnect client images on the security appliance, you should order the images in a manner that ensures the fastest connection times for greatest number of remote users.

The security appliance downloads portions of the client images to the remote computer until it achieves a match with the operating system. It downloads the image at the top of the ordered list first. Therefore, you should assign the image that matches the most commonly-encountered operating system used on remote computers to the top of the list.

Because mobile users have slower connection speeds, you should load the AnyConnect client image for Windows Mobile at the top of the list.

For mobile users, you can decrease the connection time of the mobile device by using the regex keyword. When the browser connects to the adaptive security appliance, it includes the User-Agent string in the HTTP header. When the adaptive security appliance receives the string, if the string matches an expression configured for an image, it immediately downloads that image without testing the other client images.

Configuring the Security Appliance to Download the AnyConnect Client

To prepare the security appliance to deploy the AnyConnect client, complete these steps:

- Step 1 Download the latest Cisco AnyConnect Secure Mobility client package from the Cisco AnyConnect Software Download webpage.
- Step 2 Specify the AnyConnect client package file as an SSL VPN client.

Navigate to **Configuration > Remote Access VPN > Network Access > Advanced > SSL VPN > Client Settings**. The SSL VPN Client Settings panel displays. (Figure 2-1).

This panel lists AnyConnect client files that have been identified as client images. The order in which they appear in the table reflects the order the security appliance downloads them to the remote computer.

To add a client image, click **Add** in the SSL VPN Client Images area. Enter the name of the file you downloaded from Cisco.com and click **Upload**. You can also browse your computer for the file.

L

Remote Access VPN 🗗 🕀 🗙	Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client	
Introduction AnyConnect Connection Profiles Dynamic Access Group Policies Group Policies Mobile User Security AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Profile Address Assignment Address SSL VPN Access Address SSL VPN Access Address Client Settings Address SSL VPN Access Address Client Settings Address Client Settings Address SSL VPN Access Address Client Settings Address Client Settings Address SSL VPN Access Address SSL VPN Access Address Client Settings Address SSL VPN Access Address SSL VPN Access Address Client Settings Address SSL VPN Access Address Acces	Identify AnyConnect Client related files. AnyConnect Client Images The regular expression is used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list. Image Regular expression to match user-agent Image Regular expression to match user-agent AnyConnect VPI Client Profiles	
A Device Setup	Name Package	
Firewall Image: State Access VPN Image: State Access VPN		
Device Management	AnyConnect Image: disk0:/anyconnect-win-2.5[k9.pkg Browse Flash	
	Regular expression to match user-agent	۲
	OK Cancel Help	

Figure 2-1 Specify AnyConnect Client Images

Step 3 Configure a method of address assignment.

You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a tunnel group. This guide uses the popular address pools method as an example.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools (Figure 2-2).** Enter address pool information in the Add IP Pool window.

Remote Access VPN Image: Comparison of the second	Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools Image: Configuration > Configure named IP Address Pools. The IP Address Pools can be used in either a VPN IPsec Connection Profiles, AmcConnect Connection Profiles or Group Policies configuration.
Cynamic Access Policies Group Policies Group Policies IPsec Connection Profiles Secure Mobility Solution Assignment Policy Assignment Policy	Pool Naite Starting Address Ending Address/Number of Addresses Subnet Mask/Prefix Length
Add@issr000s Add@issr000s Add@issr000s Add@issr00s Add@i	Name: Engineering Starting IP Address: 209.165.201.1 Ending IP Address: 209.165.201.30
() Firewall 중전 Remote Access VPN 중권 Site-to-Site VPN	Subnet Mask: 255.255.255.224
Device Management	Apply Reset

Figure 2-2 Add IP Pool Dialog

Step 4 Enable client download and assign the address pool in a connection profile.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. Follow the arrows in (Figure 2-3) to enable the AnyConnect client and then assign an address pool.

