Cisco MFA access with Microsoft NPS Radius and Pragma FortressCL

Author: Pragma Systems, Inc. www.pragmasys.com December 11, 2023

Accessing Cisco switches, routers and network devices using multi-factor authentication (MFA) with x509 smart cards (Govt issued CAC/PIV cards or Yubi keys or Microsoft Active Directory certificate server issued cards), instead of password, is a critical infrastructure protection mandate of government and secure enterprises. Cisco ISE 2.0 or above or Windows Server Network Policy Server (NPS) Radius can be used for AAA in Domain account logon with passwords or MFA. However, installation and configuring these elements are complex and many organizations needed help as Pragma is a primary provider of the ssh client side of the solution. Setup using Cisco ISE as AAA is described in a Cisco Pragma jointly published white paper <u>https://www.pragmasys.com/products/support/cisco-2-factor</u>. This document lists the steps needed to setup MFA using Microsoft NPS and Active Directory as the AAA.

SSH Access with DoD CAC/PIV/Smartcards



Task 1: RFC 6187 compliant SSH clients are needed. Download and install Pragma Fortress ClientSuite in a Windows computer <u>https://www.pragmasys.com/ssh-client/download</u>. It can run on any Windows OS (Windows 10/11/8.1 or Windows Server 2022/2019/2016/2012R2). Pragma Fortress ClientSuite provides an RFC 6187 compliant MFA client and is also Cisco certified & recommended. Run "FortressCL" in the start menu or in a command line to start Pragma ssh gui client. Select "Connect" button and choose +sign to define the target site (your cisco device) as shown in the figures. Name the site in "sitename" and "Host address" should be the name or ip address and fill in Authentication info.

e Edit View Option	s Help						5. Q	
innect Disconnect Co	onen.Witzerd New Windo	w Trace Window	StatusBar	Tri Preferences	al Font C	olor	About	0
								Wining Security
								Smart Card Peace enter your PNL
								E In
								Chief have for yours advantation
		X.509-RSA	sub2:AES-2	56 CTR 1.11	103x2	4		Cit has be need allowater
		X.508-R5A	ssh2-AES-2	56 CTR 1,13	103x2	4		Cit has be need allowed an
avoger		X.509-R5A	ssh2:AES-2	56 CTR 1,13	103x2 Ste Mana	ge .		Crist terre for verify sitemation
noge cenctoon Authentication	CL_clsco2901	X.504-R5A	seh2:AES-2	56 CTR 1,13	103x2 Ste Maria ⊟-CL_0	ge sco2901 the Us		Cit for the set of sealer Const
neger Authoritization Logging Kaybeard Pray	CL_clsco2901 Sie gene Hot addess	X.508-RSA	sah2AES-2	56 CTR 1,13	103x3 Ste Mana B-CL 0 - Lo - Lo - Lo - Lo	ge sco2901 stratic sigging sybcard rowy		Cite here he rest showader Conset Conset Conse
noger Lonzbold Logging Kaybaard Proxy Serial Telvel	CL_cisco2901 Sile game giort actions Hast gives	X.509-RSA [CL_cmos2501 [mmo2201	seh2:AES-2	56 CTR 1,13	103x2 Site Mana B-CL o Lo Ki S S To To To	4 ges sco2901 sco2901 statistics sogging sigging sigging sigging sigging sigging sigging sigging sigging sigging sigging sigging sigging soggi	ilian j	City have for york advantation City City Constant Authentication Unable Copulation from smart card on City City City City City City City City
noger Authenticelien Loging Keyband Proxy Serial Tehret Terminal Soh Window	CL_cisco2901 Sile gare got addess Host gare Potessi Pot	X.508-RSA [CL_eneo2501 [meo2501 [meo2501	suh2AES-2	56 CTR 1,13	103x2 Ste Mana B CL o K K P K S S S S W W	ges sco2901 chrokter soging sybseed roxy stal frost sominal ch findow sco2	liten	Contract strengther sets strengther Contract Strengther Authentication Unerld Frequilled from smart cardino If the Arrow Danam (FRACEWARYS Fit Unerld From SC - Mage (Frances Harris Fit Unerld From SC - Mage (Frances Harris Fit Unerld From SC - Mage (Frances Harris Fit Unerld From SC - Mage (Frances Harris) Fit Unerld From SC - Mage (Frances Harris) Fit Unerld From SC - Mage (Frances Harris)
anoger Authentication Logipaq Oogbeard Proxy Setial Terminal Sofi Window castil 1900	CL_cdsco2901 Sile gare: igot addess Hoat glass Podessi Figt	X.509-RSA CL_cmoo2501 5mm2201 5mm2201 222	seh2:AES-2	56 CTR 1,13	103x2 Ste Mara B CL o K K K K K K K K K K K K K K K K K K K	90 sco2901 streating syboard roxy sial frost cominal th indow psis2 00	ban	Cite two for vert advanator Cite two for vert advanator Authentification Userie: [repulsed from meet card/or Fit data from SC - Mag: [FitneDail Nerve Fit Userie from SC - Mag: [FitneDail Nerve]]
noger Authentication Legging Koyband Proxy Seial Tehret Terminal Soh Window casis2 1000	CL_clisco2901 Sile game Host addess Host addess Potessi Pgt Connent	X.508-RSA CL_caeco2501 [meco2501 [meco2501 [meco2501 [meco2501 [meco2501] [meco2501	seh2:AES-2	56 CTR 1,13	103x2 Ste Mana B CL 0 K K P K K K K K K K K K K K K K K K K	4 ge ccc2901 cftreduc sgarg sgarg sgarg sgarg sgarg sgarg sgarg stat the the cov stat the cov stat the cov stat the cov sgarg stat the cov sgarg sgarg stat the cov sgarg sgarg stat the cov sgarg sgarg stat the cov sgarg stat the cov sgarg stat the cov sgarg stat the cov stat the the cov stat the the cov stat the cov stat the the cov statt the cov statt the cov statthe the the the the the the the the the	ben	Continentication Conti
anoges Authentication Logging Rogboard Poiny Selid Teinet Terminal Shi Shi Shi Shi Shi Shi Shi Shi Shi Shi	CL_cisco2901 Sile game Hoat addees Hoat addees Postcool Pgt	X.509-RSA	seh2:AES-2	56 CTR 1,13	103x2 Ste Mona ⇒ CL o - U - U - U - U - U - U - U - U	4 get 202201 Greeting signing signing sing trivet sing trivet sing the sing trivet trivet sing trivet trivet sing trivet tri trivet trivet	lan	Cite tere for verification Case C
anoges - Authensication - Logging - Roybeand - Proxy - Serial - Ternet - Terninal - Sch - Window L, cesis2 ur1000	CL_cisco2901 Sile game Host addess Host game Potersil Pgt	X.509-RSA	seh2:AES-2	56 CTR 1,13	103x2 Ste Mona B CL o K K R R R R R R R R R R R R R R R R R	4 90 sco2901 sco2901 signed signed wither troy shat inter sources inter sources of sources sources of sources	lion i	City has been be needed addressed and addressed address

