# SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Cisco AnyConnect



All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010 - 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Number: 007-013967-001, Rev. A Release Date: January 2018

# Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	5
Environment	5
Audience	5
CBA Flow using SafeNet Authentication Client	6
Prerequisites	6
Supported Tokens and Smart Cards in SafeNet Authentication Client	7
Configuring Cisco ASA	8
Prerequisites:	8
Installing Root Certificate to the ASA ASDM	9
Installing an Identity Certificate on the ASA ASDM1	2
ADD / Configure AAA Server Group1	4
Group Policy Configuration1	7
Connection Profile2	24
Any Connect Client Profile4	5
Client Installation5	51
Running the Solution	53
Using the Cisco AnyConnect Secure Mobility Client SSL VPN5	53
Using the Clientless SSL VPN5	6
Using the Cisco AnyConnect Secure Mobility Client - IPsec IKEv2 VPN	58
Start Before Logon (SBL)6	50
Support Contacts	5
Customer Support Portal6	5
Telephone Support6	5

# **Third-Party Software Acknowledgement**

This document is intended to help users of Gemalto products when working with third-party software, such as Cisco AnyConnect.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

# Description

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

PKI is and effective strong authentication solution to the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. Gemalto's certificate-based tokens and smart cards provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

The Cisco ASA 5505 Appliance is a modular platform that provides security and VPN services for small and medium-sized business and enterprise applications.

The following integration guide describes how to authenticate users from workstations to the Cisco ASA, using certificates stored on Tokens/Smart Cards.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Cisco AnyConnect using Gemalto's tokens and smart cards.

It is assumed that the Cisco AnyConnect environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Cisco AnyConnect can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

# Applicability

The information in this document applies to:

• SafeNet Authentication Client (SAC) Typical installation mode— SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.

For more details about different SAC installation modes, please refer to the Customization section in the *SafeNet Authentication Client Administrator Guide*.

# Environment

The integration environment used in this document is based on the following software versions:

- SafeNet Authentication Client (SAC) 10.5
- Cisco AnyConnect 4.5.02033
- Cisco ASA 5505 version 9.2.(4)
- Cisco ASDM 7.6 (1)

# Audience

This document is targeted to system administrators who are familiar with Cisco AnyConnect, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

# **CBA Flow using SafeNet Authentication Client**

The diagram below illustrates the flow of certificate-based authentication:



- A user attempts to connect to the Cisco AnyConnect server using the Cisco AnyConnect client application. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
- 2. After successful authentication, the user is allowed access to internal resources.

# **Prerequisites**

This section describes the prerequisites that must be installed and configured before implementing certificatebased authentication for Cisco AnyConnect using Gemalto tokens and smart cards:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA Connector. For further details, refer to the section "Connector for Microsoft CA" in the *SafeNet Authentication Manager Administrator's Guide*.
- Users must have a Gemalto token or smart card with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (10.5) should be installed on all client machines.

# Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.5) supports the following tokens and smart cards:

#### Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

#### **Smart Cards**

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For a list of all supported devices please refer to SafeNet Authentication Client Customer Release Notes.

# **Configuring Cisco ASA**

This solution demonstrates how to use Token / Smart Card solutions incorporated with Cisco solutions. This is done by authenticating users against Cisco ASA using PKI (Smart Card User certificate) stored on the Token/Smart Card.

# **Prerequisites:**

- IPsec configuration used default options that were enabled after adding a cisco license:
  - Default IKE Parameters Default crypto map
  - NAT (Transparency enabled)
  - Default IPsec Proposals
- IKEv2 Policies IKEv2 policy example configuration:

Home 🍓 Configuration 🔯 Ma	onitoring 🔚 Save 🔇 R	efresh 💽 Back 🕥	Forward ? Help			CISCO
Device List Bookmarks	Configuration > Site-to	Site VPN > Advanced	> IKE Policies			
Device List □ ₽ ×	Configuro specific Interne	t Kow Evchange (TKE) ale	orithms and parameters	within the IDees Inter	not Focurity Association Ko	(Management Dratecal (TCAVMD)
🖶 Add 📋 Delete 🚿 Connect	framework, for the AH ar	d ESP IPsec protocols.	onu inis anu parameters	, wid in the resective	net security Association Re	(ISARIAP)
Find: Go	IKEv 1 Policies					
10.0.135	🖨 Add 📓 Edit	Delete Find:	$\bigcirc$	🔘 🗖 Match Case		
	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime (seconds)
Connection Profiles Group Policies Group Policies Group Certificate Management Groups Group Management Groups Grou	IKEv2 Policies	Delete Find:	0	Match Case		
Certificate to Connection	Priority #	Encryption	Integrity Hash	PRF Hash	D-H Group	Lifetime (seconds)
Crypto Engine		aes-256	sha	sha	5	86400
	10	aes-192	sha	sha	5	86400
	20	des 3dec	sha	stid	5	85400
A Device Setup	40	des	sha	sha	5	86400
Firewall  Remote Access VPN  Site-to-Site VPN						

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- SSL Certificate was configured on ADSM.
- For authentication using digital certificates, there must be at least one identity certificate and its issuing CA certificate on a security appliance.

# Installing Root Certificate to the ASA ASDM

**Prerequisite**: Root CA Certificate is downloaded from the CA authority. Before configuring the ASA for Remote access VPN you must enroll the Cisco ASA for the Root CA certificates and keys.

#### To enroll the ASA for the Root CA certificate:

1. From the Cisco ADSM for ASA screen select Configuration> Certificate Management, then click CA Certificate.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

2. Select CA Certificates, then click Add.

<u>File View Tools Wizards Window H</u> elp	Type topic to search G	° alate
Home 🗞 Configuration 😥 Monitoring 📮 Save 🔇	Refresh 🔇 Back 🔘 Forward 🢡 Help	CISCO
Remote Access VPN 리 무	Configuration > Remote Access VPN > Certificate Management > CA Certificates	
Remote Access VPN       Image Access VPN         Introduction       Introduction         Image Access SSL VPN Access       Image Access SSL VPN Access         Image Access SSL VPN Access       Image Access Access         Image Access SSL VPN Access       Image Access         Image Certificate Management       Image Accesting Access Signer         Image Local Certificate Authority       Image Localization         Image Localization       Image Localization         Image Access       <	Issued To       Issued By       Expiry Date       Associated Trustpoints       Usage       Active         Image: Install Certificate       X	Add Edit Show Details Request CRL Delete
	C Use SCEP: SCEP URL: http:// Retry Period: 1 minutes Retry Count: 0 (Use 0 to indicate unlimited retries) More Options	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. Under Install from a file click Browse, navigate to the path of the Root CA, and then click Install.

<b>1</b>	isco ASDM 7	.6(1) for AS	A - 10.0.0.135									_ 8 ×
File	View Tool	s Wizards	Window Help						Тур	e topic to searc	n Go	ababa
0	Home 0	Configuration	Monitoring	Save	强 Refresh 🔼	Back 🕥 Forw	ard 🦻 Help					cisco
-							0					-
	Remote Act	cess vPN	+ 'ם	To Inst	all Certificate					<		<u> </u>
2	7 Introd	ork (Client) Ac	ress	Case Summer					-	-		
kmai	🗉 📑 Client	less SSL VPN	Access	Trus	tpoint Name: A	SDM_TrustPoint6	6			Usage	Active	Add
Boo	Easy	VPN Remote			Install from a file:			Browse		nature	Yes	Edit
	Host S	.ocal Users Scan Image		C	Paste certificate in PEI	M format:						
	🗉 🦰 Secur	e Desktop Ma	nager									Show Details
	E 🔂 Certif	icate Manage	ment		💽 Install						×	Request CRL
		lentity Certific	cates		Look in:	Certificate	es		-	a 😕 🖽-		Delete
	- <b>A</b>	usted Certific	cate Pool									
		ode Signer Incal Certificati	e Authority		4	sah2.serv	er.pfx					
	- Langu	age Localizati	ion		- 22	Sha2dent	ity.cer					
	DHCP	Server			Recent Items							
	H Advar	nced										
	~											
					Desktop							
				0	L 🕞							
					s 📕							
					R Ny Documents							
					. 🔊							
	0											
	Device	Setup			Computer							
	Firewal				<u> </u>	File name:	Sha2Poot.cer				Tostall	
	O Remote	Access VPN		-	Network	and the first	phozeooteer				anstan	
	Con Meniore	- ACCESS VEIN			- HELMOIK	Hies of type:	All Files			<b>T</b>	Cancel	
	Site-to-	Site VPN			1							1
	Device	Management										
	100							Apply Res	et			
				ç			_	(CO				

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. On the CA Certificate Installed successfully window, click OK.

Trustpoint Name:	ASDM_TrustPoint6	
Install from a file:	C:\Users\Administrator.SER	VER2( Browse
C Paste certificate in	PEM format:	
Te Ce	rtificate Installation	×
	Cartert interes	1
		a successituily.
	ок	
O Use SCEP:		
C Use SCEP: SCEP URL:		
C Use SCEP: SCEP URL: Retry Period:	1	minutes
C Use SCEP: SCEP URL: Retry Period: Retry Count:	, 1 0	minutes Use 0 to indicate unlimited
C Use SCEP: SCEP URL: Retry Period: Retry Count:	<u>1</u> 0	minutes Use 0 to indicate unlimited
C Use SCEP: SCEP URL: Retry Period: Retry Count:	1 0	minutes Use 0 to indicate unlimited More Optio

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

# Installing an Identity Certificate on the ASA ASDM

Before configuring the ASA for Remote access, VPN enrollment of the ASA identity for certificates and keys is needed.

**Prerequisite**: this example demonstrates a pre-created PKCS12 certificate. The Certificate **must** contain the server authentication EKU.

