Configuring TOTPRadius and 2FA for Cisco Anyconnect

This guide will document how to configure 2 factor authentication on a Cisco ASA, using Microsoft Active Directory as the first factor and TOTPRadius Server as the second. The configuration is applied through the Cisco Adaptive Security Device Manager (ASDM) configuration tool. The assumption is made that you have a working Anyconnect VPN profile on the ASA, have deployed the TOTP appliance into an appropriate virtual environment and performed basic configuration steps such as setting an IP address and adding the server to DNS, can log in to the Admin Panel using the default username and password, and have tested reachability from the ASA INSIDE interface to the TOTPRadius Server.

TOTPServer configuration

General Settings

AnyconnectVPN Home Use	er List New user	Admin Panel	admin 👻
General Settings			
Site name 🕑	AnyconnectVPM	N	
Allow initial login 9	1		
Api key 🕑			generate
Allow http 🕑	Enabled		¥
Radius secret			generate
	after modifying RADI	IUS settings you m	ay need to restart RADIUS service (under "advanced settings")
Endpoint ip 9	10.		
Endpoint subnet 9	255.255.255.255		
Totp skew 🔮	1		

- 1. Site Name The name of this installation, will appear in any TOTP app you use. In this instance *"mycompany*AnyconnectVPN" was used.
- 2. Allow Initial Login must be set to 1 to allow self-service TOTP registration. Otherwise 0.
- 3. API key not required for ASA integration
- 4. Allow HTTP not required for ASA integration
- 5. Radius Secret Make note of this for later, generate a new one if required. Used to secure communication between ASA and TOTPRadius Server.
- 6. Endpoint IP the IP address of the INSIDE interface of the Cisco ASA.
- 7. Endpoint Subnet 255.255.255.255 to allow only the ASA to authenticate against this server.
- 8. TOTP Skew Set to 1 to allow for time sync issues between client and server.

LDAP Settings



- 1. LDAP Disabled
- 2. Enforce 2fa Disabled
- LDAP Server IP address/hostname of active directory DC(s). In this instance, 2 DCs in format Idap://Server1IP Idap://Server2IP
- 4. LDAP Username Format <u>%username%@mydomain.com</u>
- 5. LDAP Search String DN for LDAP to search, in this instance the DN of the entire domain, DC=*MyDomain*, DC=COM.
- 6. LDAP Group Restrict Leave blank
- 7. Click Test LDAP Connection button and enter active directory login details into pop-up window. This test should now succeed.
- 8. Allow LDAP enrolment Allow users to log into a portal to self-serve the creation of their second factor.
- 9. LDAP Admins provide comma separated list of LDAP accounts allowed access to the admin portal please note, at time of writing this list is case-sensitive.

ASA Configuration

In the ADSM, go to Configuration > Remote Access VPN > AAA/Local Users > AAA server Groups.

	Home 🚳 Configuration 🔯 Monitoring 🗐 Save 🄇	1
10	Remote Access VPN ASDM Assistant	
narks	Remote Access ¥PN 🗗 🖓	
Book	 Introduction Network (Client) Access Clientless SSL VPN Access AAA/Local Users AAA/Local Users AAA Server Groups MDM Proxy Local Users Secure Desktop Manager Certificate Management Load Balancing DHCP Server DNS Advanced 	
	Pevice Setup	
	🗊 Firewall	
	Remote Access VPN	
	Site-to-Site VPN	
	Device Management	
	*	

We are going to add 2 separate server groups, one LDAP server group to carry out the first authentication against active directory, and a second RADIUS group to authenticate against our TOTPRadius Server instance.

First, we will set up the TOTPRadius Server

Click the Add button next to the AAA Server Groups as highlighted below.