Remote Access VPN	P × Configuration	> Remote Access VPN >	Network (Client) Access > SSI	VPN Connection Profiles	
7 Introduction	The security	appliance automatically dep	loys the Cisco AnyConnect VPN Cli	ent or legacy SSL VPN Client to remote	
 Network (Client) Access 	users upon o	onnection. The initial client o	leployment requires end-user admi	inistrative rights. The Cisco AnyConnect	
AnyConnect Connection	VPN Client su	ipports the HTTPS/TCP (SSL) and Datagram Transport Layer S	ecurity (DTLS) tunneling options.	
Group Policies	5				
Dypamic Access Policies	(More client-	related parameters, such a	s client images and client profiles of	an be found at Client Settings)	
Mobile Liser Security	(more clienc	rolaced parameters, sacria.	clone inages and clone promos, e	and round at chore security	
AnyConnect Customiza	tion/Local				
AnyConnect Client Prof	le Adess Inter	faces			
- AnyConnect Client Sett	ings	isco ApyCoppect VPN Cliept	or legacy SSL VPN Cliept access or	the interfaces selected in the table below	
😠 🖣 Address Assignment			or logacy soc in it clone accoss of		
🖅 🗒 Advanced	Interface	Allow Access	Require Client Certificate	Enable DTLS	
E Tentless SSL VPN Access	outside	✓			
🗟 🚽 🚽 AAA/Local Users	inside	✓		✓	
🗄 🚮 Secure Desktop Manager	management	t 📃			
🛛 🛐 Certificate Management	test				
DHCP Server	Access Ports	443 DTICD	ort: 443		
DNS	ALLESS PUTC	DILSP			
arred Advanced	Click here to	Assian Certificate to Interf.	ace.		
	Cildrenol 6 Co				
	Connection P	rofiles			
Q Deuice Setup	Connection p	profile (tunnel group) table b	elow contains records that determ	ine connection policies. A record identifies	
Device Secup	a derauit gro	ap policy for the connection	and contains protocol-specific con	nection parameters.	
🕵 Firewall	🖨 Add 🗹	(Edit) 📋 Delete			
w.o	Name 2	Aliases	SSL VPN Client Protocol	Group Policy	
Remote Access VPN	DefaultRAG	'0 0 0	Enabled	DfltGrpPolicy	
- <u>-</u>	DefaultWEB!	VENGroup DefaultSSI Policy	Enabled	DfltGroPolicy	
Site-to-Site VPN	Engineering	Engineering	Enabled	DfltGrpPolicy	
<u> </u>	Sales	Sales	Enabled	DfltGrpPolicy	
Device Management				,	
		antine Deefiles Faster	un efferer.		
	E LUIT SOL VPIN CUI	iection Prome: Engine	ering		
onfiguration changes saved suc	Basic				
oningaradon anangos savoa sac		Global Llient Addr	ess Assignment Policy —		
	Advanced	This policy affects	ess Assignment Policy all Network (Client) Access connec	tions. The following are tried in order until an	
	Advanced General	This policy affects address is found.	ess Assignment Policy all Network (Client) Access connec	tions. The following are tried in order until an	
	Advanced General Client Addressing	This policy affects address is found.	ess Assignment Policy all Network (Client) Access connec	tions. The following are tried in order until an	
	Advanced General Client Addressing Authentication	This policy affects address is found.	ess Assignment Policy all Network (Client) Access connec ation server	tions. The following are tried in order until an	_
	Advanced General Client Addressing Authentication	This policy affects address is found.	ess Assignment Policy all Network (Client) Access connec	tions. The following are tried in order until an	
	Advanced General Client Addressing Authentication Authorization	This policy affects address is found.	ess Assignment Policy all Network (Client) Access connec ation server	tions. The following are tried in order until an	
	Advanced General Client Addressing Authentication Authentization Accounting SSI VPN	This policy affects address is found. Use authentice Use DHCP	ess Assignment Policy all Network (Client) Access connec ition server	tions. The following are tried in order until an	
	 Advanced General Client Addressing Authentication Authorization Accounting SSL VPN 	Global Lilent Addr This policy affects address is found. Use authentice Use DHCP	ess Assignment Policy all Network (Client) Access connec ation server	tions. The following are tried in order until an	
	■ Advanced General Client Addressing Authentication Authentication Accounting SSL VPN	Global Lilent Addr This policy affects address is found. Use authentica Use DHCP V Use address pu Allow the	ess Assignment Policy all Network (Client) Access connec tion server pol	tions. The following are tried in order until an minutes after it is released.	
	Advanced General Client Addressing Authorization Accounting SSL VPN	Giobal Lilence Addr This policy affects: address is found. Use authentica Use DHCP Use address pr Allow the	ess Assignment Policy all Network (Client) Access connec ition server sol	tions. The following are tried in order until an minutes after it is released.	
	Advanced General Client: Addressing Authentication Authorization Accounting SSL VPN	Giobal Lilent Ador This policy affects address is found. Use authentice Use DHCP Use address pr Allow the Interface-Specific	ess Assignment Policy all Network (Client) Access connec bion server pol reuse of an IP address	tions. The following are tried in order until an	