To enroll the ASA for certificate installation:

1. From the Cisco ADSM for ASA screen select Configuration> Certificate Management, then click Identity certificate, and click Add.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

2. Enter a name in the **Trustpoint Name** field, select **Import the identity certificate from a file**, then click **Browse** and navigate to the certificate location.

rustpoint Name:	Identity_Cer		
Import the identity certi-	ficate from a file (PKCS12 forma	at with Certificate(s)	+Private Key):
Decryption Passphrase:			
File to Import From:		Browse	
Add a new identity certi	ficate:		
Key Pair:	<pre><default-rsa-key></default-rsa-key></pre>	Show	New,,
Certificate Subject DN:	CN=ciscoasa1	Select	
🖵 Generate self-signed	l certificate		
🗖 Act as local certi	ficate authority and issue dyna	mic certificates to TLS	S-Proxy
			Advanced

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 3. Enter the passphrase in the **Decryption Passphrase** field.
- 4. Next to the **File to Import From** field, click browse and navigate to the certificate, then click **Add Certificate.**

rustpoint Name:	Identity_Cer		
Import the identity certif	icate from a file (PKCS12 format with	Certificate(s) +	Private Key):
Decryption Passphrase:	****		
File to Import From:	C:\Users\Administrator.SERVER20	Browse	1
Add a new identity certif	icate:		
Key Pair:	<default-rsa-key></default-rsa-key>	Show,	New
Certificate Subject DN:	CN=ciscoasa1	Select,	
Generate self-signed	certificate		
🗖 Act as local certif	icate authority and issue dynamic cer	tificates to TLS	-Ргоху
			Advanced

5. When the Identity certificate imported successfully, click OK.

ustpoint Name: Tmport the identity of	Identity_Cer	(PKCS12 form	nat with Certific	ate(s)+Priva	te Kev):
Decryption Passphras	e: ****	. U NODIE ION			
File	-			1	
Adr Informatio	n				×
Key					
Key Cer	Import PKCS12 op	peration comp	leted successfu	lly.	
Key Cer	Import PKCS12 op	peration comp OK	leted successfu	lly.	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## ADD / Configure AAA Server Group

If you want to use an external AAA server, you must first create at least one AAA server group for each AAA protocol, and add one or more servers to each group. AAA server groups are identified by name. Each server group is associated with only one type of server, such as Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

For this integration, we will use Microsoft Active Directory LDAP as AAA server for authorization.

1. From the **Cisco ADSM for ASA** screen, click the **Configuration** tag, click **Remote Access VPN** and select **AAA Local users > AAA Server Group.** 

C	Home 🗞 Configuration 🔯 Monitoring	Save 🔇 Refresh	Back 🕥 For	ward 🢡 Help				CISCO
ist	Remote Access VPN 🗗 🖓	Configuration > Remo	te Access VPN >	AAA/Local Users	> AAA Server Gro	<u>IDS</u>		
vice L	2 Introduction	AAA Server Groups						
De	E Clientless SSL VPN Access	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add
	Easy VPN Remote	LOCAL	LOCAL		Depletion	10	2	Edit
	AAA/Local Osers	SAC	LUAP		Depledon	10	5	Delata
	- 2 LDAP Attribute Map							Delete
	🗉 🚮 Secure Desktop Manager							
	Certificate Management							
	Identity Certificates	Find:	$\odot$	Match Case				
	Trusted Certificate Pool							
	Code Signer	Servers in the Selected	Group					-
		Server Name or IP Ad	dress Interfa	ce Timeout				Add
	DHCP Server	10.0.0.12	Inside	10				Edit
	E-RAdvanced							Delete
	~							Move Up
								Move Down
								Test
	Device Setup							
2	Firewall							
	Remote Access VPN							
	Site-to-Site VPN	Find:	$\bigcirc$	Match Case				
	Device Management	LDAP Attribute Map						¥
	» •			A	Apply Rese	t		

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

2. In the AAA Server Groups window, click Add.

I	Home Sav	re 🔇 Refresh 🔇 Back 🕥 Forward 🦻 Help	CISCO
	Remote Access VPN 🗗 무 Con	figuration > Remote Access VPN > AAA/Local Users > AAA Server Groups	
e List	2 Introduction	A& Carrier Craves	
vice	Network (Client) Access		
ă	E Clientless SSL VPN Access	ad Time Max Failed Attempts	Add
В	Easy VPN Remote	AAA Server Group:	Edit
	AAA/Local Users S	3	Luit
-	AAA Server Groups	Protocol: RADIUS 💌	Delete
	Local Users	Accounting Mode: C Simultaneous 📀 Single	
	Host Scan Image	Desitivities Mades C. Desition C. Trand	
	🗄 🖓 Secure Desktop Manager	Reactivation Mode: (• Depletion (* Timed	
	Certificate Management	Dead Time: 10 minutes	
	CA Certificates	Mu Salad Manada	
		Max Palled Attempts: 13	
	Trusted Certificate Pool	Enable interim accounting update	
	Code Signer Se		
	Local Certificate Authority	Update Interval: 24 Hours	Add
	DHCP Server	Enable Active Directory Agent mode	
	- DNS		Edit
	H Advanced	ISE Policy Enforcement	Delete
		Enable dynamic authorization	
			Move Up
		Dynamic Authorization Port: 1700	Move Down
		Use authorization only mode (no common password configuration required)	MOVE DOWN
	-		Test
	Device Setup		
		VPN3K Compatibility Option 🛛 🕹	
	Firewall		
	Remote Access VPN	OK Cancel Help	
	CO F	ind: 🗇 🛆 🗖 Match Case	
	Site-to-Site VPN		
	Device Management	DAP Attribute Map	×
	, *	Apply Reset	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. On the Add AAA Server Group window, complete the fields as described in the table below, and then click OK.

Add AAA Server	Group	×
AAA Server Group:	LDAPServer	
Protocol:	LDAP 💌	
Reactivation Mode:	Depletion C Timed	
Dead Time:	10 minutes	
Max Failed Attempts:	: 3	
	and the second s	

Field	Operation
AAA Server Group	Enter a server group name (for example, LDAP server)
Protocol	Select LDAP.

4. Under Servers in the selected Group (highlighted), click Add.

S'	Home Configuration Monitoring	Save 🔇 Refresh	Back 🕜 Forw	ard 🧖 Help					CISCO
	Remote Access VPN 🛛 무	Configuration > Remo	te Access VPN > /	AAA/Local Users	> AAA Server Gro	u <u>ps</u>			
vice Lis	? Introduction	AAA Server Groups							
De	E Clientless SSL VPN Access	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts		Add
	Easy VPN Remote	LOCAL	LOCAL						
	AAA/Local Users	SAC	LDAP		Depletion	10	3		Edit
_	AAA Server Groups	LDAPServer	LDAP		Depletion	10	3		Delete
	DAP Attribute Map								
	Host Scan Image								
	E A Secure Desktop Manager								
	- Certificate Management								
	CA Certificates	Find:		Match Case					
	Identity Certificates								
	Code Signer	Conversion the Colocted	Craup						
	Local Certificate Authority	Servers in the Selected	Group						
	Language Localization	Server Name or IP Ad	dress Interface	e limeout				_	Add
	DHCP Server								Edit
	DNS Advanced							_	
	E Bavanceu							_	Delete
									Move Up
								_	
								_	Move Down
									Test
	Device Setup							_	
	S. Court								
	S riewaii								
	Remote Access VPN								
	Site-to-Site VPN	Find:	$\odot$	Match Case					
	Device Management	LDAP Attribute Map							¥
	» *			, A	Apply Rese	t			

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

5. Complete the fields as described in the table below and click **OK**:

Edit AAA Server	×					
Server Group:	LDAPServer					
Interface Name:	inside					
Server Name or IP Addres	s: 10.0.0.13					
Timeout:	10 seconds					
LDAP Parameters for auth	entication/authorization					
Enable LDAP over S	SL					
Server Port:	389					
Server Type:	Detect Automatically/Use Generic Type 💌					
Base DN:	CN=Users,DC=sha2,DC=com					
Scope:	All levels beneath the Base DN 💌					
Naming Attribute:	userPrincipalname					
Login DN:	CN=Administrator,CN=Users,DC=sha2,DC=com					
Login Password:	*******					
LDAP Attribute Map:	None 💌					
SASL MD5 authentio	cation					
SASL Kerberos auth	entication					
LDAP Parameters for Group Search						
Group Base DN:						
Group Search Timeout: 10						
ОК	Cancel Help					

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

Field:	Operation:
Interface Name	Select an appropriate interface that Cisco ASA uses in order to reach the LDAP server.
IP address	Enter the IP address of the server.
Server Type	Choose Server Type (in this example Detect Automatically was used).
Server Port	In this example the default LDAP port 389 was used.
Base DN	Enter the location in the LDAP hierarchy where the server must begin to search.
Scope	Under the scope option, choose the appropriate answer. In this example, the default "All Levels beneath the Base DN" was used.
Naming Attribute	Enter the Relative Distinguished Name attribute(s) that uniquely identifies an entry on the LDAP server; <b>userPrincipalname</b> attribute in the Microsoft Active Directory.
Login DN	Enter the Distinguished Name with enough privileges in order to be able to search users in the LDAP server.
Login Password	Enter the password for the Distinguished Name account.

## **Group Policy Configuration**

A group policy is a set of user-oriented attribute/value pairs for connections that are stored either internally (locally) on the device or externally. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

## **Group Policy - SSL Protocol**

In this example: Group policy with SSL protocol is demonstrated for both client and clientless users.

#### To add a group policy, do the following:

- 1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
- 2. On the main window, click the **Configuration** tab.

3. In the left pane, click Remote Access VPN, and then select Network (Client) Access > Group Policies.

🧱 Cisco ASDM 7.6(1) for ASA - 10.0.0.135					_ 8 ×
File View Tools Wizards Window Help			Type to	opic to search Go	ababa
Home 🍪 Configuration 📴 Monitoring	Save 🔇 Refresh 🔇 B	ack 🕐 Forward 🧖	Help		cisco
Remote Access VPN 🗗 🕂	Configuration > Remote A	ccess VPN > Network (	Client) Access > Group Policies		
Introduction     Introduction     AnyConnect Connection Profiles     AnyConnect Customization/Locali     Resources     Burry	Manage VPN group policies device or externally on a RA To enforce authorization att Add V I C Edit	A VPN group is a collection IDIUS/LDAP server. The g ributes from an LDAP serv Delete	of user-oriented authorization attribute/val roup policy information is referenced by VPN ver you must use an <u>LDAP attribute map</u> .	ue pairs that may be stored intern connection profiles and user acco	ally on the unts.
GUI Text and Messages	Name	Туре	Tunneling Protocol	Connection Profiles/L Assigned To	lsers
Customized Installer Transforms	GroupPolicy_IPsec1	Internal	ikev1;ikev2	IPsec1;avi	
AnyConnect Client Profile	DfltGrpPolicy (System De	Internal	ikev1;l2tp-ipsec;ssl-dient;ssl-dientless	DefaultRAGroup;DefaultL2LGrou	p;DefaultAD
AnyConnect Client Software	GroupPolicy3	Internal	ssl-client;ssl-clientless	TunnelGroup3	
- Dynamic Access Policies	NewGroupPolicy	Internal	ssl-client		
	GroupPolicyGil	Internal	ssl-client		
IPsec(IKEv1) Connection Profiles	GroupPolicy1	Internal	ssl-clientless	TunnelGroup 1	
- 🐻 Secure Mobility Solution	GroupPolicy2	Internal	ssl-clientless	TunnelGroup2	
🕀 🗞 Address Assignment	token	Internal	ikev1	gilm	
Connection Profiles  Fortal  Out Access  Difference  Difference					
Device Management	Find:	💿 🙆 🗖 Match C	Case		
» *			Apply Reset		

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. In the center pane, click Add.