Task 2: Configure your Cisco device to allow MFA authentication following the steps listed in Cisco & Pragma white paper <u>https://www.pragmasys.com/products/support/cisco-2-factor</u>. You can avoid option 1 or option 2 steps in the white paper if you want to use Microsoft NPS Radius as your AAA. This document acts as your option 3 and lists the steps needed to configure Microsoft NPS Radius as your AAA since the white paper does not address it. MS NPS Radius is widely deployed by many sites already and can be configured to act as the AAA for sites which do not have access to Cisco ISE or other RADIUS+ server for AAA. So, we describe this option 3 in details below.

Task 3:

Option 1: Use Cisco ASA as your Radius AAA. Described in the Cisco Pragma white paper. Option 2: Use Cisco ISE or a TACACS+ server as your AAA. Described in the Cisco Pragma white paper. Option 3: Use MS NPS Radius as your AAA for MFA. Described in this document.

Step 1: If you have a Microsoft Network Policy Server (NPS) already, you can configure it for Cisco device MFA. If you do not have one, then install Microsoft NPS in a Windows Server 2022/2019/2016/2012R2 selecting "Microsoft Network Policy" role in your server role selection section.

Step 2: Define your Cisco device RADIUS link by right clicking "Radius Clients" in NPS and choosing "New". Then provide the IPv4 address of the Cisco device, a shared secret (any size string works), a friendly name for the link and choose "Cisco" as the Vendor name in "Advanced" tab.