	Advanced General Clent Addressing Authorization Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address p Allow the Interface-Specific	ess Assignment Policy	tions. The following are tried in order until an minutes after it is released.	
	Advanced General Clienk Addressing Authentication Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address p Allow the Interface-Specific	ess Assignment Policy all Network (Client) Access connec tition server sol reuse of an IP address Address Pools Delete	tions. The following are tried in order until an minutes after it is released.	
	Advanced General Clerek Addressing Authentication Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address pr Allow the Interface Specific	ess Assignment Policy all Network (Client) Access connec all network all network (Client) Access connec all network on server sol reuse of an IP address Address Pools Delete Address Pools	tions. The following are tried in order until an minutes after it is released. fress Pools	
	Advanced General Client: Addressing Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address p Allow the Interface	all Network (Client) Access connect all Network (Client) Access connect ation server and reuse of an IP address Address Pools	tions. The following are tried in order until an minutes after it is released.	
	Advanced General Clienk Addressing Authentication Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use address p Use address p Allow the Interface Specific Interface	all Network (Client) Access connection server sol Address Pools	tions. The following are tried in order until an minutes after it is released. fress Pools	
	Authentication Authentication Acuthentication Acuthentication SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address pr Allow the Interface Specific Interface	all Network (Client) Access connect all Network (Client) Access connect ation server cool reuse of an IP address Address Pools Delete Address Pools Client Assign Address P	tions. The following are tried in order until an minutes after it is released.	
	Advanced General Clent Addressing Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address p Allow the Interface	all Network (Clent) Access connect all Network (Clent) Access connect ation server and reuse of an IP address Address Pools Delete Address Pools Content Address P Interface: inside	tions. The following are tried in order until an minutes after it is released. tress Pools cole to Interface	
	Advanced General Clenck Addressing Authentication Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use address p Use address p Allow the Interface Specific Interface	ess Assignment Policy all Network (Client) Access connec tition server col reuse of an IP address Address Pools Address Pools Interface: inside Address Pools:	tions. The following are tried in order until an minutes after it is released. tress Pools tools to Interface	
	Advanced General Clerk Addressing Authentication Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address pu Allow the Interface Specific Interface	all Network (Client) Access connect all Network (Client) Access connect ation server add reuse of an IP address Address Pools Delete Address Pools Interface: Inside Address Pools	tions. The following are tried in order until an minutes after it is released. fress Pools tools to Interface) Select
	Advanced General Clenck Addressing Authorization Authorization Accounting SSL VPN	This poly: Affects address is found. Use authentice Use DHCP Use address p Allow the Interface Ot	all Network (Clent) Access connect all Network (Clent) Access connect ation server and reuse of an IP address Address Pools Delete Address Pools Interface: inside Address Pools: Pools	tions. The following are tried in order until an minutes after it is released. tress Pools cole to Interface	Feelect
	Advanced General Clerk Addressing Authentication Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address p Allow the Interface Specific Interface	ess Assignment Policy all Network (Client) Access connec tition server col reuse of an IP address Address Pools Address Pools Interface: inside Address Pools: Pools	tions. The following are tried in order until an minutes after it is released. tress Pools tools to Interface	Forest X
	Advanced General Clerk Addressing Authentication Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address pu Allow the Interface Specific Interface	ess Assignment Policy all Network (Client) Access connec ation server add reuse of an IP address Address Pools Delete Address Pools Interface: Inside Address Pools Delete	tions. The following are tried in order until an minutes after it is released. fress Pools code to Interface	Celect
	Advanced General Clenck Addressing Authorization Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address p Allow the Interface Of Select Address Of Colores	Address Pools Delete Starting Address Starting Addres	tions. The following are tried in order until an minutes after it is released.	×