F c	isco ASDM 7.10(1) for ASA - 10		
File	View Tools Wizards Window Help	Type topic to search	Goll
	Home 🗞 Configuration 🔯 Monitoring 🔚 Save 🤇	Refresh 🔇 Back 🕥 Forward 🧳 Help	CISCO
9	Remote Access VPN ASDM Assistant	Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups	
kmark	Remote Access VPN 리 무	AAA Server Groups	
Bool	Introduction Network (Client) Access	Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts	Add
	Clientless SSL VPN Access	LOCAL	Edit
	AAA/Local Users		Delete
	Local Users	Find: 💿 🔾 🗖 Match Case	
	Gertificate Management		
	anguage Localization	Servers in the Selected Group	-
		Server Name or IP Address Incerrace Timeouc	Had
	DNS		Edit
	±₩ Advanced		Delete
			Move Up
	Device Setup		Move Down
	🛐 Firewall		Test
	Remote Access VPN		
	Site-to-Site VPN	Find: 🔘 🔘 🗖 Match Case	
	Device Management	LDAP Attribute Map	¥
	» *	Apply Reset	

In the popup window that appears, give your server group an appropriate name. The remaining settings can be left at default setting. Hit OK.

🧱 Add AAA Server 0	Group 🗙
AAA Server Group: Protocol:	2FARADIUS
Accounting Mode:	C Simultaneous ⓒ Single
Reactivation Mode:	Depletion C Timed
Max Failed Attempts:	3
🔲 Enable interim acco	ounting update
Update Interv	al: 24 Hours
ISE Policy Enforcement	t
🥅 Enable dynamic au	Ithorization
Dynamic Authoriza	tion Port: 1700
Use authorization	only mode (no common password configuration required)
VPN3K Compatibility (Option 🗧
	DK Cancel Help

Select the newly created server group in the top box, and click the Add button highlighted below to add a new server to this group.

File	View Tools Wizards Window Help							Type topic to search	h Go	- alada
<u>ا</u> ا	ome 🇠 Configuration 📝 Monitoring 🔚 Save 🔇	Refresh 🔇 Back 🤇	Forward 💡 F	ielp						cisco
	Remote Access VPN ASDM Assistant	onfiguration > Remo	te Access VPN > #	AA/Local Users	> AAA Server Grou	uns				
kmarks	emote Access VPN 급 무	AAA Server Groups								
8	2 Introduction	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts			Add
	Clientless SSI VPN Access	2FARAD	RADIUS	Single	Depletion	10	3			
	AAA/Local Users	LOCAL	LOCAL							Edit
	AAA Server Groups	RALDAP	LDAP		Depletion	10	3			Delete
	🎥 LDAP Attribute Map									
	MDM Proxy	Find:		Match Case						
E P	- A Secure Deskton Manager									
8	🔁 Certificate Management	Servers in the Selected	Group							
	🔯 Language Localization									
	P Load Balancing	Server Name or IP Ad	aress internace	Timeout						A00
	B DNS									Edit
	Advanced									
	~									L Delece
										Move Up
1	Device Setup									
	8									MOVE DOWN
	13 ritewal									Test
1	Remote Access VPN									
		Find:		Match Case						
	Site-to-Site VPN		, , ,							
	Device Management	LDAP Attribute Map								×
	»				Ap	oply	Reset			
Device	configuration refreshed successfully.					tisoadmin	15 🌐	i 🕼 🍰 📊	Ê	20/06/19 13:44:16 UTC

In the pop up window, set the following.

- 1. Interface Name the interface facing your TOTPRadius Server, usually INSIDE
- 2. Server Name or IP Address the DNS name or IP address of the TOTPRadius Server.
- 3. Server Authentication Port Change this to 1812.
- 4. Server Secret Key This is the Radius Secret from step 5 of the first part of this document.

Once this is complete, hit OK.

rational Server	×
Server Group: 2F	ARAD
Interface Name:	NSIDE
Server Name or IP Address:	
Timocutu	10 cocondo
Inneout.	To seconds
RADIUS Parameters	
Server Authentication Port:	1812
Server Accounting Port:	1646
Retry Interval:	10 seconds
Server Secret Kev	****
Conversion December	
Common Password:	
ACL Netmask Convert:	Standard
Microsoft CHAPv2 Capable:	
SDI Messages	
Massages	
Message Name	
ready-ror-sys-pin	ACCEPT A SYSTEM GENERATED PIN
next-code	Enter Next PASSCODE
new-pin-req	Diagona your new Alpha-Numerical
new-pin-sup	Please remember your new PIN
new-pin-reenter	New DIN Accepted
new-pin-sys-uk	Do you want to enter your own sin
Inew-pin-meur	Do you want to enter your own pin
(Double-click in a text cell t	o make changes.)
Restore	default message texts
ОК	Cancel Help

So long as you have at least one user enrolled in TOTPRadius Server, you should then be able to hit the Test button to the right of the screen and the below window will appear. Select Authentication, and enter the windows domain username of an enrolled user, and the current TOTP code for that user. This test should come back successfully.