Step 3: Define Connection Request Policy as shown in figures below

Conductors Properties Conductors Conductors Conductors Conductors								
NPS (Local) Contraction Request Policies If ADDUS Clients and Servers Fouriestics Request Policies If ADDUS Clients Fouriestics If ADDUS Clients Fouriestics Partice RADUS Server Group Fouriestics Conditions - If the following conditions are net: Conditions - If the following conditions are net: Conditions - If the following settings are applied: Setting - Then the following settings are applied: Settings - Then the following settings are applied: Setting - Then the following settings are applied: Settings - Then the following settings are applied: Setting - Then the following settings are applied: Settings - Then the following settings are applied: Setting - Then the following settings are applied: Settings - Then the following settings are applied: Setting - Then the following settings are applied: Settings - Then the following settings are applied: Setting - Then the following settings are applied: Settings - Then the following settings are applied: Setting - Then the following settings are applied: Policy State Fenabled NPS evaluates this policy while processing co	🔹 💼 🖬 📷							
PADDS Cleants and Servers ADDUS Cleants and Servers Padded Sciences Prevents RADDUS Servers Groups Price Vision Remote RADDUS Servers Connection request publics Remote RADDUS Servers Price Vision Connection request publics Connection request publics Remote RADDUS Servers Price Vision Connection request publics Connectin Connection request public Connection Connectin Co	NPS (Local)	Connection Request Policies						
Point Processing Driver Secure Processing Driver Busked 1 Unspecified Processing Driver Discrete Busked 1 Unspecified Processing Driver Discrete Busked 1 Unspecified Conditions - If the following conditions are met: Conditions - If the following conditions are met: Conditions - If the following conditions are met: Conditions - Settings Settings - Then the following conditions are met: Conditions - Settings Policy State If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy State If enabled Network access server that sends the connection request to NPS. You can select either the network access server type or Vendo's specific, but nether is required. If your network access server is an 802 1X authenticating switch or wireless access point, select Unspecified Of Type of network access server: Unspecified Unspecified Image:	RADUS Clients and Servers RADUS Clients Remote RADUS Server Groups	Connection request policies allow you to designate whether connection requests are processed locally or forward to resiste RADUS servers.						
Conditions - If the following conditions are net: Condition Value Settings - Then the following untings are asplied: scoAccess Properties Xverview Conditions Settings Policy name: DiscoAccess Policy state If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy enabled Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific. Unspecified v O Type of network access server: Unspecified Vendor specific: v Image: The other is required. To your network access server is an BIQ2.1X authenticating switch or wireless access point, select Unspecified	Connection Request Policies Network Policies Accounting Templates Management	Policy Name Status Processing Order Source Disco/scores Use Windows authentication for all users Enabled 5939399 Unspecified						
Candition Value Setings - Then the fallowing setings are asplied. scoAccess Properties Second Constraints Verview Conditions Setings - Then the fallowing setings are asplied. scoAccess Properties Verview Conditions Setings Policy name: CiscoAccess Policy State F if enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy enabled Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but nether is required. If your network access server is an 802-11X authenticating switch or wireless access point. either Unspecified. ✓ Oracle Time ✓ Unspecified. ✓		Conditions - If the following conditions are met:						
Setings - Then the following setings are asplied:		Candition Value						
scoAccess Properties verview Conditions Settings Policy name: CiscoAccess Policy State If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy enabled Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type of Vendor specific, but neither is required. If your network access server is an 802-1X authenticating switch or wireless access point, select Unspecified Vendor specific: 10		Setings - Then the following settings are applied	_					
scoAccess Properties verview Conditions Settings Policy name: Policy State If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy. Policy enabled Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type of Vendor specific, but nether is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified Vendor specific: 10		le III						
Network connection method Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific: 10 •	Policy name:	coAccess						
Unspecified ~ Vendor specific: 10 \$	Policy name:	coAccess						
O Vendor specific:	Policy name: Policy State If enabled, NPS evaluates this policy Policy enabled Policy enabled Network connection method Select the type of network access stype or Vendor specific, but nether select Unspecified. © Type of network access server:	coAccess by while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless acces	ever ss point,					
10 🌻	Policy name: Policy State If enabled, NPS evaluates this polic Policy enabled Policy enabled Network connection method Select the type of network access is type or Vendor specific, but nether select Unspecified. Type of network access server: Unspecified	coAccess cy while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless access V	erver ss point,					
	Policy name: Policy State If enabled, NPS evaluates this polic Policy enabled Network connection method Select the type of network access s type or Vendor specific, but nether select Unspecified. Unspecified Vendor specific:	coAccess cy while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless access	rver ss point,					
	Policy name: Policy state If enabled, NPS evaluates this polic Policy enabled Network connection method Select the type of network access stype or Vendor specific, but nether select Unspecified. Type of network access server: Unspecified Vendor specific: 10	coAccess cy while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless access	erver ss point,					
	Policy name: Policy State If enabled, NPS evaluates this polic Policy enabled Network connection method Select the type of network access type or Vendor specific, but nether select Unspecified ↓ Vendor specific: 10	coAccess cy while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless access	rver ss point,					
	Policy name: Policy State If enabled, NPS evaluates this polic Policy enabled Network connection method Select the type of network access s type or Vendor specific, but nether select Unspecified Unspecified Vendor specific: 10 €	coAccess cy while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless access	rver ss point,					
	Policy name: Policy State If enabled, NPS evaluates this polic Policy enabled Network connection method Select the type of network access is type or Vendor specific, but nether select Unspecified. ● Type of network access server: Unspecified ○ Vendor specific: 10	coAccess by while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless access	ever ss point,					
	Policy name: Policy State If enabled, NPS evaluates this polic Policy enabled Network connection method Select the type of network access s type or Vendor specific, but nether select Unspecified ↓Unspecified ↓Unspecified ↓Unspecific: 10 ‡	coAccess cy while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless accer	rver ss point,					
	Policy name: Policy State If enabled, NPS evaluates this polic Policy enabled Network connection method Select the type of network access server: Unspecified Vendor specific: 10 ↓	coAccess by while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless access	nver ss point,					
	Policy name: Policy State If enabled, NPS evaluates this polic Policy enabled Network connection method Select the type of network access stype or Vendor specific, but nether select Unspecified ● Type of network access server: Unspecified ● Vendor specific: 10	coAccess cy while processing connection requests. If disabled, NPS does not evalue this policy. server that sends the connection request to NPS. You can select either the network access se is required. If your network access server is an 802.1X authenticating switch or wireless acces	rver ss point.					