	Advanced General Clerk Addressing Authentication Accounting SSL VPN	This poly: affects address is found. Use authentice Use address is found. Use address p Use address p Allow the Interface-Specific Add Carl Interface	ess Assignment Policy all Network (Client) Access connection server col reuse of an IP address Address Pools Delete Address Pools Interface: inside Address Pools: Pools Delete Starting Address _ Er 209, 155, 201, 1 _ 27	tions. The following are tried in order until an minutes after it is released. tress Pools tests to Interface a test to Interface b t) Colect
	Advanced General Clerk Addressing Authentication Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use address pr Use address pr Allow the Interface Of Select Address Col Select Address Col Select Address Col Select Address Col Select Address	ess Assignment Policy all Network (Client) Access connec all network (Client) Access connec ation server and the server and th	tions. The following are tried in order until an minutes after it is released. tress Pools science in the following and the following and the following are tried in order until an science in the following are tried in order until an science in the following are tried in order until an tries after it is released.	
	Advanced General Clenck Addressing Authorization Authorization Accounting SSL VPN	This poly: affects address is found. Use authentics Use DHCP Use address p Allow the Interface OV Select Address Add Edt Poly me Eropromo Assigned Address	ess Assignment Policy all Network (Clent) Access connec ation server abol Address Pools Delete Interface: inside Address Pools: Pools Starting Address i Er (209-165/201.1) 20	tions. The following are tried in order until an minutes after it is released. tress Pools cole to Interface ading Address Subnet Mask 19.165.201.30 Subnet Mask 255.255.225.224	Celect
	Advanced General Clerk Addressing Authentication Actuorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use address is found. Use address pr Use address pr Allow the Interface-Specific Add Ede Interface	ess Assignment Policy all Network (Client) Access connec all network (Client) Access c	tions. The following are tried in order until an minutes after it is released. tress Pools to Interface to In	Celect
	Advanced General Clerk Addressing Authentication Acuthentication Accounting SSL VPN	This poly: affects address is found. Use authentice Use address is found. Use address pr Use address pr Allow the Interface OV Interface OV Interface OV Is Select Address COV Is Select Address COV Is Select Address Assigned Address Assigned Address Cov	ess Assignment Policy all Network (Client) Access connec ation server abol Address Pools Delete Address Pools Interface: Inside Address Pools Delete Starting Address Er 209.165.201.1 20 s Pools	tions. The following are tried in order until an minutes after it is released. tress Pools octs to Interface ading Address Subnet Mask 19,165,201,30 255,255,224	≯(saec
	Advanced General Clenk Addressing Authentication Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address p Allow the Interface Or Select Address Add Edit Poly and Add Edit Poly and Add Edit Poly and Add Edit Poly and Add Edit Poly and Add Edit	ess Assignment Policy all Network (Clent) Access connec bition server bol Address Pools Delete Starting Address Pools: Pools Delete Starting Address Er Starting Address Er	tions. The following are tried in order until an minutes after it is released. tress Pools cole to Interface a mding Address Subnet Mask P9.165.201.30 Subnet Mask	Celect
	Advanced General Clerk Addressing Authentication Actuberization Accounting SSL VPN	This poly: affects address is found. Use authentice Use DHCP Use address pu Alow the Interface Specific add Edit Interface	ess Assignment Policy all Network (Client) Access connec abion server add Address Pools Delete Address Pools Delete Starting Address Er 209.165.201.1 200.101.1	tions. The following are tried in order until an minutes after it is released. tress Pools test to Interface the second s	
	Advanced General Clerk Addressing Authentication Authorization Accounting SSL VPN	This poly: affects address is found. Use authentice Use address is found. Use address pr Use address pr Allow the Interface OV Select Address OV Select Address OV Select Address Colored Deal Grane Assigned Address Engineering Assigned Address Engineering	ess Assignment Policy all Network (Client) Access connec abion server abion server Address Pools Delete Address Pools Delete Starting Address Exarting Address Starting Address Starting Address Starting Address Construction Starting Address Construction Starting Address Construction Starting Address Construction Starting Address Construction	tions. The following are tried in order until an minutes after it is released. tress Pools cold to Interface ading Address Subnet Mask 19.165.201.30 255.255.224 el Help	> Gelect

