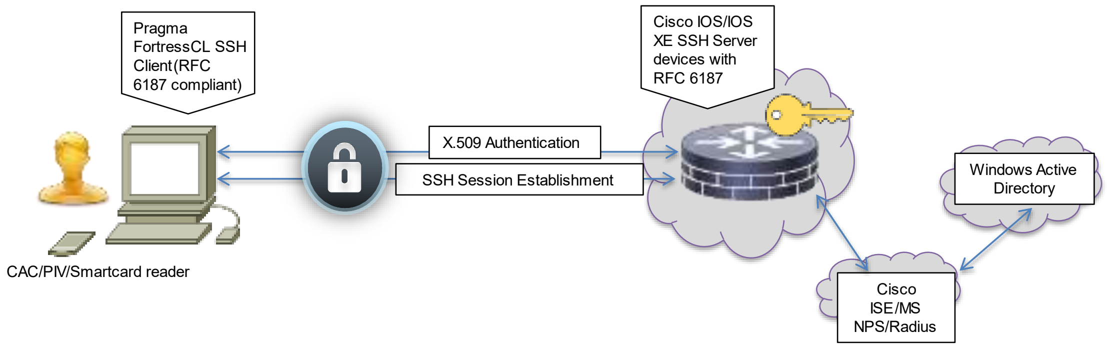
**Cisco MFA access with Microsoft NPS Radius and Pragma FortressCL**

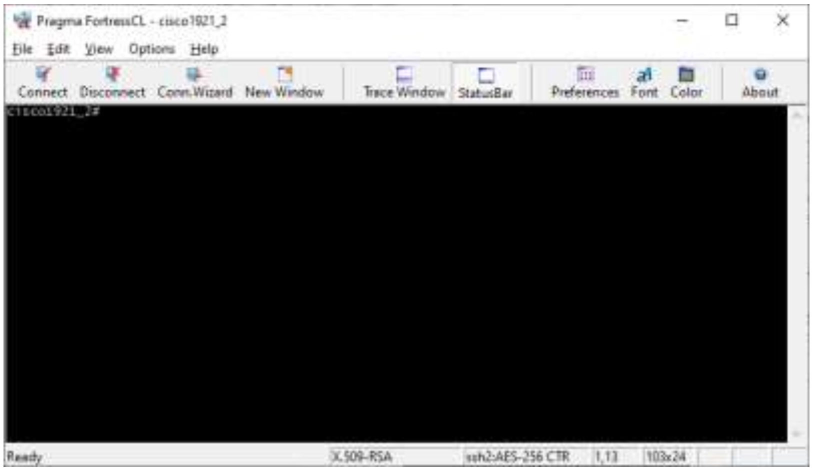
*Author: Pragma Systems, Inc. www.pragmasys.com December 11, 2023*

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 **https://www.pragmasys.com/products/support/cisco-2-factor** . 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


Pragma FortressCL SSH Client(RFC 6187 compliant)
CAC/PIV/Smartcard reader
X.509 Authentication
SSH Session Establishment
Cisco IOS/IOS XE SSH Server devices with RFC 6187
Windows Active Directory
Cisco ISE/MS NPS/Radius

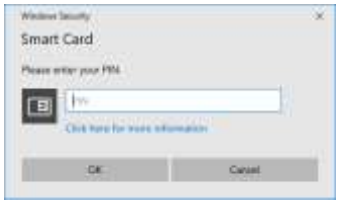
Task 1: RFC 6187 compliant SSH clients are needed. Download and install Pragma Fortress ClientSuite in a Windows computer **https://www.pragmasys.com/ssh-client/download**. It can run on any Windows OS (Windows 10/11/8.1 or Windows Server 2022/2019/2016/2012R2). Pragma Fortress ClientSuite provides an 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.



Pragma FortressCL - cisco1921_2
File Edit View Options Help
Connect Disconnect Conn.Wizard New Window Trace Window StatusBar Preferences Font Color About

```
cisco1921_2#
```

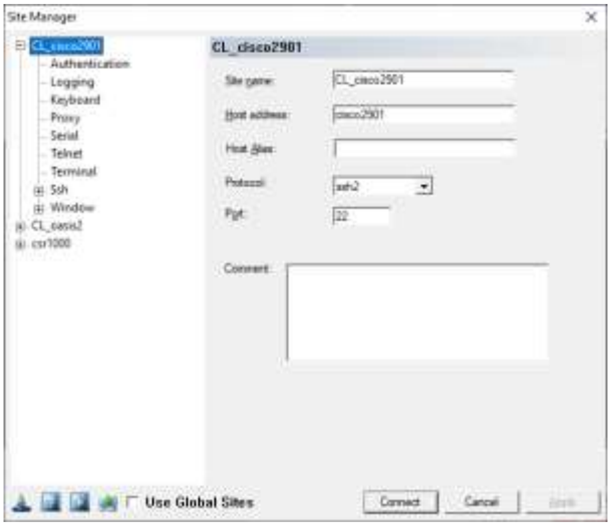
Ready
X.509-RSA
ssh2:AES-256 CTR
1,13
103x24