📻 Test AAA Server - 10	×
To test the following AAA server, enter password.	r a username and
AAA Server Group: 2FARAD (RADIUS)	
Host: 1	
C Authorization Authentication	
Username:	
Password:	
OK Car	ncel
📻 Information	×
Authentication test to h	iost 10, is successful.
	OK

We are now going to add a second AAA server group to the ASA. Once again, select the Add button beside the top block, as below.

File	View Tools Wizards Window Help						Тур	e topic to search Go	la la .
	Home 🗞 Configuration 🔯 Monitoring 🔚 Save 🔇 I	tefresh 🔇 Back 🤇	Forward ?	Help					cisco
- -	Remote Access VPN 리 무 🔤	onfiguration > Remo	te Access VPN >	AAA/Local Users	AAA Server Gro	ups			
mark	2 Introduction	AAA Server Groups							
Sook	Network (Client) Access	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts		Add
	AnyConnect Connection Profiles	2FARAD	RADIUS	Single	Depletion	10	3		
_	Resources	LOCAL	LOCAL						Edit
									Delete
	Customized Installer Transforms								
	Localized Installer Transforms								
	AnyConnect Client Software								
	Group Policies	,							
	IPsec(IKEv1) Connection Profiles	Find:	\bigcirc \bigcirc	Match Case					
	IPsec(IKEv2) Connection Profiles								
		Servers in the Selected	Group						
	H- 🛃 Advanced	Server Name or IP Ac	dress Interfac	te Timeout					Add
	Clientless SSL VPN Access								Edit
	AAA/Local Users								
	2 LDAP Attribute Map							_	Delete
									Move Up
	Local Users								Maura Daura
								-	Move Down
									Test
	Language Localization								
	A Device Setup								
	Firewall								
	Remote Access VPN								
	Site-to-Site VPN	Find:	\odot	🥅 Match Case					
	Device Management	LDAP Attribute Map							×
	×3				Ap	oply	Reset		

In the next windows, give the server group an appropriate name and select protocol LDAP, then hit OK.

🧱 Add AAA Server 🕯	Group 🔀
AAA Server Group:	RALDAP
Protocol:	LDAP 🔽
Reactivation Mode:	• Depletion • Timed
Dead Time:	10 minutes
Max Failed Attempts:	3
	OK Cancel Help

Select the newly created server group and click Add to add a server to this group.

File	View Tools Wizards Window Help							Type topic to search Go	a harden
<u>ا</u>	Home 🍓 Configuration 🔯 Monitoring 🔚 Save 🔇	Refresh 🔇 Back 🤇	Forward	Help					CISCO
F	Remote Access ¥PN 리 무	Configuration > Remo	te Access VPN >	AAA/Local Users	> AAA Server Grou	IDS			
꽃 🗖	A Taken di settera								
ğ.	Introduction	AAA Server Groups							
8	Access	Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts		Add
	AnyConnect Customization / ocalization	2EARAD	RADIUS	Single	Depletion	10	3		
	Resources	LOCAL	LOCAL						Edit
	Binary	RALDAP	LDAP		Depletion	10	3		
	Script						-		Delete
	GUI Text and Messages								
	- 📆 Customized Installer Transforms								
	AnyConnect Client Profile								
	AnyConnect Client Software								
	Crown Delivies								
	TRee(IVEv1) Connection Profiles	Find:		Match Case					
	IPsec(IKEv2) Connection Profiles								
	Secure Mobility Solution	Sorvers in the Selected	Croup						
	🕀 🦣 Address Assignment	Jei vers in the Deletted	aroop						
	🕀 🗒 Advanced	Server Name or IP Ad	dress Interfa	ce Timeout					Add
	E - Clientless SSL VPN Access								Edit
	AAA/Local Users								
	AAA Server Groups								Delete
	LDAP Attribute Map								
									Move Up
	Secure Deskton Manager								Move Down
	Bi Host Scan Image								
	Tertificate Management								Test
	Anguage Localization								
	0								
	Bevice Setup								
	Erewall								
H									
	Remote Access VPN			_					
	Site-to-Site VPN	Find:	\bigcirc \bigcirc	Match Case					
	Device Management	LDAP Attribute Map							×
	» *				Ap	oply	Reset		