Figure 2-3 Enable SSL VPN Client Download

Step 5 Specify SSL VPN as a permitted VPN tunneling protocol for a group policy.

Navigate to **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**. The Group Policies panel displays. Follow the arrows in Figure 2-4 to enable SSL VPN for the group.

	Configuration > Re	mote Access VPN > Ne	twork (Llient) Access > 6	roup Policies			
Introduction Network (Client) Access AnyConnect Connection Profiles GAnyConnect Customization/Loca GAnyConnect Client Profile GAnyConnect Client Settings Dynamic Access Policies	Manage VPN group pairs that may be policy information To enforce author & Add • I to Enforce	Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts. To enforce authorization attributes from an LDAP server you must use an <u>LDAP attribute map</u> .					
Group Policies	Name	Туре	Tunneling Protocol	AAA Server Group			
IPsec Connection Profiles	nat-exempt-group	policy Internal	Inherited	N/A			
	DfltGrpPolicy (Sys	em Default) 🛛 Internal	IPSec,L2TP-IPSec,webvpn	N/A			
Advanced							
Clie	aliew DfltCroDaliev	+					
	oney. Driter proney						
General	Name: Dflto	rpPolicy					
Servers	. T				7		
	Banner:						
	Address Pools:				Select		
1 riew							
	IPV6 Address Pools:				Select		
Cal site	More Options				۲		
	Turneline Durhanda				TD/ID		
5 Devic	Tunneling Protocols:		ICLESS SOL VPN		TP/IPSec		
	IPv4 Filter:	None	·	✓	Manage		
	IPv6 Filter:	None	·	▼ (Manage		
	NAC Policy:	None	·	▼	Manage		
	Access Hours:	Unre	stricted	▼ [Manage		
	Simultaneous Logins:	3					
	Restrict access to VLAN:	Unre	stricted	~			
	Connection Profile (Tunn	el Group) Lock: None	ı	~			
	Maximum Connect Time:	Unlin	mited minutes				
	Idle Timeout:	🔄 Unlii	mited 30 minutes				

Figure 2-4 Specify SSL VPN as a Tunneling Protocol

Prompting Remote Users for AnyConnect Client Download

By default, the security appliance does not download the AnyConnect client when the remote user initially connects using the browser. After users authenticate, the default clientless portal page displays a Start AnyConnect Client drawer that users can select to download the client. Alternatively, you can configure the security appliance to immediately download the client without displaying the clientless portal page.

You can also configure the security appliance to prompt remote users, providing a configured time period within which they can choose to download the client or go to the clientless portal page.

You can configure this feature for a group policy or user. To change these login settings, follow this procedure:

- Step 1 Go to Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Select a group policy and click Edit. The Edit Internal Group Policy window displays (Figure 2-5).
- Step 2 In the navigation pane, Select Advanced > SSL VPN Client > Login Settings. The Post Login settings display. Deselect the Inherit check box, if necessary, and select a Post Login setting.

If you choose to prompt users, specify a timeout period and select a default action to take when that period expires in the Default Post Login Selection area.

L

Remote Access VPN	o t ×	Configuration > Remote Acces	s VPN > Netwo	rk (Client) Acces	s > Group Policies	
Introduction Network (Client) AnyConnect Tysec Connect Group Policies Group Policies AnyConnect AnyConnect AnyConnect Address Assig	Access Connection Profiles tion Profiles uss Policies Customization priment	Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts. To enforce authorization attributes from an LDAP server you must use an <u>LDAP attribute</u> map. Add To Edit Delete				
		Name	Type	Tunneling Pro	AAA Server Group	1
A Device Setup		Engineering	Internal	svc.IPSec.web	N/A	
<u></u>		DfltGrpPolicy (System Default)	Internal	svc,IPSec,web	N/A	
Firewall						
Remote Access VI	🚰 Edit Internal Gro	oup Policy: DfltGrpPolicy				×
Site-to-Site VPN	General Servers	After successfully logging to clientless SSL VPN port	in, user can hav al page. The follo	e the choice to dow owing settings decid	nload the client softwa es what will happen.	re, or go
Device Manageme	Advanced					
	Split Tunneling	Post Login Setting				
	IE Browser Pro	O Do not prompt use	er to choose			
	Login Setti	ng 💿 Prompt user to ch	oose			
	Key Regen Dead Peer	Detectic User has 15	seconds to ch	oose, or Default Po	st Login Selection belov	v is taken.
	Customizat	tion Default Post Login Selecti	on			
	a soc cabite	O Go to Clientless St	5L VPN portal			
	<	Download SSL VP	I Client			
	Find:	🔘 N	ext 🛛 🙆 Previ	DUS		
		ОК	Cancel	Help		

Figure 2-5 Changing Login Settings

Step 3 Click **OK** and be sure to apply your changes to the group policy.

