

www.securenvoy.com

Cisco SA Integration Guide (ASA)

SecurAccess Integration Guide



Cisco ASA Integration Guide (ASA)

Contents

1.1	SOLUTION SUMMARY	3
1.2	GUIDE USAGE	3
1.3	PREREQUISITES	3
1.4	AUTHENTICATION	4
1.41 1.41	1 SETUP RADIUS CONNECTION	4
1.5	CISCO ANYCONNECT VPN (CLIENT)	6
1.5. 1.5. 1.5. 1.5.	1 VPN Wizard 2 ALIASES	6 7 7 8
1.6	CISCO CLIENTLESS SSL VPN ACCESS	8
1.6. 1.6. 1.6. 1.6.	1 VPN Wizard 2 ALIASES 3 AUTHORISATION 4 GROUP URL	9 9 10 11
1.7	DYNAMIC ACCESS POLICIES	12



1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Cisco's Adaptive Security Appliance (ASA) through the use of AAA Server for authorisation and Dynamic Access Policies for LDAP group membership and access control.

1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note two things:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described.

1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- A SecurAccess MFA server installed, configured and working on a system with:
 - Windows Server 2003 or higher.
 - Note: Please see SecurEnvoy's SecurAccess deployment guide on how to setup MFA server solution.
- A Cisco ASA appliance version 8.3 and above, with Adaptive Security Device Manager (ASDM) access and default AnyConnect client configuration to use for MFA.
 - Note: Default configuration can be configured by running the AnyConnect VPN wizard from the ASDM console.

3

- Cisco AnyConnect client software installed on all clients that connect remotely to the network unless the Clientless solution will be used.
 - Familiarity with the following technologies:
 - RADIUS configuration
 - Cisco ASA VPN appliance administration



1.4 Authentication

The following section describes the steps required to configure the Cisco ASA to authenticate users via RADIUS and assign security policies to users based on their LDAP groups.

1.41 Setup RADIUS Connection

Navigate to Configuration\Remote Access VPN\AAA/Local Users\AAA Server Groups and select add, to configure a new Server.

• Configure a AAA Server Group Name e.g. RADIUS and select the protocol RADIUS from the drop-down list, selecting OK to finish.

AAA Server Group:	RADIUS			
Protocol:	RADIUS			
Accounting Mode:	Simultaneous Single			
Reactivation Mode:	Depletion Timed			
Dead Time:	10 minutes			
Max Failed Attempts	s: 3			
Enable interim a	ccounting update			
Update Interval: 24 Hours				
Enable Active Directory Agent mode				
ISE Policy Enforcem	ent			
Enable dynamic	authorization			
Dynamic Autho	rization Port: 1700			
Use authorizatio	n only mode (no common password configuration r	equired)		
VPN3K Compatibili	ty Option	¥		

- Highlight the newly created Server group and click Add to define a new RADIUS server.
- Select the Interface Name (Usually the Cisco ASA interface that is closest to the RADIUS Server, which is the SecurEnvoy Server in this case).
- Fill in the Server Name (if using DNS or the IP address of the SecurEnvoy Server)
- Change the Server Authentication and Accounting port to 1812
- Enter in the Server Secret Key and Common Password that was configured and matches the key configured when RADIUS was setup on SecurEnvoy SecurAccess Server.
- Click OK to continue

📴 Edit AAA Server	×
Server Group: RADIUS Interface Name: www Server Name or IP Address: 192.168.1. Timeout: 29 seco	
RADIUS Parameters	
Server Authentication Port 1812 Server Accounting Port: 1812	
Retry Interval: 10 second	ds 🗸 🗸
Server Secret Key:	
Common Password:	
ACL Netmask Convert: Standard	\checkmark
Microsoft CHAPv2 Capable: 🔽	
SDI Messages	
Message Table	*
ОК Са	ancel Help



1.41 Setup LDAP Connection

- Navigate to Configuration\Remote Access VPN\AAA/Local Users\AAA Server Groups and select add, to configure a new Server.
- Configure a AAA Server Group Name e.g. LDAP and select the protocol LDAP from the drop-down list, selecting OK to finish.