In the windows that pops up set

- 1. Interface name select the interface facing your Active Directory DC
- 2. Server name or IP Address The IP or FQDN of your DC
- 3. Server Type Microsoft
- 4. Base DN DN for LDAP to search, in this instance the DN of the entire domain, DC=*MyDomain*, DC=COM.
- 5. Scope All levels beneath the Base DN.
- 6. Naming Attribute samaccountname
- 7. Login DN the DN of an account with appropriate permission to query active directory.
- 8. Login Password the password of the above account.

🧱 Edit AAA Server	×
Server Group:	RALDAP
Interface Name:	INSIDE
Server Name or IP Address	
Timeout:	10 seconds
LDAP Parameters for autho	entication/authorization
🔲 Enable LDAP over SS	5L
Server Port:	389
Server Type:	Microsoft
Base DN:	DC=
Scope:	All levels beneath the Base DN 💌
Naming Attribute:	samaccountname
Login DN:	cn=(,ou=(),ou=(),dc=(),dc=()
Login Password:	*****
LDAP Attribute Map:	None
🔲 SASL MD5 authentica	ation
🔲 SASL Kerberos authe	entication
LDAD Deverseberg for Crow	
Group Base DN:	
Group Search Timeout:	10
	OK Cancel Help

You should now have 2 separate server groups set up. We now need to add these to your Anyconnect Connection Profile. In ASDM, browse to Configuration > Remote Access VPN > Anyconnect Connection profile. Select your VPN Connection Profile in the Connection Profiles block at the bottom of this screen and click Edit, as highlighted below.