🧱 Cisco ASDM 7.6(1) for ASA - 10.0.0.135					_ 8 ×
File View Tools Wizards Window Help			Type topic	to search Go	alada
Home 🍪 Configuration 🔯 Monitoring	Save 🔇 Refresh 🔇 Ba	ack 🔘 Forward 🧖 He	lp		CISCO
Remote Access VPN 🗖 🕂	Configuration > Remote Ad	cess VPN > Network (Cli	ent) Access > Group Policies		
Introduction     Metwork (Client) Access     AnyConnect Connection Profiles     AnyConnect Customization/Local:     Resources     Sinary     Sinat	Manage VPN group policies, A device or externally on a RA To enforce authorization attr Add v 2 Edit	A VPN group is a collection of DIUS/LDAP server. The grou ributes from an LDAP server Delete	user-oriented authorization attribute/value p policy information is referenced by VPN co you must use an <u>LDAP attribute map</u> .	pairs that may be stored interna nnection profiles and user accou	ally on the unts.
GUI Text and Messages	Name	Туре	Tunneling Protocol	Connection Profiles/U Assigned To	isers

5. On the **Add Internal Group Policy** window, in the left pane, select **General** and complete the fields described in the table below.

General	Name: GrounPolicySS
Servers	
Advanced	Banner: 🔽 Inherit
	SCEP forwarding URL: 🔽 Inherit
	Address Pools: 🔽 Inherit
	Defidient Date IT Taket
	12 YO AULIESS POOLS: V LITTERIL
	More Options
	Tunneling Protocols:
	Filter: 🔽 Inherit
	Access Hours:
	Simultaneous Logins:
	Restrict arcress to M AN:
	Connection Prome (runner Group) Look: V Innent
	Maximum Connect Time: V Inherit   Unimited   minutes
	Ide Timeout:
	On smart card removal: 🔽 Inherit C Disconnect C Keep the connection
	-

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

Name	Enter a name for the group policy (for example, <b>GroupPolicySSL</b> ).			
More Options Tunneling Protocols	Click <b>More Options</b> to expand the window and then do the following in the <b>Tunneling Protocols</b> field to choose the required VPN protocol :			
	1. Clear Inherit.			
	2. Select Clientless SSL VPN.			
	3. Select SSL VPN Client.			

- 6. In the left pane select Servers.
- 7. Deselect **DNS servers: Inherit**, and enter the IP address.
- 8. Deselect **Default domain: Inherit,** and enter the domain name.

🔄 Edit Internal Group Policy	:SmartCard
General	
Servers	DNS Servers: Inhent 10.0.0.13
-Advanced	WINS Secure II Ishert
Browser Proxy	Ward Selvers. (* Lineau )
-AnyConnect Client	More Options
	DHCP Scope: V Inherit
Key Regeneration	
Dead Peer Detection	Derault Domain: ] innent jsna2.com
Custom Attributes	
IPsec(IKEv1) Client	
	-
Find:	Winext Wirevious
	OK Cancel Help

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

9. Leave all other configuration fields with their default settings, and click OK

#### **Group Policy - IPsec Protocol**

In This example: Group Policy with IPsec Protocol is demonstrated for Client only.

To add a group policy:

- 1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
- 2. On the main window, click the **Configuration** tab.

3. In the left pane, click the **Remote Access VPN** tab, and then select **Network (Client) Access > Group Policies**.

Cisco ASDM 7.6(1) for ASA - 10.0.0.135					<u> </u>
le View Tools Wizards Window Help			Type t	copic to search Go	alah
home 🖓 Configuration 🔯 Monitoring 🔚	Save 🔇 Refresh 🔇 B	ack 🔘 Forward  🢡	Help		cisco
Remote Access VPN 급 무	onfiguration > Remote A	ccess VPN > Network (	Client) Access > Group Policies		
Introduction     I	Manage VPN group policies. device or externally on a RA To enforce authorization at Add      C C Edit	A VPN group is a collection DIUS/LDAP server. The g tributes from an LDAP serv Delete	of user-oriented authorization attribute/v roup policy information is referenced by VP ver you must use an <u>LDAP attribute map</u> .	alue pairs that may be stored intern N connection profiles and user acco	ally on the unts.
GUI Text and Messages	Name	Туре	Tunneling Protocol	Connection Profiles/U Assigned To	lsers
Localized Installer Transforms	GroupPolicy_IPsec1	Internal	ikev1;ikev2	IPsec1;avi	
AnyConnect Client Profile	DfltGrpPolicy (System De	Internal	ikev1;l2tp-ipsec;ssl-dient;ssl-dientless	DefaultRAGroup;DefaultL2LGrou	p;DefaultAD
AnyConnect Client Software	GroupPolicy3	Internal	ssl-client;ssl-clientless	TunnelGroup3	
Dynamic Access Policies	NewGroupPolicy	Internal	ssl-client		
Group Policies	GroupPolicyGil	Internal	ssl-client		
IPsec(IKEv1) Connection Profiles	GroupPolicy1	Internal	ssl-clientless	TunnelGroup1	
- 🔄 Secure Mobility Solution	GroupPolicy2	Internal	ssl-clientless	TunnelGroup2	
🕀 🎭 Address Assignment	token	Internal	ikev1	gilm	
Clienties SSL VPN Access					
Remote Access VPN					
Site-to-Site VPN	Find:	🗇 🙆 🗖 Match C	Case		
Device Management			Apply Reset		

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. In the center pane, click Add.

💽 Cis	co ASDM 7.6(1) for ASA - 10.0.0.135					_ 8 ×
File	View Tools Wizards Window Help			Type top	ic to search Go	ababa
<b>ان ()</b>	ome 🗞 Configuration 🔯 Monitoring	🛛 Save 🔇 Refresh 🔇 Ba	ck 🕐 Forward 🧖 He	elp		cisco
R	emote Access VPN 🗖 🕂	Configuration > Remote Ac	cess VPN > Network (Cli	ent) Access > Group Policies		
Device Lis	Introduction     Network (Client) Access     AnyConnect Connection Profiles     AnyConnect Customization/Locali      Resources     Binary     Government	Manage VPN group policies. A device or externally on a RAI To enforce authorization attr	VPN group is a collection of DIUS/LDAP server. The grou ibutes from an LDAP server Delete	user-oriented authorization attribute/valu p policy information is referenced by VPN or you must use an <u>LDAP attribute map</u> .	e pairs that may be stored interr connection profiles and user acco	ually on the sunts.
	GUI Text and Messages	Name	Туре	Tunneling Protocol	Connection Profiles/	Jsers

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

5. On the Add Internal Group Policy window, select General and complete the fields as described in the table below.

ers	INAME: JGroupPolicyIPsec	
anced	Banner: 🔽 Inherit	
	SCEP forwarding URL: 🔽 Inherit	
	Address Pools: V Inherit	
	IPV6 Address Pools: IV Inhent	
	More Options	
	Tunneling Protocols:	☐ Inherit ☐ Clientless SSL VPN ☐ SSL VPN Client ☐ IPsec IKEv1 🔽 IPsec IKEv2 ☐ L2TP/IPsec
	Filter:	🔽 Inherit
	Access Hours:	🔽 Inherit
	Simultaneous Logins:	Iv Inherit
	Restrict access to VLAN:	Inherit
	Connection Profile (Tunnel Group) Lock:	Inherit
	Maximum Connect Time:	✓ Inherit Unlimited minutes
	Idle Timeout:	Vinherit Vinne minutes
	On smart card removal:	✓ Inherit C Disconnect C Keep the connection

Name Enter a name for the group policy (for example **GroupPolicyIPsec**)

Name	Enter a name for the group policy (for example, <b>Group: Oregin Sec</b> ).
More Options Tunneling Protocols	Click <b>More Options</b> to expand the window and then do the following in the <b>Tunneling Protocols</b> field choose the required VPN protocol :
	<ol> <li>Clear Inherit.</li> <li>Select IPsec IKEv2.</li> </ol>

- 6. In the left pane select Servers.
- 7. Deselect **DNS servers: Inherit**, and enter the IP address.
- 8. Deselect **Default domain: Inherit,** and enter the domain name.

🧧 Edit Internal Group Policy	: SmartCard	x
General		-
	DNS Servers:  Inherit 10.0.0.13	
Split Tunneling	WINS Servers: 🔽 Inherit	
- AnyConnect Client	More Ontions	
Login Setting Client Firewall	DHCP Scope: V Inherit	-
Key Regeneration	Default Domain: Tinherit Sha2.com	-
Customization		
- 75 - 28 - 28		
		-
	<u> ۱</u>	•
Find:	Next O Previous	
	OK Cancel Help	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

9. Leave all other configuration tabs with their default settings, and click OK.

#### Group Policy - Enable Start before Logon (SBL)

Start Before Logon (SBL) enables the user to see the AnyConnect GUI logon window before the Windows logon window appears. SBL establishes the VPN connection first.

- 1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
- 2. In the left pane, click the **Remote Access VPN** tab, and then select **Network (Client) Access > Group Policies**.
- 3. In Group Policy Expand Advanced, deselect Inherit for Optional Client Module to Download, and choose AnyConnect SBL from the drop-down list.
- 4. Click **OK**, click **Apply**, and click **Save**.

Edit Internal Group Policy	: GroupPolicySSL					
General	Keep Installer on Client System:	✓ Inherit	C Yes	C No		<u>^</u>
<ul> <li>Advanced</li> </ul>	Datagram Transport Layer Security (DTLS):	🔽 Inherit	$\mathbf{C}$ Enable	C Disable		
Split Tunneling Browser Proxy	DTLS Compression:	🔽 Inherit	C Enable	C Disable		
AnyConnect Client	SSL Compression:	🔽 Inherit	C Deflate	C LZS	C Disable	
E a sectador y cache	Ignore Don't Fragment(DF) Bit:	🔽 Inherit	C Enable	C Disable		
	Client Bypass Protocol:	Inherit	C Enable	C Disable		
	FQDN of This Device:	FQDN				
	MTU:	🔽 Inherit				
	Keepalive Messages:	🔽 Inherit	Disable	Interval:	seconds	
	Optional Client Modules to Download:	🔲 Inherit	vpngina			
	Always-On VP AnyConnect DART AnyConnect AMP Enabler AnyConnect Network Visib Client Profiles V AnyConnect Network Visib AnyConnect SBI AnyConnect SBI	ility ming Securit	y			
	AnyConnect Web Security	ess Manager				
						OK Cancel

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## **Connection Profile**

A connection profile consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. Connection profiles include a small number of attributes that pertain to creating the tunnel itself.