🔯 Edit AAA Server Group 🛛 🗙				
AAA Server Group: Protocol:	LDAP LDAP			
Reactivation Mode:	Depletion O Timed			
Max Failed Attempts:	3			
ОК	Cancel Help			

- Highlight the newly created Server group and click Add in the Servers in the selected group section.
- Select the Interface Name (Usually the Cisco ASA interface that is closest to the LDAP Server, which is the Domain Controller in this case).
- Fill in the Server Name (if using DNS or the IP address of the Primary Domain Controller)
- Select the Server Type from the drop-down list (Dependent on your type of LDAP Server)
- Enter the Base DN: of your domain in the format DC=your-domain-name,DC=com
- Enter in an account username and password that has read access to the domain controller under the section Login DN: and Login Password
- Complete the Group Base DN: of your domain in the format DC=your-domain-name,DC=com
- Click OK to continue

Edit AAA Server ×	
Server Group: LDAP Interface Name: Server Name or IP Address: 192.168.1.1 Timeout: 10 seconds LDAP Parameters for authentication/authorization	
Server Port: 389 Server Type: Microsoft Base DN: DC=domain,DC=com Scope: All levels beneath the Base DN Naming Attribute: Image: Common second s	
Group Base DN: DC=domainDC=com Group Search Timeout: 10	



1.5 Cisco AnyConnect VPN (Client)

The following section describes steps required to configure the Cisco AnyConnect SSL VPN client to authenticate with SecurEnvoy's MFA solution, using LDAP groups to define the Cisco ASA security policy that will be assigned to the user.

1.5.1 VPN Wizard

- Run the Cisco AnyConnect VPN Wizard from the Cisco ASDM and give it a meaningful Connection Profile name e.g. Client-SSL
- Navigate to Wizards\VPN Wizards\AnyConnect VPN Wizard.... From the Cisco ASDM tool bar.
- Note: Select the previously configured group RADIUS when the wizard asks for Authentication methods.
- On completion of all steps in the Wizard, navigate to the Remote Access VPN connections section. Configuration\Remote Access VPN\Network (Client) Access\AnyConnect Connection Profiles
- From the Network (Client) Access home page, make sure "Allow user to select connection profile on the login page" is selected.

The securi Client sup	ty appliance auto ports IPsec (IKE)	omatically deplo /2) tunnel as w	oys the Cisco Ar ell as SSL tunne	yConnect VPN Client to re I with Datagram Transpor	emote users u t Layer Securi	pon connection. The ir ty (DTLS) tunneling op	nitial client deployment requires end-u tions.	ser administrative rights. The Cisco AnyConnect VPN
Access Inter	aces							
Enable	Cisco AnyConn	ect VPN Client a	access on the in	terfaces selected in the tab	le below			
SSL access	must be enable	d if you allow A	AnyConnect clie	nt to be launched from a l	orowser (Web	Launch) .		
Interface	SSL Access		IPsec (IKEv2)	Access	Device C	ertificate		
outside	Allow Access	Enable DTLS	Allow Access	Enable Client Services	Ces Port Settings			
Access list	s from group po Setting user to select co wwn portal login Profiles n profile (tunnel	licy and user pontential provided and the provided and th	olicy always app on the login pa es how user is a	ly to the traffic.	rameters. You	can configure the maj	oping from certificate to connection pr	ofile <u>here</u> .
₩ Add @	Edit 🔟 Delete	CCL Enabled		IDees Enabled		Alizon	Authentication Method	Craup Balia
Name	C	SSL EndDied		IPSec Enabled		Alldses		Group Policy
DefaultRA	Group							DfltGrpPolicy
Clientless	/PN					web		GroupPolicy Clientless-SSI
Client-SSI						Client-SSL	AAA(RADIUS)	GroupPolicy_Client-SSL



1.5.2 Aliases

On completion of the Wizard, we will need to create an alias for the newly created Client-SSL profile.

- Highlight and edit the newly created Client-SSL Profile
- Create a meaningful name under the Aliases section

2 Edit AnyConnect Connection Profile: Client-SSL	~
Basic Name: Client-SSL Advanced -General Aliases: -Client Addressir Authentication -Authentication Authentication -Accounting Method: -Group Alias/Gre Method: AAA Server Group: RADIUS Use LOCAL if Server Group fails	9

1.5.3 Authorisation

The following section will configure the ASA to check the user logging in, is present in the LDAP directory before allowing access.

- Whilst editing the Connection Profile, select the Advanced\Authorization section
- Select from the list, the previously created LDAP Group and select Users must exist in the authorisation database to connect
- Click OK to continue

Basic Advanced - General - Client Addressit - Authentication - Secondary Auth - Accounting - Accounting - Group Alias/Gro	Authorization Server Group Server Group: DAP Users must exist in the authorization database to connect Interface-specific Authorization Server Groups Add gr Edit Delete	
	Interface Server Group www LDAP	
	Username Mapping from Certificate Specify the certificate fields to be used as the username Primary Field: CN (Common Name) Secondary Field: OU (Organization Unit) Use the entire DN as the username Use script to select username Add of Edit Delete	
Find:	Next Previous	



1.5.4 Group Policy

As best practice it is advisable to create a Group Policy for the newly created AnyConnect SSL Client VPN.

