



Cisco ASA SSL VPN and

SendQuick ConeXa One-Time-Password

Configuration Guide

Prepared by

TalariaX Pte Ltd

No. 11 Howard Road #04-00 Tat Hong Industrial Building Singapore 369583

> Tel: +65 62802881 Fax: +65 62806882

E-mail: info@talariax.com Web: www.talariax.com

CISCO ASA SSL VPN & SENQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

This document is prepared as a guide to configure Cisco ASA SSL VPN to run with SendQuick Conexa for One-time-password via SMS.

The pre-requisite is that SendQuick Conexa OTP server is configured with RADIUS on port 1812. Ensure that both applications are using the same port for radius.

The software version for Cisco ASA is

2.0 CONFIGURE CISCO SSLVPN

First login into the Cisco ASDM management console. In the Cisco SSL VPN configuration, select **Remote Access VPN > AAA Local Users > AAA Server Groups** and **Add** a new **AAA Server** as shown below.



Figure 1: Authentication Server Configuration

In the pop-up window, provide a server group name for the sendQuick Conexa (eg, Conexa), select the **Radius** protocol and leave the failed attempts as 3, as shown in Figure 2 below.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
Conexa	RADIUS	Single	Depletion	10	3
OCAL	LOCAL				
		Constant and the second	to make the second s		
		🗯 Add AAA Serve	r Group		
		Server Group:	Conexa		
		Protocol:	RADIUS		
		Accounting Mode:	🔿 Simultaneous 💿 Sir	ngle	
	exercised of	Reactivation Mode		med	
vers in the Selected	Group	- Kededvodon Hode.		ilea	
Server Name or IP	Address	Dead Time: 10	minutes		Timeout
192. 168. 1. 144		Max Failed Attempts	3	_	
		Enable interim ac	counting update		
				(2)	
		VPN3K Compatib	liity Option	۲	

Figure 2: Add AAA Server Group

Select **OK** once completed. Then, select the Conexa server group and add a server configuration as shown in Figure 3 below.

In the Add AAA Server pop-up window, configure the following items as below:

- Interface Name Inside
- Server Name or IP Address IP address of sendQuick Conexa
- Timeout configure a value of between 40-60 seconds (value need to be higher than 25 seconds for the system to perform well)
- Authentication Port (for Radius): 1812 (this must be 1812 as this is the port used in Conexa). Accounting port value is non-important as it is not used. Hence, a value of 1813 is fine.
- Shared secret the same secret need to be included in Conexa
- ACL Netmask Standard

Once completed, select **OK** and the server is configured.

Server Group	Protoc	ol Accounting Mo	ode	Reactivation Mode	Dead Time		Max Failed Attempts
Conexa	RADIUS	Sinale		Depletion	110	1.	
OCAL	LOCAL	🕼 Add AAA Server					
		Server Group:	Co	nexa			
		Interface Name:	ins	side	*		
		Server Name or IP Address: 192.168.1.144 Timeout: 10		192.168.1.144			
				seconds	s.		
		RADIUS Parameters —					a l
-		Server Authentication	Port:	1812			-
vers in the Selected Group —		Server Accounting Pol	rt:	1813			
Server Name or IP	Address	Retry Interval:	[10 seconds	~		Timeout
192.168.1.144	-	Server Secret Key:	[•••••			
		Common Password:	[
		ACL Netmask Convert	: [Standard	~		
		Microsoft CHAPv2 Cap	pable: [✓			
		SDI Messages					8
		Message Table				*	

Figure 3: Add AAA Server

After configuring the AAA servers, it is necessary to configure the IPSec and SSLVPN (clientless) profile for the user to access using the different modes.

This is explained in Figure 4 and 5 respectively.

In the Cisco ASDM, select **Remote Access VPN** > **Network (Client) Access** > **IPSec Connection Profiles** (for IPSec). You will need to Add an IPSec profile and the window in Figure 4 will appear.

Select Conexa (which was configured earlier) in User Authentication > Server Group. This will direct the authentication to Conexa, for IPSec authentication sessions.

For the rest of the IPSec configuration, consult the Cisco manual or refer to your Cisco service provider.

Once the configuration is completed, select **OK** as shown in Figure 4 below.

inside nnection Profiles Connection profile (tunnel group)	IKE Peer Authentication Pre-shared Key: Identity Certificate:	•••••••		Manage
Innection Profiles	Identity Certificate:	None		Manage
nnection Profiles	User Authentication —			
inection Profiles	Part Hartertacadori			
	Server Group:	Conexa	•	Manage
🗣 Add 🗹 Edit 🛅 Delete	Fallback:	Conexa LOCAL		
Name	Client Address Assigned	nt		
IPSecVPN DefaultRAGroup	DHCP Servers:			
SSLVPN	Client Address Pools:	IPVPN_Pool	[Select
IPSecLimitedVPN DefaultWEBVPNGroup	Default Group Policy —			
	Group Policy:	IPSecVPN		Manage
		(Following fields are attribute	s of the group policy	selected above.)
			eren a	
		Enable L2TP over IPsec p	rotocol	