the second term for t		
ringure the control is the	THE NEW WE DOLL	Control of
conditions match the corm mection request, NPS sk	rection request. NPS uses this policy to authorate the connection request, it conditions do not nee gos this policy and evaluates other policies, if additional policies are configured.	ish the
Condition	Value	1.1
Clerk Friendly Name	casos 1921_2	
	Client Friendly Name ×	
	Specify the hierdy name of the RADIUS client. You can use pattern matching	
	nyrtan	
	1000 1000 C	
	OK Cancel	
	Contraction of Contractions	
	NG08	Parcove
	OK Caro	al buly
coAccess Properties		_
coAccess Properties erview Conditions Sett	inge	_
coAccess Properties erview Conditions Bett ordinate the actions for the	tinge ar nativank solice	
coAccess Properties erview Conditions Set ordigue the settings for the conditions and constraints	trige in nativeric policy, in match the curvinction request and the policy grants access, sattings are applied.	
coAccess Properties erview Conditions Sett orfigure the settings for the conditions and constraints ettings	inge en nativerk policy i match the connection insparet and the policy grants access, sattings are applied.	
coAccess Properties ervice Conditions Bett andgue the settings fur th conditions and constraints ettings: Require of Authentication Wetthoch	inge in nativerk, policy in match the connection request and the policy grants access, sattings are applied.	vende
coAccess Properties erview Conditions Bett artigue the settings for the conditions and constraints ettings: Required Authentication Methods and Authentication Methods	tings in nativerk, policy instatch the commedian request and the policy grants access, settings are applied. Specify whether commedian requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication.	rende
coAccess Properties erview Conditions Bett artigue the settings for the conditions and constraints ettings: Required Authentication Methods	trige in nativerk, policy instatch the commedian request and the policy grants access, settings are applied. Specify whether commedian requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication ods	rende
coAccess Properties erview Conditions Bett artigue the settings for the conditions and constraints ettings: Required Authentication Methods Arthemicration Methods Forwarding Connection Required	tings in nativerk policy insists the commedian insuest and the policy grants access, settings are applied. Specify whether connection insuests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication. (Authenticate inspects on this server Connect insuests to the following model RADIUS server on on the authentication.	rende
coAccess Properties erview Conditions Bett artigue the settings for the conditions and constraints ettings: Required Authentication Methods Authentication Methods Required Required Constraints Authentications	Inge in nativerk policy insiste the commedian insuest and the policy grants access, settings are applied. Specify whether connection insuests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication RADIUS servers for authentication, or are accepted without authentication Authenticate inspects on this server Forward inspects to the following remains RADIUS server group for authentication	rembe
coAccess Properties erview Conditions Bett andgue the settings for the conditions and constraints ettings: Required Authentication Methods	Inge in nativerk policy insiste the connection requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication Authenticate requests to the following remain RADIUS server group for authenti- Forward requests to the following remain RADIUS server group for authenti- initiat serving remains to the following remain RADIUS server group for authenti- initiat serving remains to the following remains RADIUS server group for authenti- initiat serving remains to the following remains RADIUS server group for authenti- initiat serving remains to the following remains the fol	rende hodsry:
coAccess Properties erview Conditions Bett artigue the settings for the conditions and constraints ettings: Required Authentication Methods	Inge a network poky in insish the connection requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication Authenticate requests in the server Forward requests to the following results RADIUS server group for authenti- instanting preside	rende hodsry
coAccess Properties erview Conditions Bett arbyze the settings for th conditions and constraints ettings: Required Authentication Methods	Inge a network policy an instant free connection requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication Prover for authentication the server Prover requests to the following results RADIUS server group for authenti- instanting precision Prover requests to the following results RADIUS server group for authent (instanting precision) Prover requests to the following results are provided and the following condectuals Proved and the server of the following condectuals Proved and the server of the following condectuals	rende hoder;