## Configuring a Connection Profile for Network (Client) Access SSL VPN Access

A connection profile consists of a set of records that determines tunnel connection policies.

#### To configure a connection profile:

- 1. Open Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
- 2. On the main window, click the **Configuration** tab.
- 3. In the left pane, click **Remote Access VPN**, and then select **Network (Client) Access > AnyConnect Connection Profiles.**



- 4. In the right pane, under Access Interfaces, perform the following steps:
  - a. Select Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below.
  - b. In the Access Interface table, for outside or inside interfaces, under the SSL Access column, select Allow Access and Enable DTLS.
  - c. Select Bypass interface access lists for inbound VPN sessions.
  - d. Under Login Page Setting, select Allow user to select connection profile on the login page.

Home 🦓 Configuration 🔯 Monitoring	Save 🔇 Refresh	Back 🕥 Forward	💡 Help			CISCO
Remote Access VPI	Confidurations Ref me secondy oppion end-user administra Security (DTLS) turn Access Interfaces — I ⊂ Enable Cisco An SSL access must be	The Access of the fit of aromatically acpuyed tive rights. The Cisco An heling options. yConnect VPN Client acc enabled if you allow Any	etwork (Milent) Accession of Cases Any Connect VPN Client sup ess on the interfaces self	S > Any connect ports IPsec (IKEv2) ected in the table be iched from a browse	connection profiles, oscia oporteoreceber, rice was tunnel as well as SSL tunnel with D slow r (Web Launch) ,	Cicrit ocparyment re Datagram Transport L
IPsec(IKEv1) Connection Profiles	Interface	SSL A	ccess	IPs	ec (IKEv2) Access	
Secure Mobility Solution		Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certifi
Address Assignment	outside					Dank Calling
Clenties SS. VPN Access Connection Profiles Connection Profiles Convection Profiles Convection Profiles Convection Vol Access Convection Vol Access Convec	Bypass interface     Access lists from gro     Login Page Setting     ✓ Allow user to sel     ✓ Allow user to sel     ✓ Shutdown porta     Connection profile 5     Connection profile 6     ▲ Add	e access lists for inbound sup policy and user policy lect connection profile or l login page. (tunnel group) specifies t ierce. t Delete Find: J	VPN sessions v always apply to the train the login page. (*) now user is authenticated (*)	ffic.	ers. You can configure the mappin	ng from certificate to
Remote Access VPN	Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Polic
	DefaultRAGroup				AAA(RADIUS)	DfltGrpPolicy
Site-to-Site VPN	DefaultWEBVP	V			Certificate	GroupPolicy3 👻
Device Management	•		Apply	Reset		

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

#### 5. Under Connection Profiles, click Add.

Connection Profiles Connection profile (tunnel group) specifies how user is authenticated a certificate to connection profile <u>here</u> .	and other parameters. You can configure the mapping from
Add C Edit Delete Find:	) 🔘 🗖 Match Case

6. In the Add AnyConnect Connection Profile window, in the left pane, click Basic. In the right pane, complete the fields as described in the table below.

	Name:	AnyConnect	
ed.	Aliases:	AnyConnect	
	Authentication		
	Method:	C AAA <ul> <li>C certificate</li> <li>C Both</li> </ul>	
	AAA Server Group:	LOCAL	✓ Manar
		Use LOCAL if Server Group fails	
	Client Address Assignment –		
	DHCP Servers:		
		None     O     DHCP Link     O     DHCP Subnet	
	Client Address Pools:	DomainPool	Selec
	Client IPv6 Address Pools:	. [	Selec
			JUNC
		• ]	
	Default Group Policy		
	Default Group Policy	GroupPolicyIPsec	▼ Manag
	Default Group Policy Group Policy: (Following fields are linked	GroupPolicyIPsec	▼ Manag
	Default Group Policy Group Policy: (Following fields are linked	GroupPolicyIPsec	▼ Manag
	Default Group Policy Group Policy: (Following fields are linked I Enable SSL VPN clier Enable IPsec(IKEv2)	GroupPolicyIPsec	▼ Manag
	Default Group Policy Group Policy: (Following fields are linked I Enable SSL VPN clier Enable IPsec(IKEv2) DNS Servers: 10.0.0	GroupPolicyIPsec  I to attribute of the group policy selected above.)  nt protocol  O cliant protocol	▼ Manac
	Default Group Policy Group Policy: (Following fields are linked © Enable SSL VPN clier © Enable IPsec(IKEv2) DNS Servers: 10.0.0 WINS Servers: 172.1	GroupPolicyIPsec d to attribute of the group policy selected above.) nt protocol 0.13 (9.19.100	Manac

Field Name:	Enter the name for the connection profile (for example, <b>AnyConnect</b> ).
Aliases	Enter the <b>Aliases</b> for the connection profile (for example, <b>AnyConnect</b> ). The alias will be displayed to the user.
Authentication	Select the certification authentication method associated with the connection profile.
Client Address Pools	Click Select and then assign an address pool (for example, DomainPool)
Group Policy	Select an appropriate group policy (for example, GroupPolicySSL)
Enable SSL VPN client protocol	Check and enable this option.
DNS Servers	Enter the DNS server details.
Domain Name	Enter the Domain name.

7. In the left pane select Advanced > Authentication, and in the right pane click Add.

🚰 Add AnyConnect Connectio	n Profile		×
Basic I H-Advanced General	nterface-Specific Authentication Ser	ver Groups	<u> </u>
Client Addressing <mark>Authentication</mark> Secondary Authenticat Authorization Accounting Group Alias/Group URL	Interface	Server Group	Fallback to LOCAL

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 8. In the Assign Authentication Server Group to Interface window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses to reach the AAA server.
  - b. From the Server Group drop down list, choose the previously created AAA server group and click OK.

Interface:	inside		+	
Server Group:	LDAPServ	er	Mana	ge
Fallback:	Use LO	CAL if Server Grou	up fails	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

9. In Authentication, a server is added to the Interface list.

Basic	Interface-Specific Authentication	Server Groups	
Advanced General	🗣 Add 📝 Edit 📋 Dele	ete	
Client Addressing	Interface	Server Group	Fallback to LOCAL
Secondary Authenticat	inside	LOCAL	
Accounting Group Alias/Group URL			

- 10. In the left pane, select **Advanced > Authorization** and perform the following:
  - a. In **Server Group**, select the previously created AAA server group.
  - b. Select Users must exist in authorization database to connect.

Basic	Authorization Server Group	
Advanced General Client Addressing Authentication	Server Group: LDAPServer	Manage
Secondary Authenticat <mark>Authorization</mark> Accounting	Interface-specific Authorization Server Groups	
Single of the Allas of the OKE	Interface	Server Group

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

11. Under Authorization Server Group in the right pane, under Interface-specific Authorization Server Groups, click Add.

Add AnyConnect Connec	tion Profile	
Basic	Authorization Server Group	<u>.</u>
⊡…Advanced General	Server Group: LDAPServer	Manage
Client Addressing Authentication	Users must exist in the authorization	database to connect
Secondary Authentica	Interface-specific Authorization Server Groups	
Authorization Accounting Group Alias/Group LIPL	🖶 Add 🗹 Edit 📋 Delete	
Allas/Group Allas/Group OKL	Interface	Server Group

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 12. In the Assign Authorization Server Group to Interface window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server.
  - b. From the **Server Group** drop-down window, select the previously created AAA server group and click **OK.**

and an and a second	Inside	
Server Group:	LDAPServer	Manage

- 13. Under Authorization Server Group in the center pane, under User Mapping from Certificate, select Specify the certificate fields to be used as the username, and perform the following:
  - a. From the Primary field drop down-list, select UPN (User's principal Name).
  - b. From the Secondary field drop-down list, select None and click OK.

add AnyConnect Connect	tion Profile	×
Basic General Client Addressing Authentication Secondary Authenticat Authorization	Authorization Server Group Server Group: LDAPServer Users must exist in the authorization database to connect Interface-specific Authorization Server Groups	<u> </u>
Group Alias/Group URL	Interface Server Group inside IDAPServer	
Find:	Username Mapping from Certificate © Specify the certificate fields to be used as the username Primary Field: UPN (User's Principal Name) Secondary Field: None © Use the entire DN as the username Secondary Field: None © Use the entire DN as the username Primary Berline Previous	

14. If the Connection Profile was added successfully, click **Apply**, then click **Save**.

	Home 🗞 Configuration 🔯 Monitoring	Save 🔇 Refresh	G Back 🕜 Forward	🥐 Help			CISCO
	Remote Access VPN 🛛 🖓	Configuration > Re	emote Access VPN > N	etwork (Client) Acce	ss > AnyConnect	Connection Profiles	C.
Device Li	Introduction     Network (Client) Access	Security (DTLS) tur	nneling options.				
	AnyConnect Customization/Localize     AnyConnect Client Profile     AnyConnect Client Software	SSL access must be	nyConnect VPN Client acc	ess on the interfaces se Connect client to be lau	elected in the table b Inched from a brows	elow er (Web Launch) .	
	Dynamic Access Policies		SSL #	ccess	IF	sec (IKEv2) Access	7
	TPsec(IKEv1) Connection Profiles	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	- Douico Cortifi
	Secure Mobility Solution	outside	<u> </u>	2	<b>v</b>		
	🗄 🎭 Address Assignment	inside	<b>v</b>	•	<b>V</b>	<b>v</b>	Port Setting
	Croup Policies  Croup Policies  Dynamic Access Policies  AAA,Local Users  AAA,Local Users  Hots Scaure Desktop Manager  Scaure Desktop Manager  Croup Policies  Device Setup  Firewal	Login Page Setting – Allow user to si Shutdown port Connection Profiles – Connection profile Connection profile Add Z E	elect connection profile or al login page. (tunnel group) specifies l here. dit 1 Delete Find:	n the login page. ()	ed and other parame	eters. You can configure the mapping	ng from certificate to
	Contraction (Contraction)	Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Polic
	Remote Access VPN	DefaultRAGroup				AAA(RADIUS)	DfltGrpPolicy
	29	DefaultWEBVP				Certificate	GroupPolicy3
	Site-to-Site VPN	AnyConnect	<u> </u>		AnyConnect	Certificate	GroupPolicySSL
	Device Management						
-	»			Apply	Reset	]	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

### **Configuring a Connection Profile for Clientless SSL VPN Access**

- 1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
- 2. On the main window, click the **Configuration** tab.
- 3. In the left pane, click **Remote Access VPN**, and then select **Clientless SSL VPN Access > Connection Profile**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 4. In the right pane, under Access Interfaces, perform the following steps:
  - a. In the **Enable interfaces for clientless SSL VPN access** table, in the **outside** and **inside** interface rows, select **Allow Access**.
  - b. Select Bypass interface access lists for inbound VPN session.
  - c. Under Login Page Setting, select Allow user to select connection profile on the login page.