Figure 4: Configure IPSec Profile

Configuration > Remote Access VPN > C	ientless SSL VPN Access > C	onnection Profiles		
Access Interfaces	🚰 Add Clientless SSL VPN	Connection Profi	ile	
Enable interfaces for clientless SSL VPN acc				
Interface A		Name:	SSLVPN	
outside		Aliases:	SSLVPN	
inside		Authentication		
		Method:	⊙ AAA O Certificate O Both	
Access Port: 443		AAA Server Group:	Conexa 💌	Manage
			Conexa	
Click here to Assign Certificate to Interfac		0.000	LOCAL	
Login Page Setting		DNS		
Allow user to select connection profile,		Server Group:	DefaultDNS 💌	Manage
Allow user to enter internal password o			(Following fields are attributes of the DNS server group selected above.)	
			Servers: 165.21.83.88, 165.21.100.88	
Connection Profiles			Domain Name: default.domain.invalid	
Connection profile (tunnel group) specifies				
Add Add Edit Delete		Default Group Policy		
Name Enabl		Group Policy:	DfltGrpPolicy	Manage
IPSecVPN			(Following field is an attribute of the group policy selected above.)	
DefaultRAGroup			Enable clientless SSL VPN protocol	
SSLVPN				
IPSecLimitedVPN				
DefaultWEBVPNGroup				
				-
	Find:		Next Previous	
		-		

Figure 5: Configure Clientless SSL VPN Profile

Similar to configuring the IPSec profile, you will need to configure the Clientless SSL VPN profile as well. In the Cisco ASDM, select **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles** (for SSLVPN). You will need to **Add** a new SSL VPN profile as shown in Figure 5 above.

Assign a Name to the profile. In Authentication, select AAA and Conexa (configured earlier) in AAA Server Group. This will direct the authentication to Conexa, for SSL VPN authentication sessions.

For the rest of the SSL VPN configuration, consult the Cisco manual or refer to your Cisco service provider.

Once the configuration is completed, select **OK** as shown in Figure 5 above.

After this configuration, you can access via SSL VPN or IPSec with SMS OTP. The example of SSL VPN and IPSec login using 2FA as described in the next section.

3.0 REMOTE ACCESS WITH TWO FACTOR AUTHENTICATION

Before accessing using IPSec or SSL VPN, you may need to configure the user policy or grouping in the Cisco ASA. Please refer to Cisco ASA manual for the required configuration.

After configuring, start the IPSec client and select the Connection required and the dialog box for Username and Password will appear as shown in Figure 6 below.

Cancel Connect New	Import Modify	Delete	ahaha cisco
Connection Entries Certi	ficates Log	1	1-
Connection	Entry /	Host	
TalariaxLimit	ed	202.172.41.229	IPSec/UDP
	C. VDN		

Figure 6: IPSec Login with Username and Password

Enter the **Username** and **Password** and select **OK**. Once the first authentication is successful, the Enter OTP page will appear as shown in Figure 7 below.

The OTP will be sent to the mobile phone. Enter the **OTP** in the space provided and enter **OK** (Figure 7). Once it is approved, the IPSec will make the connection and the yellow closed padlock will appear at the bottom of the Window taskbar (Figure 8 below).

👌 status: Di	sconnected VPN Client - Version 5	.0.06.0160	
Connection Ent	ries Status Certificates Log Options Help	p	
Cancel Connec	t New Import Modify	Delete	cisco
Connection Ent	tries Certificates Log		
	Connection Entry	Host	Transport
	TalariaX	202.172.41.229	IPSec/UDP
-	VPN Client User Authentication	on for "TalariaX"	
Authenticating	cisco Response:	OK Cancel	

Figure 7: OTP Prompt for IPSec



Figure 8: Successful Connection for IPSec

When accessing using SSL VPN, open a web browser and access the Internet address (URL) for SSL VPN access. The Username and Password will appear as shown in Figure 9 below.

() C (X) (h) (202.172.41.229 https://202.172.41.229/+CSCOE+/logon.html	Google •
Most Visited * Getting Started Latest Headlines & Apple Yahool Google Maps YouTube Wikipedia News * Popular * jsfavourites * SSL VPN Service +	
CISCO SSL VPN Service	

Please enter	your username and password
USERNAME	E: khin
PASSWORD):

Figure 9: SSLVPN Login with Username and Password

Enter the **Username** and **Password** and select **Login**. Once the first authentication is completed, an Enter OTP page will appear on the web page. The SMS will be sent to the mobile phone.

Enter the OTP in the **Response** space provided and select **Continue**, as shown in Figure 10 below. Once the second factor authentication is approved, the success page or user access realm will be shown as in Figure 11 below. Do note that the AnyConnect client can be used at this stage as well.

cisco	SSL VPN Service		
		Login	
		Enter OTP:	
		More information is required to log in.	
		Response	
		(Continue) (Cancel)	

Figure 10: Enter OTP for SSL VPN Authentication

Home Addres	s http:// +	Browse
Image: Web Applications I	AnyConnect	Initiate an AnyConnect client session to provide client applications on your deskton network access through your VPN, depending on your company's VPN configuratio your own network access rights. For example, an AnyConnect session might be necessary to use Microsoft Outlook or Microsoft Outlook Express to send or receiv e-mail. The following instructions describe how you can use your browser to get remote a to Microsoft Terminal Services running on computers in your network: Bedore you Connect - Add to Trusted Sites How to Connect Always Log Outl Requirements To access remote services over an AnyConnect client session, your system must h the following setup: Your VPN site must be in the list of trusted sites, as described below. (Requ for Windows Vista, highly recommended for all.) The operating system must be Microsoft Windows XPS P1 of Windows 2000 SP4, Linux (RedHat Linux 9, RedHat Enterprise Linux 3, SUS Linux 10, Exclorement 14, or Expend or 65, or Mic OF 21.10.4

Figure 11: Successful Access with SSL VPN