- Navigate to Configuration\Remote Access VPN\Network (Client) Access\Group Policies
- Click Add (Select Internal Group Policy if asked) and provide a meaningful name e.g. GroupPolicy_Client-SSL
- Untick the Inherit checkbox next to Tunnelling Protocols and uncheck all except SSL VPN Client

If it is required for the client to have local internet breakout additional to the VPN tunnel, then this can be configured under Split Tunnelling in the Advanced section of the Group Policy.

On completion of the above configuration, select OK to proceed

We now need to assign the Group Policy to the Connection Profile created following the run of the VPN Wizard.

- Highlight the newly created GroupPolicy_Client-SSL and click Assign
- Tick the box next to the Connection Profile created earlier e.g. Client-SSL

assign Group Policy: GroupPolicy_Cl	×
Assign the selected group policy to one or more connection profiles or LOCAL users.	
Connection Profile DefaultRAGroup DefaultL2LGroup DefaultWEBVPNGroup defaultWEBVPNG defaultWE	
OK Cancel Help	

1.6 Cisco Clientless SSL VPN Access



1.6.1 VPN Wizard

- Run the Cisco Clientless SSL VPN Wizard from the Cisco ASDM and give it a meaningful Connection Profile name e.g. Clientless-SSL
- Navigate to Wizards\VPN Wizards\ Clientless SSL VPN Wizard.... From the Cisco ASDM tool bar.
- Note: Select the previously configured group RADIUS when the wizard asks for Authentication methods.
- As best practice it is advisable to create a new Group Policy for the Clientless SSL VPN. When the Wizard asks for group policy, select Create New Group Policy and give it a meaningful name e.g. GroupPolicy_Clientless-SSL
- Complete the Wizard and select Finish
- On completion of all steps in the Wizard, navigate to the Remote Access VPN connections section.
 Configuration\Remote Access VPN\Clientless SSL VPN\Connection Profiles
- From the Connection Profiles home page, make sure "Allow user to select connection profile on the login page" is selected.

acc Interfaces									
	linethere CCL 1								
nable interfaces for c	inenuess SSL	VPN access.							
Interface	Allow Acce	ess	Davica Cartificat	0					
outside			Device Certificati	e					
dap			Port Setting						
N3N3N		<u> </u>	1						
Bypass interface a	ccess lists for	inbound VPN sessio	ons						
Access lists from arou	n policy and i	user policy always a	apply to the traffic.						
in Page Setting									
Allow user to sele	ct connection	profile on the login	page. 🙃						
Allow upon to onto	r internal man	used on the login							
Allow user to ente	r internal pas	sword on the login	page.						
Shutdown portal le	ogin page.								
inection Profiles									
Connection profile (tu	innel group) s	pecifies how user is	s authenticated and ot	her parameters. You ca	n configure the map	ping from certificate to	connection profile	here.	
🕈 Add 🗹 Edit 📋 De	lete Find:		○ ○ Match	Case					
Name		Enabled		Aliases	Auth	entication Method		Group Policy	
DefaultRAGroup					AAA(LOCAL)		DfltGrpPolicy	
DefaultWEBVPNGroup)				AAA(RADIUS)		DfltGrpPolicy	
ClientlessVPN			✓ \	web	AAA(RADIUS)		GroupPolicy_Clientless-SSL	
lient-SSL				Client-SSL	AAA(RADIUS)		GroupPolicy_Client-SSL	
	o procedence	if aroun LIDL and a	artificate man match d	lifferent connection prof	files Otherwise the	connection profile that	natches the sertific	nto man will be used	

1.6.2 Aliases



On completion of the Wizard, we will need to create an alias for the newly created Clientless-SSL profile.

- Highlight and edit the newly created Clientless-SSL Profile
- Create a meaningful name under the Aliases section e.g. Web
- Make sure the Group Policy created during the VPN Wizard is selected from the list

Basic Advanced	Name:	ClientlessVPN	
Auvanceu	Aliases:	web	
	Authentication		
	Method:	• AAA Certificate AAA and Certificate Saml	
	AAA Server Group:	RADIUS	✓ Manade
		Use LOCAL if Server Group fails	
	DNS		
	Server Group:	DefaultDNS	Manage
		(Following fields are attributes of the DNS server group selected above.)	
		Servers: 8.8.8.8	
		Domain Name: aq.net.uk	
	Default Group Policy		
	Group Policy:	GroupPolicy_Clientless-SSL	✓ Manage
		(Following field is an attribute of the group policy selected above.)	
		✓ Enable clientless SSL VPN protocol	
	SAML Identity Provide	r	
	SAML Server :	None	✓ Manage

1.6.3 Authorisation



The following section will configure the ASA to check the user logging in, is present in the LDAP directory before allowing access.