Remote Access VPN 🗗 🖓	Configuration > Rem	ote Access VPN > C	lientless SSL VPN A	ccess > Connection Profiles	
Introduction     Network (Client) Access     Gientless SSL VPN Access	Access Interfaces Enable interfaces for o	lientless SSL VPN acce	ss.		<u> </u>
Connection Profiles  Connection Profiles  Connection Profiles  Contained Connection Profiles  Contained Co	Interfa joutside inside		Allow Acce	Device Certificat	e
Easy VPN Remote     AAA/Local Users     AAA/Local Users     Secure Desktop Manager     Certificate Management     Language Localization     DHCP Server     DNS     Advanced	Bypass interface a Access lists from group Login Page Setting — Allow user to select Allow user to enter Shutdown portal lo Connection Profiles — Connection profile (tu certificate to connect	access lists for inbound o policy and user policy at connection profile or r internal password on ogin page.	VPN sessions v always apply to the n the login page. (1) the login page.	traffic.	nfgure the mapping from
	Add 🖉 Edit	Delete Find:		🛇 🗿 🗖 Match Case	
Firewall	Name	Enabled	Aliases	Authentication Method	Group Policy
	DefaultWEBVPNGr			Certificate	GroupPolicy3
Remote Access VPN	TunnelGroup3	<b>V</b>	SAC	Certificate	GroupPolicy3
<u></u>	IPsec1		IPsec1	Certificate	GroupPolicy_IPsec1
Site-to-Site VPN	SmartCards		Gemalto	Certificate	DfltGrpPolicy
Device Management		if	IDI		Od€I- ▼
2	•		Apply	/ Reset	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

5. Under **Connection Profiles** in the right pane, click **Add**.

Connection Profiles Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configur certificate to connection profile <u>here</u> .	e the mapping from
Add Z Edit Delete Find: O O Match Case	

- 6. On the Add Clientless SSL VPN Connection Profile window, in the left pane, click Basic.
- 7. In the right pane, enter the fields as described in the table below.

Name:	AnyConnect	
Aliases:	AnyConnect	
Authentication		
Method:	C AAA C Certificate C Both	
AAA Server Group:	LOCAL	Manage,
	Use LOCAL if Server Group fails	
DNS		
Server Group:	DefaultDNS	Manage.
	(Following fields are attributes of the DNS server group selected above.)	
	Servers: 10.0.0.13	
	Domain Name: sha2.com	
Default Group Policy		
Crew Delieur	GroupPolicySSL	Manage.
Group Policy:		
Group Policy:	(Following field is an attribute of the group policy selected above.)	
	Aliases: Authentication Method: AAA Server Group: DNS Server Group: Default Group Policy	Name: AnyConnect   Aliases: AnyConnect   Authentication Method:   Method: C AAA C Certificate Both   AAA Server Group: LOCAL   I Use LOCAL if Server Group fails   DNS Server Group:   Server Group: DefaultDNS   (Following fields are attributes of the DNS server group selected above.)   Servers: 10.0.0.13   Domain Name: sha2.com

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

Field Name:	Enter the name for the connection profile (for example, <b>AnyConnect</b> ).
Aliases	Enter the <b>Aliases</b> for the connection profile (for example, <b>AnyConnect</b> ). The alias will be displayed to the user.
Authentication	Select <b>Certificate</b> authentication method associated with the connection profile.
Under DNS	
Server Group	Select the DNS server group needed (DNS server group needed to be added).
Servers	Enter the DNS server detail.
Domain Name	Enter the Domain name.
Under Default Group Policy	
Group Policy	Select an appropriate group policy (for example, GroupPolicySSL).
Enable clientless SSL VPN protocol	Check this option.

8. In the right pane select Advanced > Authentication, and in the center pane click Add.

Basic	Interface-Specific Authentication Ser	ver Groups	
⊡Advanced General	Add 🗹 Edit 📋 Delete		
	Interface	Server Group	Fallback to LOCAL

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 9. In the Assign Authentication Server Group to Interface window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server.
  - b. From the Server Group drop-down list, select the previously created AAA server group and click OK.

Interface:	inside		Ŧ	
Server Group:	LDAPServe	er	Manag	e
Fallback:	Use LO	CAL if Server Gro	up fails	
T allback.	j_ ose co	CALIT SERVER GIO		
	ОК	Cancel	Help	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

Under Authentication, Interface-Specific Server Groups, a server was added in the Interface column.

Basic	Interface-Specific Authentication	Server Groups	
Advanced General	🛧 Add 🗹 Edit 📋 Dele	ete	
Authentication	Interface	Server Group	Fallback to LOCAL
Secondary Authenticat	inside	LOCAL	
Accounting			
-NetBIOS Servers			
Clientless SSL VPN			

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

10. In the right pane expand Advanced, click on Authorization and perform the following:

- a. From the Server Group drop-down list, select the previously created AAA server group.
- b. Select Users must exist in authorization database to connect.

Basic	Authorization Server Group	
Advanced General Authentication	Server Group: LDAPServer  Manage  Manage  Server Group: LDAPServer  Manage	
Authorization 	Interface-specific Authorization Server Groups	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

#### 11. Under Interface-specific Authorization Server Groups click Add.

Basic	Authorization Server Group	
Advanced General Authentication Secondary Authenticat	Server Group: LDAPServer Manage	
Authorization Accounting	Interface-specific Authorization Server Groups	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 12. In the Assign Authorization Server Group window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server
  - b. From the Server Group drop-down list, choose the previously created AAA server group and click OK

nterface:	inside	<b>_</b>
Server Group:	LDAPServer	▼ Manage

#### 13. Under User Mapping from Certificate perform the following:

- a. Select Specify the certificate fields to be used as the username.
- b. From the Primary Field drop-down list, select UPN (User's principal Name).
- c. From the Secondary Field drop-down list, select None and click OK.

Add Clientless SSL VPN Co	onnection Profile
Basic	Authorization Server Group
Advanced	Server Group: IDAPServer
General	
Authentication	Users must exist in the authorization database to connect
Accounting	Interface-specific Authorization Server Groups
NetBIOS Servers	💠 Add 📝 Edit 📋 Delete
Clientless SSL VPN	
	Interface Server Group
	IDAPServer
	Username Mapping from Certificate
	Primary Field: UPN (User's Principal Name)
	Secondary Field: None
	C Use the entire DN as the username
Find:	Next O Previous

14. If the Connection Profile was added successfully, click **Apply** and then click **Save**.

Home 🚳 Configuration 🔯 Monitoring	Save 🔇 Refresh	Back O Forward	💡 Help		CISCO
Home V Consultation in Monitoring	Access Interfaces Enable Interfaces Interfac	Back Porward	Allow Access	s Device Certificat Port Setting	e
Pop Address Assignment     Pop Address Assignment     Connection Profiles     Connection Profiles     Portal     Out Access     Connection Profiles     Out Access     Connection Profiles     Portal     Out Access     Connection Profiles     Out Access     Connection Profiles     Out Access     Connection Profiles     Out Access     Connection Profiles     Out Access     Out	Access lists from group Login Page Setting Allow user to select Allow user to enter Shutdown portal log	cess lists for indound a policy and user policy connection profile on internal password on 1 jin page.	always apply to the tr the login page.	affic.	
Host Scan Image Host Scan Image Control And Scare Control And Sca	Connection Profiles	nel group) specifies ho n profile <u>here</u> . <u> </u> Delete <u>Find:</u>	ow user is authenticate	ed and other parameters. You can cor	nfigure the mapping from
Sirous I	Name	Enabled	Aliases	Authentication Method	Group Policy
S - i ewaii	DefaultWEBVPNGr	V		Certificate	GroupPolicy3
Remote Access VPN	AnyConnect		AnyConnect	Certificate	GroupPolicySSL
<u> </u>	TunnelGroup3	V	SAC	Certificate	GroupPolicy3
Site-to-Site VPN	IPsec1		IPsec1	Certificate	GroupPolicy_IPsec1
Device Management	Lakarana 1001 kalia	if i	Apply	Reset	où

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## Configuring a Connection Profile for AnyConnect Client IPSEC Remote Access VPN

A connection profile consists of a set of records that determines tunnel connection policies.

#### To configure a connection profile:

- 1. Open Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
- 2. On the main window, click the **Configuration** tab.
- 3. In the left pane, click **Remote Access VPN**, and then select **Network (Client) Access > AnyConnect Connection Profiles.**



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 4. In the middle pane, under Access Interfaces, perform the following steps:
  - a. Select Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below.
  - b. In the table, for outside or inside interfaces in the IPsec (IKEv2) Access column, select Allow Access and Enable Client Services.
  - c. Select Bypass interface access lists for inbound VPN sessions.
  - d. Under Login Page Setting, select Allow user to select connection profile on the login page.