coAccess Properties erview Conditions Bett arbyze the settings for the conditions and constraints ettings: Required Authentication Methods	Inge a network policy an instant free connection requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication Authenticate requests to the following render RADIUS server group for authenti- Forward requests to the following render RADIUS server group for authenti- instanting policy Accept users without volidating credentials	rende hoder:
CoAccess Properties erview Conditions Bett antigue the settings for the conditions and constraints ettings: Require at Authentication Methods Antibertication Meth Forwarding Connection Required Authentication Activities anti- accounting Specify a Realm Name Activities Antibula RADIBIS Antibulas RADIBIS Antibulas (Contaction)	Inge a network policy an instant fre connection requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication Authenticate requests on this server Forward requests to the following renable RADIUS server group for authenti- initial configuration Accept users without validating credentials	rende hoder:
CoAccess Properties erview Conditions Sett artigue the settings for the conditions and constraints ettings: Require of Authentication Authentication Method Authentication Method Authentication Method Authentication	Inge a network poky an instant fre connection request and the poky guints access, settings are applied. Specify whether connection requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication. Authenticate requests to the following render RADIUS server group for authenti- initial configuration Accept users without validating credentials	rende halter:
coAccess Properties erview Conditions Bett antigue the settings for the conditions and constraints ettings: Required Authentication Methods Activetication Metho Forwarding Connection Required Activetication Activeticatio Activetication Activetication Activetica	Inge Ingel Instatch file contraction request and the policy gunts access, settings are applied.	rende todor:
CoAccess Properties erview Conditions Bett antigue the settings for the conditions and constraints ettings: Required Authentication Methods Activetication Metho Forwarding Connection Required Activetication Activeticatio Activetication Activetication Activetica	Inge an network policy an attempt policy gunts access, settings are applied. Specify whether connection requests are processed locally, are forwarded to RADIUS servers for authentication, or are accepted without authentication. Authenticate requests to the following results RADIUS server group for authenti- ient configuration Accept users without validating credientals	rembe hoating
Conductess Properties erview Conditions Bett antigue the settings for the conditions and constraints ettings: Required Authentication Authentication Metho Forwarding Connection Required Authentication	Inge an intwork policy in statch the contraction request and the policy gunts access, settings are applied. Specify whether connection requests are processed locally, are forwarded to RADIUS servers for adheritation, or are accepted without adheritation. Adheritation requests on the server Forward requests to the following rende RADIUS server group for authorit initiation requests Accept users without validating credentiale Accept users without validating credentiale	rembe haditory
CoAccess Properties erview Conditions Bett antigue the settings for the socialisms and constraints ettings: Required Authentication Methods Activetication Metho Forwarding Connection Required Activetication Activeticatio Activetication Activetication Activetica	Inge an intwork policy in statch the contraction request and the policy gards access, settings are applied. Specify whether connection requests are processed locally, are forwarded to RADIUS servers for authentication, is are accepted without authentication. Authenticate requests on this server Forward requests to the following rende RADIUS server group for authent initiation requests Accept uses without validating credentials Accept uses without validating credentials	rembe haditry
CoAccess Properties erview Conditions Bett antigue the settings for the conditions and constraints ettings: Required Authentication Methods Authentication Metho Forwarding Connection Required Authentication Authorities Accounting Specify a Realm Name Accounting Specify a Realm Name Accounting Specify a Realm Name Accounting Specify a Realm Name Context of Specific Wordor Specific	Inge an network policy an active the contraction request and the policy grants access, settings are applied.	rembe haditry