me 🧭 Configuration 🔗 Monitoring 🔚 Sav	ave 🔇 Refresh 🔇 Back 🤅	Forward 🦻 Hel	P				CIS
mote Access VPN	A Configuration > Remo	te Access VPN > Nel	work (Flient) Acce	s > AnyConnect Co	nnection Profiles		
Network (Client) Access	The security appliance	automatically deploys t	he Cisco AnyConnect	PN Client to remote us	ers upon connection. The	initial client deployment requires e	nd-user administrative rights.
AnyConnect Connection Profiles	Cisco AnyConnect VPN	Client supports IPsec (IKEv2) tunnel as well a	s SSL tunnel with Data	gram Transport Layer Sec	urity (DTLS) tunneling options.	
🕀 📆 AnyConnect Customization/Localization	Access Interfaces						
- 🌆 AnyConnect Client Profile	Fnable Cisco AnvC	oppect VPN Cliept acces	ss on the interfaces se	ected in the table belo			
- 🌆 AnyConnect Client Software	i cidolo cisco rity c	Simple Yin Cabin dece.	so on the incontaces so				
Dynamic Access Policies	SSL access must be en	abled if you allow AnyC	onnect client to be lau	nched from a browser ((Web Launch) .		
IPser(IKEv1) Connection Profiles	Interface	SSL Ac	cess	IPsec	(IKEv2) Access		
IPsec(IKEv2) Connection Profiles		Allow Access	Enable DTLS	Allow Access	Enable Client Servic	es Device Certificate	
- 🐻 Secure Mobility Solution	INSIDE						
🗄 🎭 Address Assignment	OUTSIDE		•	v	v	Port Settings	
🕀 🐻 Advanced							
Clientless SSL VPN Access							
AAA/Local Users Socium Dockton Manager	IV Bypass interrace a	ccess lists for indound \	PIN sessions				
Certificate Management	Access lists from group	policy and user policy a	always apply to the tra	ffic.			
Anguage Localization	Login Page Setting						
Load Balancing	Login Page Setting						
P DHCP Server	Allow user to select	connection profile on I	the login page. 🕤				
R DNS	Sbutdown portal lo	gin page.					
	1 pridedorini por cario						
🐯 Advanced							
🐯 Advanced	Connection Profiles						
🚳 Advanced	Connection Profiles	nnel group) specifies ha	w user is authenticate	d and other parameter:	s. You can configure the n	apping from certificate to connect	ion profile <u>here</u> ,
평 Advanced	Connection Profiles	nnel group) specifies ha	w user is authenticate	and other parameters	s. You can configure the n	apping from certificate to connect	ion profile <u>here</u> ,
3 Advanced	Connection Profiles	nnel group) specifies ha	w user is authenticate	d and other parameters	s. You can configure the n Case	apping from certificate to connect	ion profile <u>here</u> ,
Advanced	Connection Profiles Connection profile (tur Add C total	nnel group) specifies ha Delete Find: Find: SSL Enabled	w user is authenticate	d and other parameter:	s. You can configure the n Case Aliases	apping from certificate to connect Authentication Method	ion profile <u>here</u> , Group Policy
Advanced	Connection Profiles — Connection profile (tu	nnel group) specifies ha Delete Find: SSL Enabled	w user is authenticate	d and other parameters	s. You can configure the n Case Aliases AA	apping from certificate to connect Authentication Method 4(LOCAL)	ion profile <u>here</u> , Group Policy DftGrpPolicy
∰ Advanced 	Connection Profiles Connection profile (tu de Add 22 Edg Name DefaultRAGroup DefaultWEBVPNGroup	Delete Find:	w user is authenticate	d and other parameters	s. You can configure the n Case Aliases AA AA AA	Authentication Method Authentication Method A(LOCAL) A(LOCAL)	ion profile <u>here</u> , Group Policy DftGrpPolicy DftGrpPolicy
∰ Advanced 	Connection Profiles Connection Profile (tu Connection profile (tu Connection Profile Connection Profile Connection Profile Name DefaultRAGroup DefaultWEBVPNGroup VPNUsers2FA	nnel group) specifies ha Delete Find: SSL Enablea V	w user is authenticate	d and other parameters	s. You can configure the n Tase Aliases AA AA AA	Authentication Method Authentication Method A(LOCAL) A(LOCAL) A(RALDAP)	ion profile <u>here</u> , Group Policy DftGrpPolicy DftGrpPolicy NOACCESS
Advanced Device Setup Firewall Remote Access VPN	Connection Profiles Connection profile (tu the Add Car Edit Name DefaultRAGroup DefaultRAGroup DefaultRAGroup	nnel group) specifies ha Delete Find: SSL Enabled	w user is authenticate	d and other parameters Match C ac Enabled C	s. You can configure the n Case Aliases AA AA AA	Authentication Method Authentication Method A(LOCAL) A(RALDAP)	Group Policy OftGrpPolicy DftGrpPolicy DftGrpPolicy NOACCESS
Device Setup Firewall Remote Access VPN Site-to-Site VPN	Connection Profiles Connection Profile (tur Add 27 Edg DefaultRAGroup DefaultRAGroup DefaultRAGroup VPNUsers2FA	Inel group) specifies ha	w user is authenticate	d and other parameters	s. You can configure the n Case Aliases A AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	Authentication Method Authentication Method A(LOCAL) A(RALDAP)	ion profile <u>here</u> , Group Policy DfRGrpPolicy DfRGrpPolicy NOACCESS
Device Setup Firewall Sete-to-Site VPN Device Management	Connection Profiles Connection profile (tu Connection profile (tu Connection profile (tu Connection profile (tu Cannection Profiles) Name DefaultRAGroup DefaultRAGroup DefaultRAGroup DefaultRAGroup DefaultRAGroup DefaultRAGroup DefaultRAGroup DefaultRAGroup DefaultRAGroup DefaultRAGroup DefaultRAGroup	nnel group) specifies ha Delete Find: SSL Enablec	w user is authenticate	d and other parameters	s. You can configure the n Case Aliases A ANA AA AA AA AA AA	Authentication Method Authentication Method A(LOCAL) A(RALDAP) the connection profile that matche	ion profile <u>here</u> , Group Policy DfKsrpPolicy DfKsrpPolicy NOACCESS
Device Setup Firewall Ste-to-Site VPN Device Management	Connection Profiles Connection profile (tu Connection profile (tu Connection profile (tu Connection profile (tu Connection Profiles Name DefaultRAGroup DefaultRAGroup DefaultWEBVPNGroup VPNUsers2FA	nnel group) specifies ha Delete Find: SSL Enabled SSL Enabled Procedence if group U	w user is authenticate	d and other parameters Image: match of the second secon	s. You can configure the n Tase Allases AA AA AA AA Con profiles. Otherwise,	Authentication Method Authentication Method A(LOCAL) A(LOCAL) A(RALDAP) the connection profile that matche	ion profile <u>here</u> , Group Policy DfKgrpPolicy DfKgrpPolicy NOACCESS