🔥 Home 🗞 Configuration 🔯 Monitoring 🗐	Save 🔇 Refresh	Back 🕥 Forward				CISCO
Remote Access VPN 🗗 무	Configuration > Ren	note Access VPN > N	etwork (Client) Acce	ss > AnyConnect C	onnection Profiles	
Introduction     I	The security appliance end-user administrat Security (DTLS) tunn Access Interfaces C Enable Cisco Any SSL access must be e	ce automatically deploys tive rights. The Cisco An leling options. /Connect VPN Client acc enabled if you allow Any	the Cisco AnyConnect N yConnect VPN Client sup ess on the interfaces sel Connect client to be law	PN Client to remote u ports IPsec (IKEv2) to ected in the table bela inched from a browser	sers upon connection. The initial unnel as well as SSL tunnel with I ow (Web Launch) .	client deployment re 🔺
IPsec(IKEv1) Connection Profiles	Interface	SSL A	ccess	IPse	c (IKEv2) Access	
H Address Assignment	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Device Certifi
THE Reduced	outside			-	V	
E	inside					Port Setting
Certificate Management	Bypass interface     Access lists from gro     Login Page Setting     Shutdown portal     Shutdown portal     Connection profile     Connection profile     Add	access lists for inbound up policy and user policy ect connection profile or login page. tunnel group) specifies f erc. t Delete Find: SSL Enabled	VPN sessions v always apply to the tra n the login page.	ffic. d and other paramete C C Match Aliases	rs. You can configure the mappin Case Authentication Method Room(Color) Certificate	ng from certificate to Group Polic Dimorpromy GroupPolicy
»			Apply	Reset		

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

5. Under Connection Profiles, in the middle pane, click Add.

Connection Profiles	
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile <u>here</u> .	
💠 Add 📝 Edit 📋 Delete Find: 💿 💿 🔽 Match Case	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

6. On the Add AnyConnect Connection Profile window, in the left pane, select **Basic**, and in the right pane, complete the fields as described in the table below.

Add AnyConnect Connecti	on Profile		×
Basic	Name:	AnyConnectIPsec	<u> </u>
-Advanced	Aliases:	IPsec_Connection	
Client Addressing	Authentication		
Secondary Authenticat	Method:	C AAA 💿 Certificate C Both	
Authorization	AAA Server Group;	LOCAL	Manage
Group Alias/Group URL		Use LOCAL if Server Group fails	
	Client Address Assignment –		
	DHCP Servers:		
		None C DHCP Link C DHCP Subnet	
	Client Address Pools:	DomainPool	Select
	Client IPv6 Address Pools:		Select
	Default Group Policy		
	Group Policy:	GroupPolicyIPsec	Manage
	(Following fields are linked	to attribute of the group policy selected above.)	
	Enable SSL VPN clien	it protocol	
	Enable IPsec(IKEv2)	client protocol	
	DNS Servers: 10.0.0	0.13	
	WINS Servers: 172.19	9.19.100	
	Domain Name: sha2.c		
	4		▼ ▲
Find:	Ne	xt 🔘 Previous	
	OK	Cancel Help	

Field Name:	Enter the name for the connection profile (for example, <b>AnyConnectIPsec</b> ).
Aliases	Enter the <b>Aliases</b> for the connection profile (for example, <b>IPsec_Connection</b> ). The alias will be displayed to the user.
Authentication	Select <b>Certificate</b> authentication method associated with the connection profile.
Client Address Pools	Click <b>Select</b> and then assign an address pool (for example, <b>DomainPool</b> ).
Group Policy	Select an appropriate group policy (for example, <b>GroupPolicyIPsec</b> ).
Enable IPsec (IKEv2) client protocol	Check this option.
DNS Servers	Enter the DNS server detail.
Domain Name	Enter the Domain name.

7. In the left pane, select Advanced > Authentication and in the right pane click Add.

🚰 Add AnyConnect Conne	ection Profile			×
Basic ⊡Advanced General	Interface-Specific Authentication Ser	ver Groups	<u>.</u>	
Client Addressing <mark>Authentication</mark> Secondary Authentic Authorization Accounting Group Alias/Group UI	Cat Interface	Server Group	Fallback to LOCAL	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 8. In the Assign Authorization Server Group window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server.
  - b. From the Server Group drop-down list, choose the previously created AAA server group and click OK.

nterface:	inside 🔰	-
erver Group:	LDAPServer	Manage

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

In Authentication > Interface-Specific Authentication Server Groups, a Server was added to the list.

Advanced			
General	Add A Edit Delete		
Authoritication	Interface	Server Group	Fallback to LOCAL
Secondary Authenticat	inside L	OCAL	
Authorization Accounting Group Alias/Group URL			

- 9. In the left pane, select Advanced > Authorization and perform the following:
  - a. In the **Server Group** field, select previously created AAA server group.
  - b. Select Users must exist in authorization database to connect.

Basic	Authorization Server Group
Advanced	Server Group: LDAPServer Manage
Client Addressing Authentication	Users must exist in the authorization database to connect
Secondary Authentical	nterface-specific Authorization Server Groups
Authorization Accounting	🖶 Add 📝 Edit 📋 Delete
Group Alias/Group URL	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

10. Under Authorization Server Group, in the center pane, under Interface-specific Authorization Server Group, click Add.

Basic	Authorization Server Group	
Advanced	Server Group: LDAPServer	Manage
Client Addressing Authentication	Users must exist in the authorization	database to connect
Secondary Authenticat	Interface-specific Authorization Server Groups	
Authorization Accounting	🔂 Add 🗹 Edit 📋 Delete	
Group Alias/Group URL	Interface	Server Group

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 11. In the Assign Authorization Server Group window, perform the following:
  - a. From the **Interface** drop-down list, select an appropriate interface that Cisco ASA uses in order to reach the AAA server.
  - b. From the Server Group drop-down list, choose the previously created AAA server group and click OK.

nterface:	inside	<u> </u>
erver Group:	LDAPServer	▼ Manage

#### 12. In Authorization Server Group, under User Mapping from Certificate perform the following:

- a. Select Specify the certificate fields to be used as the username.
- b. From the Primary Field drop-down list, select UPN (User's principal Name).
- c. Form the Secondary Field drop-down list, select None and click OK.

Basic General Client Addressing Authentication Secondary Authenticat <mark>Authorization</mark> Accounting Group Alias/Group URL	Authorization Server Group Server Group: LDAPServer Users must exist in the authorization data Interface-specific Authorization Server Groups Add C Edit Delete	Manage
	Interface LDAF	Server Group PServer
	Username Mapping from Certificate	
	Username Mapping from Certificate	• •_

13. If the Connection Profile was added successfully, click Apply and then click Save.

Home 🗞 Configuration 🔯 Monitoring	Save 🔇 Refresh	Back 🕥 Forward	Help			cisco
ि Remote Access VPN न म	Configuration > Remo	te Access VPN > Netwo	rk (Client) Access	> AnyConnect Co	onnection Profiles	
2 Introduction	SSL access must be en	abled if you allow AnyConn	ect client to be launche	ed from a browser	(Web Launch) .	
AnyConnect Connection Profiles		SSL Access		IPsec	(IKEv2) Access	Т
AnyConnect Customization/Localiza	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Davies Cartif
Binary	outside	<b>V</b>	<b>V</b>	2	<b>v</b>	
Script	inside	V	v	2		Port Settin
Customized Installer Transform	Bypass interface a Access lists from group Login Page Setting     Alow user to select     Shutdown portal lo Connection Profiles     Connection profile (tur connection profile (tur connection profile )     Ext     Add     C Edit	ccess lists for inbound VPN i policy and user policy alwa t connection profile on the l gin page. mel group) specifies how u e. Delete Find: CES Enabled	sessions ys apply to the traffic ogin page. () ser is authenticated ar () () () () () () () () () ()	Ind other parameter	s. You can configure the mappin Case	g from certificate to
	Name	SSL Enabled	IPsec Enabled	Aliases	Authentication Method	Group Policy
S. Device Setup	TunnelGroup3			SAC	Certificate	GroupPolicy35L
	TPsec1			IPsec 1	Certificate	GroupPolicy TPse
Firewall	TunnelGroup 1				AAA(I OCAL)	GroupPolicy5
Remote Access VPN	AnyConnectIPsec	precedence if group URL a	nd certificate map mai	IPsec_Connect	Certificate	GroupPolicyIPsec
	the second	will be used	and a second point of the		, she co	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

# **Any Connect Client Profile**

This Option is used to manage AnyConnect Client Profile. In this example the option is demonstrated with IPsec Connection.

#### To configure an AnyConnect Client profile:

- 1. Open Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
- 2. On the main window, click the **Configuration** tab.

3. In the left pane, click the **Remote Access VPN** tab, and then select **Network (Client) Access > Any Connect Client Profile** 

home 🍇 Configuration 🔯 Monitoring 🔚 Sa	ave 💽 Refresh 🚺 Back 🚺	Forward 💡 Help		CISCO
Remote Access VPN 🗇 🕂 🖉	Configuration > Remote Acces	s VPN > Network (Client) Access	s > AnyConnect Client Profile	
Introduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localizz Binary Binary Customized Installer Transform Customized Installer Transforms	This panel is used to manage Anyi profile to edit, change group or to upload and download of clent pro The profile Usage field is introduce later.	Connect Client Profiles and perform g delete. You can select the 'Add' but files between local machine and devis d with the Secure Mobility Solution. T e Group Policy	roup assignment for AnyConnect to ton to add a new profile. Pressing to This field contains different profile wort B C Apport A Validate	version 2.5 or later. You can select a he Import or Export button is for usage in AnyConnect version 3.0 and
AnyConnect Client Profile	Profile Name	Profile Lisage	Group Policy	Profile Location
- In AnyConnect Client Software	useroro b	ApyConnect VPN Profile	GroupPolicy3	disk0:/usergrp_b_vml
Dynamic Access Policies	IPsec1 client profile	AnyConnect VPN Profile	GroupPolicy IPsec1	disk0://usergip_ot.thi
Group Policies	AnyConnectIPsecClient	AnyConnect VPN Profile	GroupPolicyIPsec	disk0:/anyconnectiosecclient.xml
Group Policies Secure Mobility Solution Centers Sasignment Contest SSL VPN Access Contection Profiles VDI Access VDI Access Group Policies Concerce Deliciee VDI Access Group Policies Concerce Deliciee VDI Access Concerce Deliciee VDI Access Concerce Deliciee Concerce Deliciee Concerce Deliciee Concerce Deliciee Concerce Deliciee Concerce Deliciee Concerce Deliciee				
Site-to-Site VPN		Apply	Reset	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. Under Connection Profiles, in the right pane, click Add and complete the fields in the AnyConnect Client Profile window, as described in the table below, and then click OK.