- Whilst editing the Connection Profile, select the Advanced\Authorization section
- Select from the list, the previously created LDAP Group and select Users must exist in the authorisation database to connect
- Click OK to continue

🔯 Edit AnyConnect	Connection Profile: Client-SSL X
→Basic Advanced -General -Client Addressir -Authentication -Secondary Auth -Authorization -Accounting -Group Alias/Gro	Add af Edit in Delete
	Interface Server Group WWW LDAP
	Username Mapping from Certificate
	Specify the certificate fields to be used as the username Primary Field: CN (Common Name) Complete Set (LTR)
	Use the entire DN as the username
< >	- None Add # Edit Delete
Find:	Next Previous
	OK Cancel Help

1.6.4 Group URL

This section will configure a group URL that will automatically select the correct connection profile for the Clientless SSL VPN when the user browses to the Cisco ASA with the included alias. This URL can be bookmarked in the client's browser to return to the same URL for connectivity.

- From within the same Clientless SSL VPN Connection profile select Clientless SSL VPN from the left-hand navigation.
- Make sure the Connection Aliases configured earlier is ticked
- Under Group URL's, select Add and type in the full URL that the user will use to access the Clientless SSL VPN portal, appending the alias created earlier e.g. /web
- Select Disable CSD for both AnyConnect and Clientless SSL VPN
- Click OK to continue

Note: When clients browse to the Clientless VPN portal, please use the URL you defined under Group URL's. If the alias is not used it will present a drop-down box for the client to select at login.

🔟 Edit Clientless SSL VF	N Connection Profile: ClientlessVPN		\times	
Basic Advanced - General - Authentication - Secondary Authentic - Authorization - Accounting NetBIOC Scenars	Login and Logout Page Customization: DfltCustomization Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of SecurId messages on the login screen	✓ Manage		n Guic ′ <mark>oy.co</mark>

04/18



1.7 Dynamic Access Policies

The following section describes steps required to configure the Cisco ASA to authenticate with SecurEnvoy's MFA solution, using LDAP groups to create individual polices against the LDAP directory group that the user is part of, restricting what applications or networks they are allowed to access. These groups are reutilised for both the Client based VPN profile as well as the Clientless VPN Portal access.

> Navigate to Configuration\Remote Access VPN\Network (Client) Access\Dynamic Access Policies

The first thing we need to do is make sure the default policy blocks or denies access to users if they are not approved to connect and login.

- Highlight DfltAccessPolicy and click Edit
- Under the Action tab, select Action: Terminate
- Click OK to continue

04/18

Policy Name: Df	ItAccessPolicy				
Description:					
Accose/Authori	zation Doligy Attrib	utoc			
Access/Authori	zation Policy Attrib	utes attributes for this policy. Att	ribute values specified here will override those values obt	tained from the	
Access/Authori Configure acc	zation Policy Attrib ess/authorization a and the group-poli	utes attributes for this policy. Att cy hierarchy. The resulting	ribute values specified here will override those values obt	tained from the	
Access/Authori Configure acc AAA system attributes, an	zation Policy Attrib :ess/authorization a and the group-poli d group-policy hier	utes attributes for this policy. Att cy hierarchy. The resulting rarchy attributes (those that	ribute values specified here will override those values obt vPN authorization policy is an aggregation of DAP attribu are not specified in DAP).	tained from the ites, AAA	AS
Access/Authori Configure acc AAA system attributes, an Port For	zation Policy Attrib :ess/authorization a and the group-poli d group-policy hier warding Lists	utes attributes for this policy. Att cy hierarchy. The resulting rarchy attributes (those that Bookmarks Access	ribute values specified here will override those values obt vPN authorization policy is an aggregation of DAP attribu are not specified in DAP). Method AnyConnect AnyConnect Custon	tained from the ites, AAA m Attributes	AS

ASA Integration Guide www.securenvoy.com



We will now create Dynamic Access Polices that determine a user's privileges based on a particular LDAP group.