Step 4: Define "Network Policies" for your AAA as below. Here we define two policies "CiscoPriv1" and "CiscoPriv15" to provide privilege level 1 and privilege level 15 access to two different sets of Active Directory Groups (NetworkOperators getting level 1 and NetworkAdmins getting level 15 access).

Alatuntek Ballou Taran			Ý
File Address Policy Server	2	- u	~
File Action View He	P		_
NPS (Local)	Network Policies		
RADIUS Clients	Annen Network policies allow you to designate who is authorated to connect to the network and server Groups which they can be cannot connect.	the discumitances un	der .
Policies			
Connection Regi	Jest Policies Policy Name Status Processing Order Access Type Source		_
Nocounting	Gsophw15 Enabled 2 Grant Access Unspecified		-
🖌 🐳 Templates Managen	sent		
	g CamPite1		
			- 12
	Canadiona - e ele relevent conadiona are nel		-
	Condition Value		
	Windows Groups PRAGMASYS/Jetwork/Operations Clarit Energity Name croco 1921 2		
	come i come presenta come i se cue		- 1
	secretar - then the topowing secretar are apprecia		
	15.8		10
accPriv1 Properties	×		
herves Canditors Carattante	Settigs		
Poles name	21		
Policy State			
Ferabled, NPS evaluates the p	day of the performing authorization. If it subject, NPS does not environment this policy.		
Palicy enabled			
Access Permanen			
R conditions and constraints of access, that is access	The network policy multil the connection request, the policy can either gravit access or deny		
1000 March and Allina	and the second		
Bawt access Grant access #	The connection request matches the policy.		
O Deny access. Deny access if	he connection request nationes the policy		
Fife correction request nation	pertex free the conditions and combinents of this nativole policy and the policy grants access, particles		
authentiation with mats-ook pub	co only, do not evaluate the dual in properties of user accounts.		
Network connection wethod Select the type of network acces or Vendor specific, but retifies to	in server that serves the connection request is 1975. This can select either the nativolv access server type required. Types retream access every a an OSC 1X admonstrating sector or winning access part,		
and the second			
Type of network access serv	e		
Unpedied	-		
With the			
10. 79.			
Section of the sectio			
Overview Conditions Constructo	(Satings		
Configure the conditions for the ne	inak palay. Sanat 1950 ani kanala kanala kanala kanala sanata sa kanala kanala sa kanala sa kanala sa kanala sa		
connection request. NPS slops the	mouses, or o uses no pace to advante the convertion region. In conditions do not matter the policy and evoluates ofter policies if additional policies are configured.		
	adapa Reseat		
Candidon We	belower services		
Clert Riesdy Name	pecify the group membership required to match this policy		
1	Groups		
	PRAGMASTS (JanvoinOperation)		
	atorie - estatemente (1524/152) D		
	Add Groups		
Condition description	Carcel		
The Westown Groups correlling	Jenos		
	Add. Edit Temove		
	DK Genee unt		
The second s			