C	Home 🗞 Configuration 🔯 Monitoring	Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help	CISCO
Device List	Remote Access VPN     P       Introduction     Introduction       AnyConnect Connection Profiles       AnyConnect Customization/Localion/L	Continuentions Remote Access Vol 5: Network (Oren 1 Access ) Any Connect Client Profile This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or profile to edit, change group or to delete. You can select the 'Add button to add a new profile. Pressing the Import or upload and download of client profiles between local machine and device. The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyClaeter.  For Add AnyConnect Client Profile Profile Name AnyConnectIPsecClient	Later. You can select a Export button is for Connect version 3.0 and
	AnyConnect Clent Profile     AnyConnect Clent Software     Dynamic Access Policies     Group Policies     Group Policies     Secure Mobility Solution     AnyConnection Profiles     Address Assignment     Gonection Profiles     Connection Profiles     Connection Profiles     Group Policies     You Policies     Group Policies	Profile Usage   AnyConnect VPN Profile	Profile Location grp_b.xml c1_client_profile.xml
	Device Setup     Device Setup     Firewall     Set to -Site VPN     Device Monagement	OK Cancel Help	
	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	Apply Reset	

Profile Name	Enter the name for the connection profile (for example, <b>AnyConnectIPsecClient</b> ).
Profile Usage	Choose AnyConnect VPN Profile
Group Policy	Select an appropriate group policy (for example, GroupPolicyIPsec)

5. Click On the new profile created (In this example, AnyConnectIPsecClient) and in the right pane click Edit

🚮 Home 🦓	Configuration Monitoring	Save 🔇 Refresh 🔇 Back 🔅	Forward 💡 Help		CISCO
Remote A	ccess VPN 🗗 🖓	Configuration > Remote Access	s VPN > Network (Client) Access	s > AnyConnect Client Profile	
	oduction work (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localizz Bresources Briary Script Customized Installer Transform Customized Installer Transform	This panel is used to manage Anyt profile to edit, change group or to upload and download of client pro The profile Usage field is introduce later.	Connect Client Profiles and perform of delete. You can select the 'Add but files between local machine and devi d with the Secure Mobility Solution."	roup assignment for AnyConnect v ton to add a new profile. Pressing t ce. This field contains different profile of Dort B Export B Validate	ersion 2.5 or later. You can select a he Import or Export button is for usage in AnyConnect version 3.0 and
	AnyConnect Client Profile	Profile Name	Profile Usage	Group Policy	Profile Location
	Dynamic Access Policies	usergrp_b	AnyConnect VPN Profile	GroupPolicy3	disk0:/usergrp_b.xml
	Group Policies	IPsec1_dient_profile	AnyConnect VPN Profile	GroupPolicy_IPsec1	disk0:/IPsec1_client_profile.xml
	IPsec(IKEv 1) Connection Profiles	AnyConnectIPsecClient	AnyConnect VPN Profile	GroupPolicyIPsec	disk0:/anyconnectipsecclient.xml

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 6. Under AnyConnect Client Profile Editor click on left pane click on VPN and perform the following:
  - a. Select Use Start Before Logon.
  - b. Under Windows VPN Establishment, from the drop-down list choose AllowRemoteUsers.

N Preferences (Part 1) Preferences (Part 2)	Preferences (Part 1)		
Backup Servers Certificate Pinning Certificate Matching Certificate Enrollment Mobile Policy Server List		User Controllable	
	Auto Connect On Start	User Controllable	
	Minimize On Connect	User Controllable	
	Cocal Lan Access	User Controllable	
	Disable Captive Portal Detection	User Controllable	
	V Auto Reconnect	User Controllable	
	Auto Reconnect Behavior ReconnectAfterResume	User Controllable	
	🔽 Auto Update	User Controllable	
	RSA Secure ID Integration Automatic	User Controllable	
	Windows Logon Enforcement		
	SingleLocalLogon		
	Windows VPN Establishment		

7. In the AnyConnect Client Profile Editor window, select Server List and click Add.

erences (Part 1) erences (Part 2)	Server List						
ficate Pinning ficate Matching ficate Enrollment	Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate
le Policy er List							

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

- 8. In the Server List Entry window, perform the following and click OK:
  - a. In the Display Name (required) field, enter in the name that will be displayed on the client.
  - b. In the FQDN or IP Address field, enter the ASA Gateway FQDN or IP Address.
  - c. Under Connection Information, in the Primary Protocol field, select IPsec.
  - d. Select ASA Gateway.

Primary Server	Connection Information	
Display Name (required) Client_IPsec FQDN or IP Address https://ciscoasa1.sha2.com	User Group IV ASA gateway Auth Method During IKE Negotiation EAP-	AnyConnect 💌
Backup Servers Host Address	bba	
	Move Up Move Down	

9. If the server list was added successfully, click **OK**, click **Apply**, and click **Save**.

AnyConnect Client Profile Edito	or - AnyConnectIPs	secClient					About
VPN	Server List						Abbu
Backup Servers Certificate Pinning Certificate Matching Certificate Errollment Mobile Policy	Hostname Client_IPsec	Host Address https://ciscoasa1	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins
	Note: it is highly n	ecommended that at le	ast one server be d	efined in a profile.		Add	Details

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

10. The client profile XML file is created. Click **Export** to save this XML profile.

Home 🆓 Configuration 🔯 Monit	toring 🔚 Save 🔇 Refresh 🔇	Back 🔘 Forward  🦓 Help		Ċ	ISCO
Device List Bookmarks	Configuration > Remote Access VP	N > Network (Client) Access > Any	Connect Client Profile		
Device List 리 무 ×					
	This panel is used to manage AnyConn change group or to delete. You can sel profiles between local machine and dev The profile Usage field is introduced wit	ect Client Profiles and perform group as lect the 'Add' button to add a new profile <i>ice</i> . It the Secure Mobility Solution. This field	signment for AnyConnect version e. Pressing the Import or Export b l contains different profile usage i	2.5 or later. You can select a profile t utton is for upload and download of o n AnyConnect version 3.0 and later.	o edit, dient
	🖶 Add 🛛 🗹 Edit 👯 Change Gro	up Policy 📋 Delete 📳 Import 🖷	Export 🔐 Validate		
Remote Access VPN	Profile Name	Profile Usage	Group Policy	Profile Location	
Introduction	usergrp_b	AnyConnect VPN Profile	GroupPolicy3	disk0:/usergrp_b.xml	
AnyConnect Connection Profiles	IPsec1_client_profile	AnyConnect VPN Profile	GroupPolicy_IPsec1	disk0:/IPsec1_client_profile.xm	al
AnyConnect Customization/Local	AnyConnectIPsecClient	AnyConnect VPN Profile	GroupPolicyIPsec	disk0:/anyconnectipsecclient.x	ml
Resources Resources Guinary					
Device Management     *		Apply	Reset		



#### NOTE:

In this example the XML file is imported to the client manually after Client Installation is performed (see page 51).

Win 7 Client Profile Import Path:

%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

# **Client Installation**

In this example, Cisco AnyConnect - 4.5.02033 predeploy was installed with an MSI installer.

1. Click Setup

				x
anyconr	ect-win-4.5.02033-predeploy-k9 ►	✓  Search anyco	nnect-win-4.5.02033-pre	2 P
Organize 👻 🐻 Oper	n Share with 🔻 New folder		· · ·	0
🔶 Favorites	Name	Date modified	Туре	Size
Nesktop	Profiles	10/2/2017 2:08 PM	File folder	
🗼 Downloads	퉬 Setup	10/2/2017 2:08 PM	File folder	
🖳 Recent Places	🛃 anyconnect-win-4.5.02033-amp-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	1,
	😼 anyconnect-win-4.5.02033-core-vpn-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	8,
📜 Libraries	😼 anyconnect-win-4.5.02033-dart-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	2,
Documents	🛃 anyconnect-win-4.5.02033-gina-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	1,
🌙 Music	🛃 anyconnect-win-4.5.02033-iseposture-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	1,
E Pictures	😼 anyconnect-win-4.5.02033-nam-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	4,
📑 Videos	🔀 anyconnect-win-4.5.02033-nvm-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	1,
	😼 anyconnect-win-4.5.02033-posture-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	6,
👰 Computer	😼 anyconnect-win-4.5.02033-umbrella-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	2,
	😼 anyconnect-win-4.5.02033-websecurity-predeploy-k9	10/2/2017 2:07 PM	Windows Installer	1,
📬 Network	Setup	10/2/2017 2:07 PM	Application	
	setup	10/2/2017 2:07 PM	HTML Application	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

2. In the Cisco AnyConnect Secure Mobility Client Install Selector, select Core & VPN and Start Before Login, and then click Install Selected.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. Click Ok



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. To accept the End User License Agreement (EULA), click Accept.

Cisco	AnyConnect Secure Mobility Client EULA		X
	Supplemental End User License Agreement for AnyConnect® Secure Mobility Client v4.x and other VPN-related Software	•	
	IMPORTANT: READ CAREFULLY		
	This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You and the business entity you represent) and Cisco (collectively, the "Agreement"). Capitalized terms used in this SEULA but not defined will have the meanings assigned to them in the EULA. To the extent that there is a conflict between the terms and conditions of the EULA and this SEULA, the terms and conditions of this SEULA will take precedence.		
	In addition to the limitations set forth in the EULA on your access and use of the Software, You agree to comply at all times with the terms and conditions provided in this SEULA. DOWNLOADING, INSTALLING, OR USING THE SOFTWARE CONSTITUTES ACCEPTANCE OF THE AGREEMENT, AND YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE	*	
	Accept Decline		

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

5. Click OK on Installation complete

Cisco AnyConnect Secure Mobilit	ty Client Install Selector 🔜
Installation complete.	
	ОК

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

# **Running the Solution**

## Using the Cisco AnyConnect Secure Mobility Client SSL VPN

The Cisco AnyConnect Secure Mobility Client provides remote users with secure VPN connections to the Cisco ASA

In this example, a connected Token/Smart Card is used with an Alice smart card user certificate

1. Select Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

2. On the **Cisco AnyConnect Secure Mobility Client** window, in the field, enter the fully qualified domain name or IP address for Cisco ASA, and then click **Connect**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. In SafeNet Authentication Client Token Logon window, enter the Token Name and Token Password and click OK.

SafeNet Authentica	tion Client	gemalto*		
Enter the Token Password Token Name: Token Password:	My Taken •••••••• Current Language: EN	Cancel	**	
	Cancel	90	isco AnyConnect Secure Mobility Client	23
<b>R</b> V	Vindows <sup>-</sup> 7 Enterprise		VTE: Contacting https://csccaesi.sha2.com. https://cscceasi.sha2.com • Connect	

4. When the message "Your client certificate will be used for authentication" appears, Select the appropriate configured group alias (for example, AnyConnect) and click OK.

O Cisco	AnyConnect   https://ciscoasa1.sha2.com
Cisco /	OK Cancel
	VPN: Your client certificate will be used for authentication https://ciscoasa1.sha2.com Connect
<b>‡</b> (	altala cisco

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

The VPN Connection is established.





(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

#### **Cisco ASA Monitoring VPN connection**

VPN Connection can be monitored on Cisco ASA from the ASDM screen.