- Navigate to Configuration\Remote Access VPN\Network (Client) Access\Dynamic Access Policies
- Select Add to create a new Dynamic Access Policy and provide a meaningful name under • Policy Name E.g. Privileged-User
- Define which LDAP group the user will be matched against in order to be assigned this policy by selecting Add from the Selection Criteria

cription: Dynamic Acco	ess Policy for Privileged Users with no F	Restrictions			ACL Priority: 0	
ection Criteria Define the AAA and end ind every endpoint attrib expression text. User has ANY of the foll	point attributes used to select this access oute has been satisfied. These attributes owing AAA Attributes values	ss policy. A policy is s can be created usin	used when a user's auth g the tables below and/ and the following e	norization attributes match or by expanding the Advar endpoint attributes are satis	the AAA attribute onced option to spec	criteria below ify the logica
AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/V	/alue	Add
dap.memberOf	= VPNAdmin	Edit				Edit
		Delete				Delete
						Logical Op.
cess/Authorization Polic Configure access/authori ilerarchy. The resulting ' n DAP).	y Attributes zation attributes for this policy. Attribul VPN authorization policy is an aggregat	te values specified he lion of DAP attribute	ere will override those va s, AAA attributes, and g	alues obtained from the A group-policy hierarchy attri	AA system and the ibutes (those that a	group-policy re not specific
ccess/Authorization Polic Configure access/authorit lierarchy. The resulting ' n DAP). Port Forwarding Action	y Attributes zation attributes for this policy. Attribut VPN authorization policy is an aggregat g Lists Bookmarks Network ACL Filters (client)	te values specified he tion of DAP attribute Access Method	ere will override those vo s, AAA attributes, and g AnyConnect Webtype AC	alues obtained from the Au proup-policy hierarchy attri AnyConn 1. Filters (clientless)	AA system and the ibutes (those that an nect Custom Attribu F	group-policy re not specifi tes Functions
cess/Authorization Polic Configure access/authori lierarchy. The resulting' n DAP). Port Forwarding Action Action Action: O Continue Specify the message It User Message:	y Attributes zation attributes for this policy. Attribut VPN authorization policy is an aggregat g Lists Bookmarks Bookmarks Network ACL Filters (client) Quarantine O Terminate O aat will be displayed when this record is ged Users Policy	te values specified he ion of DAP attribute Access Method s selected.	re will override those vi s, AAA attributes, and g AnyConnect Webtype AC	alues obtained from the A. proup-policy hierarchy attri AnyConn I. Filters (clientless)	AA system and the lbutes (those that a nect Custom Attribu F	group-policy re not specifi tes Functions

- We will now select the LDAP group by selecting LDAP from the list AAA Attribute Type
- Make sure the Attribute ID: has memberOf specified in the field
- Select Get AD Groups and browse for the AD group that you would like to match against • this Dynamic Access Policy
- Click OK to continue

🖺 Edit AAA Attribute X	
AAA Attribute Type: LDAP Attribute ID:	isco ASA Integration Guide www.securenvoy.com

04/18



- Dependent on the level of restrictions required on the Dynamic Access Policy, it is possible to define an ACL restricting the users network access to applications or locations.
- Select the Network ACL Filters (Client) tab under Access/Authorisation Policy Attributes and select from the drop-down list or create (Manage) a new ACL that can be assigned to the group.

Port Forwardin	iq Lists Bookmarks	Access Method	AnyConne	ect	AnyConnect Custor	n Attributes
Action	Network ACL Filters (dient)		Webtype	ACL Filters (client)	ess)	Function
				Network ACLs		
outside covotomar	2	~	Add>>	UserVPN		
ouside_dyptoining	,	Managa	Addy			
		Manage	Delete			

Please Reach Out to Your Local SecurEnvoy Team...



UK & IRELAND

The Square, Basing View Basingstoke, Hampshire RG21 4EB, UK

Sales

- E sales@SecurEnvoy.com
- T 44 (0) 845 2600011

Technical Support

- E support@SecurEnvoy.com
- T 44 (0) 845 2600012



EUROPE

Freibadstraße 30, 81543 München, Germany

General Information

E info@SecurEnvoy.com T +49 89 70074522



ASIA-PAC

Level 40 100 Miller Street North Sydney NSW 2060

Sales

E info@SecurEnvoy.com T +612 9911 7778



USA - West Coast

Mission Valley Business Center 8880 Rio San Diego Drive 8th Floor San Diego CA 92108

General Information

- E info@SecurEnvoy.com
- T (866)777-6211



USA - Mid West

3333 Warrenville Rd Suite #200 Lisle, IL 60532

General Information

E info@SecurEnvoy.com T (866)777-6211



USA - East Coast

373 Park Ave South New York, NY 10016

General Information

E info@SecurEnvoy.com T (866)777-6211



www.securenvoy.com

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010 Company No. 04866711 VAT Number GB 862076128