Figure 2-6 shows the prompt displayed to remote users if you choose **Prompt user to choose** and **Download SSL VPN Client**:

Figure 2-6 Post Login Prompt Displayed to Remote Users



Enabling Modules for Additional AnyConnect Features

As new features are released for the AnyConnect client, you must update the AnyConnect clients of your remote users for them to use the new features. To minimize download time, the AnyConnect client requests downloads (from the security appliance) only of modules that it needs for each feature that it supports.

To enable new features, you must specify the new module names as part of the group-policy or username configuration. To enable module download for a group policy, follow this procedure:

- **Step 1** Go to Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Select a group policy and click **Edit**. The Edit Internal Group Policy window displays (Figure 2-7).
- **Step 2** In the navigation pane, select Advanced > SSL VPN Client. Click the Optional Client Module to Download drop-list and select a module.



Figure 2-7 Specifying an Optional Client Module to Download

Step 3 Click **OK** and be sure to apply your changes to the group policy.

If you choose Start Before Logon, you must also enable this client feature in the AnyConnect client profile. See Configuring AnyConnect Client Features for details.

Configuring Certificate-only Authentication

You can specify whether you want users to authenticate using AAA with a username and password or using a digital certificate (or both). When you configure certificate-only authentication, users can connect with a digital certificate and are not required to provide a user ID and password.

You can configure certificate-only authentication in connection profiles. To enable this setting, follow this procedure:

L

Step 1 Go to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles. Select a connection profile and click Edit. The Edit SSL VPN Connection Profile window displays (Figure 2-8).

Remote Access VPN	Configuration > Remote A	cess VPN > Network	(Client) Access > Ar	nvConnect Connection	Profiles 🗖
Introduction Network (Client) Access AnyConnect Connection Profiles Dese Connection Profiles	The security appliance autor users upon connection. The VPN Client supports the HTT	natically deploys the Cis initial client deployment PS/TCP (SSL) and Datag	co AnyConnect VPN Clie requires end-user admir ram Transport Layer Se	ent or legacy SSL VPN Clier nistrative rights. The Cisco ecurity (DTLS) tunneling op	t to remote AnyConnect tions.
Group Policies	(More client-related parame	ters, such as client imag	jes and client profiles, c	an be found at <u>Client Setti</u>	ngs.)
Address Assignment	Access Interfaces				
Advanced Glientless SSL VPN Access	Enable Cisco AnyConne	t VPN Client or legacy S	SL VPN Client access on	the interfaces selected in	the table below
AAA/Local Users	Interface 🔬 🛛 Allow	Access Requir	re Client Certificate	Enable DTLS	
Secure Desktop Manager Certificate Management	inside			 Image: A start of the start of	
E - Contractor Hanagement	management				
Load Balancing	outside	 		~	
DHCP Server					
	Access Port: 443	DTLS Port: 443			
~	Click here to Assign Certific	ate to Interface.			
	Login Page Setting				
	Allow user to select con	action profile, identified	by its alias, on the logi	n narre. Otherwice	
	DefaultWebVPNGroup w	ill be the connection pro	file.	n page, ocherwise,	
	Concertion Define				
A Device Setup	Connection Profiles	roup) specifies how user	is authenticated and of	ther parameters	
			is authenticated and of	uter parameters.	
Firewall	Add Edit Dele	te			
Remote Access VPN	Name 🚈 🛛 En	abled A	liases	Authentication Method	
2 Site-to-Site VPN	DefaultRAGroup		foultSSI Dolicy 0	AA(LOCAL)	<u>^</u>
	Edit SSL VPN Connecti	on Profile: Default	RAGroup		
Device Management					
» *	Basic	Name:	DefaultRAGroup		
	±#dvanced	Aliases:			
		Authoritication			
		Mothod		-ata 🔿 Bath	
		mechou:		ate O both	
		AAA Server Group:	LDAP	*	Manage
			Use LOCAL if Ser	ver Group fails	
		Charle address actions			
		Client Address Assignt			
		DHCP Servers:			
		Client Address Pools	Engineering		Select
		Default Group Policy -			
		Group Policy:	DfltGrpPolicy	~	Manage
		a oup roney r	(Following field is an	attribute of the group polic	v celected above)
			(Policiwing field is an a	accubace or one group polic	y selected above.)
			Enable SSL VPN C	lient protocol	
	Find		A Next	12	
	Fillid:		Previou		
		ОК	Cancel H	ielp	
		ОК	Cancel H	lelp	