- 1. Click the Monitoring tab
- 2. Click VPN in the left pane
- 3. In the center pane, in the Filter by field, select the required filter from the drop-down list.

In this example, a Cisco AnyConnect Secure Mobility Client SSL VPN is established

Home 🗞 Configuration 🔯 Mo	nitoring 🔚 Save 🔇 R	Refresh 🕜 Back 🕥 Fo	rward 🦻 Help			CISCO
Device List Bookmarks	Monitoring > VPN > VPI	<u>N Statistics &gt; Sessions</u>				
Device List 리우×						
💠 Add 📋 Delete 🚿 Connect	Туре	Active	Cumulative	Peak	Concurrent	Inactive
Find: Go	AnyConnect Client SSL/TLS/DTLS		1	11 6	1	0
<u></u>	IKEv2 IPsec		0	5	1	0
VPN  VPN VPN VPN VPN Statistics Crypto Statistics	Filter By: AnyConnect C	Client 💽 All S Group Policy	essions Assigned IP Address	Protocol	Filter Login Time	Details
Compression Statistics	alice@sha2.com	Connection Profile GroupPolicySSL 1 AnyConnect 1	Public IP Address 72.19.19.23 0.0.0.200	Encryption AnyConnect-Parent SSL-Tu AnyConnect-Parent: (1)nor	Duration nnel DTLS 15: 17:06 IST Mon e SSL-Tu 0h:0 1m:45s	11551 Logout
Global IKE/IPsec Statistics Protocol Statistics U.U.NI Mapping Sessions Glentless SSL VPN Glentless SSL						Ping
Interfaces						
Properties	To sort VPN sessions, righ Logout By: All Session	nt-click on the above table an	d select Table Sort Order	from popup menu. ut Sessions		
			Re	fresh		

# **Using the Clientless SSL VPN**

The clientless SSL VPN creates a secure, remote-access VPN tunnel to Cisco ASA using a web browser without requiring a software or hardware client.

In this, example, a connected Token/Smart Card is used with an Alice smart card user certificate

- 1. Open the following URL in a web browser: https://<Public IP or Address of Cisco ASA>
- 2. On the Confirm Certificate window, click OK.



3. In the SAC Token Logon windows enter the Token Name and Token Password and click OK

🤶 Token Logon		×
SafeNet Authentication	on Client	gemalto <sup>×</sup>
Enter the Token Password		
Token Name:	My Token	
Token Password:	•••••	
	Current Language: EN	
		OK Cancel

The Login window a message "Your client certificate will be used for authentication" opens.

4. Select the appropriate configured group alias (in this Example **AnyConnect**) and click **Login**.

uluilu cisco	SSL VPN Service		
		Login	
	Your client ce	rtificate will be used for authentication	
	GRO	DUP: AnyConnect	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

The user is logged in.

e https://ciscoas	a1. <b>sha2.com</b> /+CSCOE+/portal.html	오 두 🚔 오 🖉 🎯 ciscoasa1.sha2.com	→ 伊 × × ① ☆ ③
uluulu cisco	SSL VPN Service		
Home     Web Applications     Browse Networks     AnyConnect	<ul> <li>[http:// v]</li> <li>[organization]</li> <li></li></ul>	Brows	e) [Logout]
Terminal Servers	3		

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

#### **Cisco ASA Monitoring VPN connection**

VPN Connection can be monitored on Cisco ASA from the ASDM screen.

- 1. Click Monitoring and then, in the left pane, click VPN.
- 2. In the right pane, select the required filter in the Filter By field.

In this example Cisco AnyConnect Secure Mobility Clientless SSL VPN is established

Home 🦓 Configuration 🔯 Mon	itoring 🔲 Save 🔇 Re	fresh 🔇 Back 🕥	Forward 🧖 Help			CISCO
Device List Bookmarks	Monitoring > VPN > VPN	Statistics > Sessions				
Device List 급 무 ×						
🕈 Add 📋 Delete 🚿 Connect	Туре	Active	Cumulative	e Pe	eak Concurrent	Inactive
Find: Go	AnyConnect Client SSL/TLS/DTLS	Par I	0 0	57 32	1	0
Mp. Foreitere	IKEv2 IPsec		0	25	1	0
	Clientless VPN Browser		1	12	3	
VPN - +	Filter By: All Remote Acc	ess 💌 🗖 All	Sessions	<b>_</b>	Filter	
Crypto Statistics	Username	Group Policy Connection Profile	Public IP Address Assigned IP Address	Protocol Encryptio	Login Time n Duration	e Details
Encryption Statistics	alice@sha2.com	GroupPolicySSL AnyConnect	10.0.0.200	Clientless Clientless: (1)AES128	11:42:05 IST T 0h:00m:27s	ue 203. Logout
Global INE/IPSec Statistics     Global INE/IPSec Statistics     Protocol Statistics     VLAN Mapping Sessions     Clentless SSL VPN     Easy VPN Client     VPN Connection Graphs     WSA Sessions						Ping
Interfaces						
	To sort VPN sessions, right	-click on the above table a	and select Table Sort Order	from popup menu.		
Roperties	Logout By: All Sessions	s 💌	Logo	out Sessions		
			Re	fresh		

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## Using the Cisco AnyConnect Secure Mobility Client - IPsec IKEv2 VPN

Prerequisites: See "Any Connect Client Profile", on page 45.

In this example, a connected Token/Smart Card is used with an Alice smart card user certificate

1. Click Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client.

🕤 Cisco AnyCo	nnect Secure Mobility Client			
	VPN: Ready to connect.	•	Connect	
<b>\$</b> ()			_	a halfa cisco

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

 On the Cisco AnyConnect Secure Mobility Client window, select the appropriate display name as configured in "Any Connect Client Profile" on page 45 (in this example Client\_IPsec) and then click Connect.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. On the Cisco AnyConnect - Certificate Selection window, click OK.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. In the SAC Token Logon window, enter Token Name and Token Password, and click OK

🤶 Token Logon		×	
SafeNet Authenti	cation Client	gemalto*	
Enter the Token Password			
Token Name:	My Token		
Token Password:	••••••		
	Current Language: EN		
		OK Cancel	lient 🗖 🛛 🖾
		Contacting Client_IPse	c.
	-	Client_IPsec	Connect
	\$	<b>i</b>	ofudio cisco

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

The message "Your client certificate will be used for authentication" is displayed.

5. Select the appropriate configured group alias (in this example, IPsec Connection) and click OK.

Cisco	Your die	nect   Client	_IPsec will be used fo	or authentica	tion	
🔊 Cisco	o AnyCon	nect Secure	ОК Mobility Clie	Cancel		8
		VPN: Your client ce Client_IPsec	rtificate will be	e used for au	thentication Connect	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

The VPN connection is established.

🕙 Cisco AnyCi	onnect Secure Mobility Client		
	VPN: Connected to Client_IPsec.	<b>–</b>	Disconnect
00:00:16			IPv4
<b>\$</b> ()			arfiailte cisco

## **Cisco ASA Monitoring VPN connection**

VPN Connection can be monitored on Cisco ASA from the ASDM screen.

- 1. Select the Monitoring tab, and click on VPN in the left pane
- 2. In the right pane, select the required filter in the Filter By field.

In this example, Cisco AnyConnect Secure Mobility Client IPsec VPN is established

Home 🖓 Configuration 🔯 Mon	itoring 🔚 Save 🔇 R	efresh 💽 Back 🔘	Forward 🤗 Help				CISCO
Device List Bookmarks	Monitoring > VPN > VPN	Statistics > Sessions	13				
Device List 리구 ×							
💠 Add 📋 Delete 🚿 Connect	Туре	Active	Cumulative	2	Peak Concurren	t	Inactive
Find: Go	AnyConnect Client		1	55		1	0
10.0.0.135	SSL/TLS/DTLS		0	31		1	0
	IKEv2 IPsec		1	24		1	0
	Clientiess VPN		0	11		3	
	browser		U	11		3	
VPN 라무							
P IVPN Statistics	Filter By: All Remote Acc	cess 💌 A	All Sessions	<b>•</b>	F	Filter	
		Group Policy	Public IP Address		Protocol	Login Time	Details
Compression Statistics	Username	Connection Profile	Assigned IP Address		Encryption	Duration	
Encryption Statistics	alice@sha2.com	GroupPolicyIPsec	10.0.0.200	IKEv2 IPsecO	verNatT AnyConnect-Pa		Logout
		AnyConnectIPsec	172.19.19.25	IKEV2: (1)AE	S256 IPsecOverNat1: (1	1. 0h:00m:11s 2	.90.
Protocol Statistics							Ping
VLAN Mapping Sessions							
H Easy VPN Client							
VPN Connection Graphs							
WSA Sessions							
Interfaces							
					_		ъ
A Routing	To sort VPN sessions, right	t-click on the above table	and select Table Sort Order	from popup m	enu.		
Properties	Logout By: All Session	IS ▼	Logo	out Sessions			
			Re	fresh			

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

## Start Before Logon (SBL)

**Start Before Logon** is a feature of the Cisco AnyConnect Client that allows the user to establish a VPN connection before logging onto the computer.

In this example, SSL VPN is demonstrated using a connected Token/Smart Card with the **Alice** smart card user certificate.

1. In User Log on Screen click Switch User.

	sha2.com\administrator	×
C	Password 🔊	

2. Click **Network Logon** button (next to the shut-down button).

	sha2.com/sdministrator Other/User Alice Smatricard (opion	*
R	Cancel	

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. On the **Cisco AnyConnect Secure Mobility Client** window, enter the fully qualified domain name or IP address for Cisco ASA, then click **Connect**.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

4. In the SAC Token Logon window, enter the Token Name and Token Password and click OK.

SofeNet Authentica SafeNet Authentica Prer file Token Password Token Password	tion Client My Token CurrentLanguage: EN OK	gemalto"	*
<b>R</b> . V	Concel	Cisco AnyConnect Se	cure Mobility Client E3 ng https://cscoasa1.sha2.com. Icscoasa1.sha2.com  Connect

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

The message "Your client certificate will be used for authentication" is displayed

5. Select the appropriate configured group alias (for example, AnyConnect) and click OK.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.) The VPN connection is established successfully before the user is logged in.



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

6. After logging on to windows, the AnyConnect Client is already connected



(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

# **Support Contacts**

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

## **Customer Support Portal**

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.



**NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

# **Telephone Support**

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	<b>Telephone number</b> (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421

Region	<b>Telephone number</b> (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Japan	0066 3382 1699
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608