		Charlen Augustan		
woftict Properties	x	Dversee Conditions Development		
ener Desition Containts 5	etrop :	Configure the settings for the nativox policy. If conditions and constraints reach the connection	must addepate onto post at a	e acchet.
adque the noninaria to the neuro	A parties	Setros		1797
all constraints are not matched by the	Connection request, retrict, access a densel.	RADUS Arteliant	Attribute Information	×
Constants		(Contract	arch to came	-
A Advanced House	Not still be to the card of Armitical solide Enter in the	Werdou Spicific	Service Type	
the Timetal	EVP types are regolized between IZPS and the shart to the only in which they are been	A. Multick and Sandroth	Alternation:	
R Called Tables D	EAP Type	Allocation Protocol (EAP)	Attribute format	-12
Des and line testrolians	[36436]	T P Figure	Grunaratur	
T SAL Post Type	26442645	A P Setton	Abbute Value Cricemonik-used for Dail-Ibi or VPN	
	Contraction descention of the local data	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	10000	
	Add.		Canveority used for 802 %	
	Percent Dropped Advertisation version 2 (45-CHUP v0)		iniai -	
	Dise the file of the second of the file of the second Disease Branges Advertuation (MSCANC)	1	#Ofer	
	The set they amond the (far mink)		100	THE PARTY INCOME
	Theroped attention PW. IFM	0		CRACK COMMENT
	Allow clentric convect schoul regitating at authentication method			
	.00 Canada State			OK Casol Luis
chist hapotes		× Vendor-Specific Attribut	te Information	×
ever Ceditore Committe	Settinge	Aurel		
ortigize the entirips for the network conditions and constraints match its	policy a convertion request and the policy grants access, lattings are applied.	Vendor Specific		
Scyle				
EADILIE M& Ender	To send additional attributes to RADLID classis, senior a Version Specific attribute, and	Specify network access se	arver vendor.	
a landa landa	and RR013 dem duperation for require an attracter. It is not service requires the	Salact from list	Creek	
Routing and Research Accord		Select from list:	CISCO	Y
All Multilett and Danshvidth Allocation Protocol (EAP)	Methods	O Enter Vendor Code:	0	0
T P Filters	Name Venille Value Venille Search RADUS Standard Reducted I			
G Groupine		Specify whether the attribu	te conforms to the RADIUS R	FC specification for
W is parted.		vendor specific attributes.		1
				ų
		Tes. it conforms		
	Add Ball Plancos	No. It does not conform	1	
		Configure Attribute		
	-11%		OK	Cancel
	Dit. Canad	100		
Vendor-Specific A	tribute Information X			
venuor-specific A				
Attribute name:	44			
Configure V	/SA (RFC Compliant)			
Spec				
Vendor-assig	ned attribute number:			
- I				
Attribute form	iat:			
String	v .			
vend	for			
Attribute valu	ie:			
Shell:priv-lvl	=1			
ON				
-	OK Cancel			
C				
	OK Creat			
	UK Lancel			

Step 5: Windows Server 2019 NPS has a bug of not opening ports properly in the Firewall. Run these commands in an admin level powershell cmd line session if your NPS is on Windows Server 2019:

\$Ports = 1812,1813,1645,1646

New-NetFirewallRule -DisplayName "NPS Allow inbound" -Direction inbound -LocalPort \$Ports -Protocol UDP -Action Allow

Step 6: We suggest these additional steps and guidelines for your remainder testing.

- 1. For just x509 login and no AAA, do not define any radius or ISE in your cisco devices (avoid option 1 or option 2 part in our Cisco Pragma white paper).
- 2. If Radius servers are used for AAA, Active Directory domain accounts with password can be authenticated and authorized for your Cisco devices. But for x509 card MFA (with CAC/PIV card or Yubi keys) login and AAA, the A/D account password must be "cisco" for the account. This is a limitation imposed by Cisco. To avoid it, use Cisco ISE instead of a Radius server as your AAA.
- 3. First try the Active Directory domain account with password to login to your Cisco device using FortressCL. If that succeeds, it means your NPS Radius is configured correctly for AAA and you can try the CAC/PIV card or Yubikey for MFA login to the Cisco device. Don't forget that your A/D password for the user account of the card must be "cisco". Change that if you want MFA for that account.
- 4. Issue the following command in your Cisco device to test radius AAA for a A/D user and password test aaa group radius domainname\\username password new-code
- 5. If you want to run Pragma's command line ssh client included in our Clientsuite, type "ssh -oSC=upn ciscodevipaddr" for MFA login or "ssh domain\username@ciscodevipaddr" for password login.
- 6. Windows Server Active Directory, Cisco ISE 2.0 or above (3.x works well) and Pragma FortressCL provides the best combination for a scalable multi-factor authentication (MFA) into all Cisco devices of an enterprise. Follow the steps listed in the Cisco Pragma white paper to configure your Cisco ISE and A/D.

References:

Pragma Fortress ClientSuite (Windows multi-factor RFC 6187 SSH client): <u>https://www.pragmasys.com/ssh-client/download</u>

Cisco & Pragma White paper on how to configure Cisco devices for multi-factor authentication: <u>https://www.pragmasys.com/products/support/cisco-2-factor</u>

An actual setup of Cisco 1921 router for MFA login using NPS and Active Directory is listed below. Yellow marked lines will be important in your setup:

Current configuration : 4241 bytes Т ! Last configuration change at 18:06:11 UTC Fri Dec 8 2023 by pragmasys\admin L version 15.5 hostname cisco1921 2 L boot-start-marker boot system usbflash0:c1900-universalk9-mz.SPA.155-3.M6a.bin boot-end-marker Т shell processing full aaa new-model aaa group server radius myradius server name fatty1 server name NPS1

!
aaa authentication login default group myradius local
aaa authorization exec default group myradius local
aaa authorization network default group myradius local
!
aaa session-id common
!
radius server fatty1
address ipv4 10.0.1.33 auth-port 1812 acct-port 1813
key pragmaYYYZZZ
!
radius server NPS1
address ipv4 10.0.1.13 auth-port 1812 acct-port 1813
key pragmaYYYZZZ