In the Basic section of the window that pops up, where highlighted below select the AAA Server Group you created to perform LDAP authentication against your AD DC.

🧱 Edit AnyConnect Connect	ion Profile: ¥PNUsers2FA		×
Basic	Name:	VPNUsers2FA	
⊡⊶Advanced	Aliases:		
	Authentication		
	Method:		
	AAA Server Group:		Mapage
			Hanagerri
		J Use LOCAL IF Server Group Fails	
	SAML Identity Provider —		
	SAML Server :	None	Manage
	Client Address Assignment -		
	DHCP Servers:		
		None C DHCP Link C DHCP Subnet	
	Client Address Pools:		Select
	Client IPv6 Address Pools:		Select
	Default Course Dellas		
	Group Policy		Mapage
	(Following fields are linked	to attribute of the group policy selected above)	Managerri
	Enable SSL VPN clier	nt protocol	
	Epable IDser(IKEv2)		
	UND Servers:		
	Demois Nervers:		
Find:	🔘 Ne	ext 🔘 Previous	
		Capcel Help	
	OK		

Now navigate to Advanced > Secondary Authentication. Set the server group to the AAA Server you created to authenticate against TOTPRadius Server. Be sure to also tick Use Primary Username, this will ensure users are presented with a single username field, one password field for their AD password and a second password field for their TOTP code.

🧱 Edit AnyConnect Connecti	on Profile: VPNUsers2Fa	4		×		
Basic	Secondary Authentication	Server Group				
-Advanced	Server Group:	2FARAD		Manage		
General Cliept Addressing						
Client Addressing Authentication		Use LOCAL if Ser	Use LOCAL if Server Group fails			
Secondary Authenticat		🔽 Use primary user	Vise primary username (Hide secondary username on login page)			
Authorization	Attributes Server:	Primary C Secondary				
Group Alias/Group URL	Session Username Serv	er: 📀 Primary 🔿 Sec	ondary			
	Interface-Specific Secondary Authentication Server Groups					
	Add Edit Delete					
	Interface	Server Group	Fallback to LOCAL	Use primary username		
	Viserpame Mapping from Certificate					
	Pre-fill username from certificate					
	☐ Hide username from end user					
	Fallback when a certificate is unavailable					
	Specify the certificate fields to be used as the username					
	Primary Field:	N (Common Name)	~			
	Secondary Field:)U (Organization Unit)	V			
	C Use the entire DN a	s the username				
	C Use script to select	username				
	J None	Add	Edit Delete			
Find:	,	Next 🙆 Previous				
		OK Cancel	Help			

Once applied to the ASA, Anyconnect connection attempts should present a password window similar to the below.

🕥 Cisc	o AnyConnect	×			
	Please enter your username and password.				
_	Group:				
	Windows Username:				
	Windows Password:				
	Authenticator Code:				
	OK Cancel				

Optional

It is possible to customise the text fields presented to users by the Anyconnect client, e.g. to display the "Password" label to show as "Windows Password" as in the above screenshot. This is controlled in Configuration > Remote Access VPN > Anyconnect Customization/Localization > GUI Text and Messages. Edit an existing translation table or add a new one. Within the text of the window that pops up, find the line with msgid "Password" and change the corresponding msgstr to "Authenticator Code" or similar suitable description. Due to the volume of text here, you may find it easier to copy this text to a text editor, use CTRL+F to find and the msgid and make the changes, and then copy/paste it back into ASDM.