Windows Security

Smart Card

Please enter your PIN



CL_cisco2901

Site name: CL_cisco2901

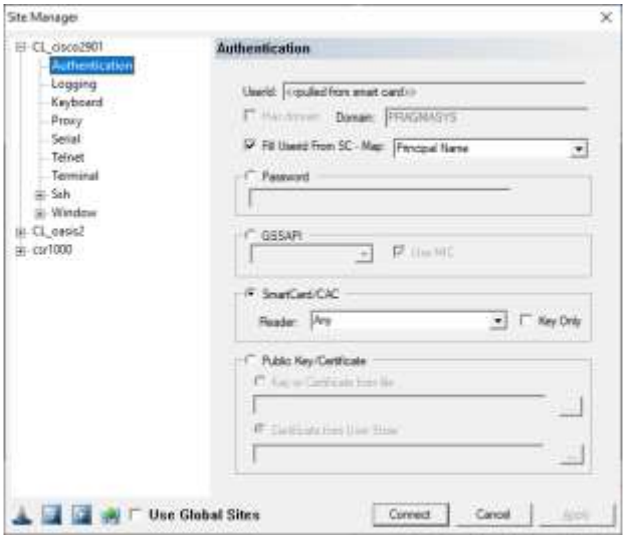
Host address: cisco2901

Host Alias:

Protocol: ssh2

Port: 22

Comment:



Authentication

UserId: <<pulled from smart card>>

☐ Mac domain Domain: PRAGMASYS

☑ Fill UserId From SC - Map: Principal Name

○ Password

○ GSSAPI ☑ Use MIC

● SmartCard/CAC

Reader: Any ☐ Key Only

○ Public Key/Certificate

○ Key or Certificate from file

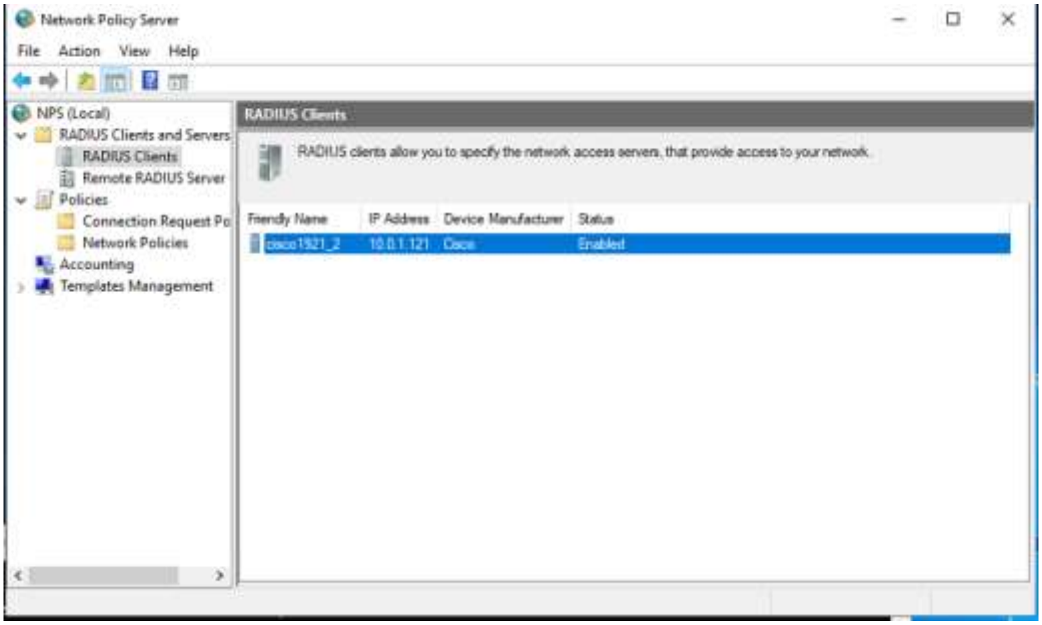
● Certificate from User Store

Task 2: Configure your Cisco device to allow MFA authentication following the steps listed in Cisco & Pragma white paper **https://www.pragmasys.com/products/support/cisco-2-factor**. 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.