ļ

ļ

ip domain name pragmasys.local ip name-server 10.0.1.8 ip name-server 10.0.1.6

<mark>crypto pki trustpoint CA2</mark>

enrollment terminal revocation-check none authorization username alt-subjectname userprinciplename

crypto pki certificate chain CA2

certificate ca 2F344531720AE29E424F77D5494ED336 3082030B 308201F3 A0030201 0202102F 34453172 0AE29E42 4F77D549 4ED33630 0D06092A 864886F7 0D01010B 05003018 31163014 06035504 03130D50 5241474D 41524F4F 542D4341 301E170D 31363132 32393232 30323532 5A170D33 36313232 39323231 3235325A 30183116 30140603 55040313 0D505241 474D4152 4F4F542D 43413082 0122300D 06092A86 4886F70D 01010105 00038201 0F003082 010A0282 010100E3 7F07C2C9 35C4CC4B CF6FB147 A5A141B8 82D174B1 3E864196 74C7E49E A417F73C 8B6E4576 99DFDE04 CBE4B920 7200C243 FC096787 E1AC26FF 9953A919 BA974B26 783D7497 AF04B14B 29731BD4 1271250A 6833B55B 01B903C9 4764D105 8A14A85C 99BB3032 2C20D3BC 93A21A36 E4FC5C5C 3D0BC953 D8C7E0AB F7B02E49 BA3DACCD ACB6A007 82DD90B6 9039F8E6 63C22209 B7AB9D30 78C23434 6228626B 58BA8A28 02285422 FA7C50AC 34F65504 5CD420D1 D8034353 F51CE197 072DFF12 797CC02B 895FF1D3 8C339FE4 A34A5573 31A14479 EECE8AB0 80DA7EEB A4420474 E4752312 1FC3966C C0267DEB EF02B8CD 16EDF7F2 91BEC735 C8B6A782 85CEE524 08187D02 03010001 A351304F 300B0603 551D0F04 04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1418A229 4D1B6AD1 CA5E9D1B C6A41348 9245985B 6C301006 092B0601 04018237 15010403 02010030 0D06092A 864886F7 0D01010B 05000382 0101001B 02C4F8A6 B73C7180 41352B92 EA8AC1C2 CEECB4AA 34D6F224 E17EA723 6FF722B4 42E5600A D2FDE21F 9BAA4177 ED54C4D6 C353FCB3 B82E7ACE F53A4998 AEBE3CBF 8E7F90BC 8F1C12DD 113778CE 12B854CC D2C838B7 29DCB8C8 3050C13E 5D59DCAD 2008DF2E B6C51EAA 287FC661 F8C606E8 E5FA9687 521CC931 AF1254E7 3C2CFB70 C3953A4F A0BB3429 496D08F9 E901C48C 51CFBFEC EEBA2B83 FAABE31C 41A70F8E 0C163C2C 2DD558CD B0EAC486 528278B2 B501B651 4817A55A A8D38524 8F691D1D 104291E1 5671C18D 3EE030C9 36055F53 1A0868E2 D8E23FF9 E592ED69 DC740FF9 A4A0D0C9 23481842 BD837FA8 F44262D2 193A091A 91C65D34 1E9EDFE6 D8A6A7

license udi pid CISCO1921/K9 sn FJC1939E3B7 1 username cisco privilege 15 secret 5 \$1\$Fi9T\$dVcIJOZTCtdbkq51ZHMn20 interface Embedded-Service-Engine0/0 no ip address shutdown 1 interface GigabitEthernet0/0 ip address 10.0.1.121 255.255.255.0 duplex auto speed auto ! interface GigabitEthernet0/1 no ip address shutdown duplex auto speed auto I ip default-gateway 10.0.1.1 ip forward-protocol nd no ip http server no ip http secure-server i ip ssh rsa keypair-name SSH-RSA ip ssh version 2 ip ssh server certificate profile user trustpoint verify CA2 ip ssh server algorithm hostkey ssh-rsa ip ssh server algorithm authentication keyboard password publickey ip ssh server algorithm publickey x509v3-ssh-rsa Т control-plane no vstack Ţ line con 0 line aux 0 line vty 04 privilege level 15 password cisco transport input ssh line vty 5 15 privilege level 15 transport input telnet ssh T scheduler allocate 20000 1000 ntp server 192.5.41.40 L end