Figure 2-8 Configuring Certificate-Only Authentication

- **Step 2** In the Authentication area, enable the method Certificate.
- **Step 3** (Optional) You can assign a specific certificate to an interface. Click Require Client Certificate (Figure 2-9).

Remote Access VPN	a a x	Configuration > Remote Access VPN > Network (Client) Access > Group Policies				
Introduction Network (Client) Any IPsec Connect Group Policies Dynamic Acces Dynamic Acces AnyConnect Client AnyConnect Client AnyConnect Client AnyConnect Client AnyConnect Client Market AnyConnect Client Market AnyConne	ccess onnection Profiles ion Profiles is Policies ustomization iment	Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally on the device or externally on a RADIUS/LDAP server. The group policy information is referenced by VPN connection profiles and user accounts. To enforce authorization attributes from an LDAP server you must use an LDAP attribute map. Add the Edit policies				
Bevice Setup		Engineering Internal syrc. IPSec. web N/A				
		DfltGrpPolicy (System Default) Internal svc,IPSec,web N/A				
👫 Firewall						
Remote Access V	🗟 Edit Internal Grou	oup Policy: DfltGrpPolicy 🛛 🗙				
	General Servers	After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN portal page. The following settings decides what will happen.				
Device Manageme	Split Tunneling	Post Login Setting				
	IE Browser Prox	XY O Do not prompt user to choose				
	SSL VPN Client					
	Key Regener	eration				
	Dead Peer D	Detectic User has 15 seconds to choose, or Default Post Login Selection below is taken.				
	Customizatio ⊡IPsec Client	Default Post Login Selection				
		O Go to Clientless SSL VPN portal				
	<	Download SSL VPN Client				
	Find:	💿 Next 🛛 🙆 Previous				
		OK Cancel Help				

Figure 2-9 Requiring a Certificate on an Interface

Step 4 (Optional) You can specify which certificates, if any, you want to use for SSL authentication on each interface. If you do not specify a certificate for a particular interface, the fallback certificate will be used.

To do this, go to Configuration > Remote Access VPN > Advanced > SSL Settings. In the Certificates area, select an interface and click **Edit**. the Select SSL Certificate window displays (Figure 2-10). Select a certificate from the drop-list. Click **OK** and apply your changes.

Remote Access VPN ⊡ ₽ × Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles Introduction The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote Network (Client) Access users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect AnyConnect Connection F IPsec Connection Profiles VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options Group Policies client-related parameters, such as client images and client profiles, can be found at Client Settings.) Dynamic Access Policies 📆 AnyConnect Customization Address Assignment Sp Address As Enable Cisco AnyConnect VPN-Cli nt or legacy SSL VPN Client access on the interfaces selected in the table belo Clientless SSL VPN Access AAA/Local Users Interface Allow Access Enable DTLS Require Client 🗯 ificate 🕺 Secure Desktop Manager \checkmark \checkmark 🟹 Certificate Management faildata ✓ 🗑 Language Localization inside Provide Balancing management Advanced Access Port: 443 DTLS Port: 443 Click here to Assign Certificate to Interface

Figure 2-10 Specifying a Certificate for an Interface

To configure in which certificate store the AnyConnect client searches for the authentication certificate, see Configuring a Certificate Store, page 3-27. You will also find information on configuring certificate restrictions for Linux and Mac OS X operating systems.

Γ

Note



Cisco AnyConnect VPN Client Administrator Guide