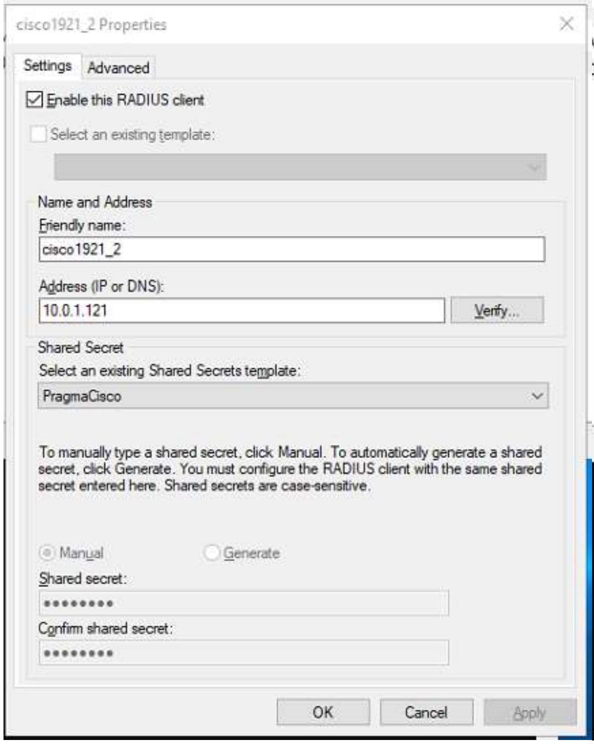
Step 2: Define your Cisco device RADIUS link by right clicking “Radius Clients” in NPS and choosing “New”. Then provide the IPv4 address of the Cisco device, a shared secret (any size string works), a friendly name for the link and choose “Cisco” as the Vendor name in “Advanced” tab.



RADIUS Clients

RADIUS clients allow you to specify the network access servers, that provide access to your network.

| Friendly Name | IP Address | Device Manufacturer | Status |
|---|---|---|---|
| cisco1921_2 | 10.0.1.121 | Cisco | Enabled |


cisco1921_2 Properties

☑ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name: cisco1921_2

Address (IP or DNS): 10.0.1.121 [Verify...]

Shared Secret

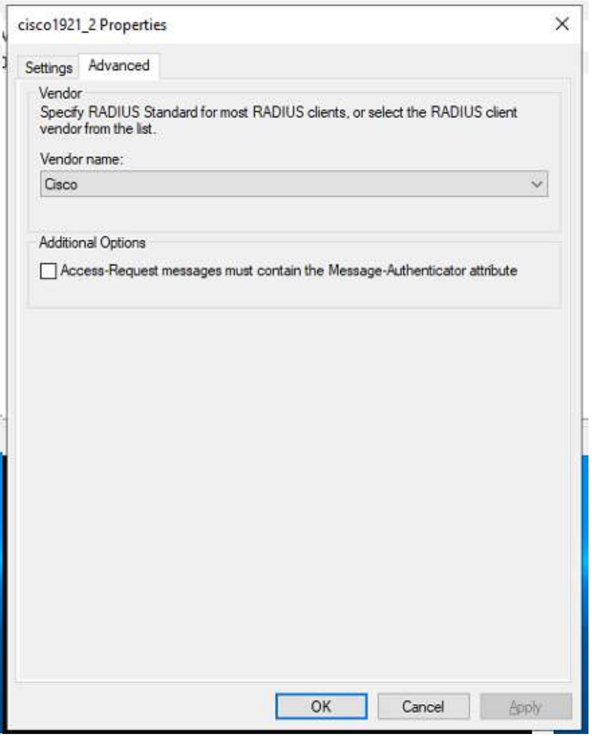
Select an existing Shared Secrets template: PragmaCisco

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••

Confirm shared secret: ••••••••


cisco1921_2 Properties

Vendor

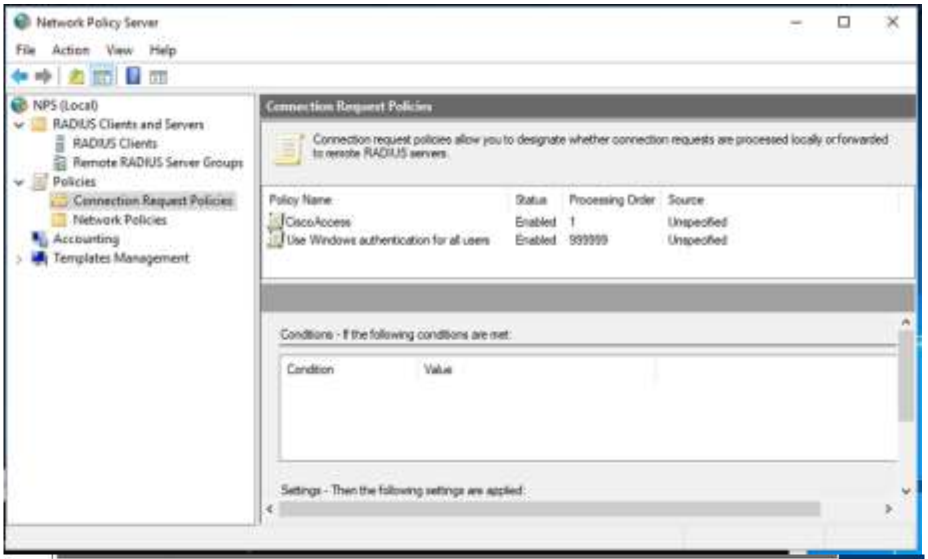
Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: Cisco

Additional Options

☐ Access-Request messages must contain the Message-Authenticator attribute

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



Network Policy Server

File Action View Help

- NPS (Local)
  - RADIUS Clients and Servers
    - RADIUS Clients
    - Remote RADIUS Server Groups
  - Policies
    - Connection Request Policies
    - Network Policies
  - Accounting
  - Templates Management

Connection Request Policies

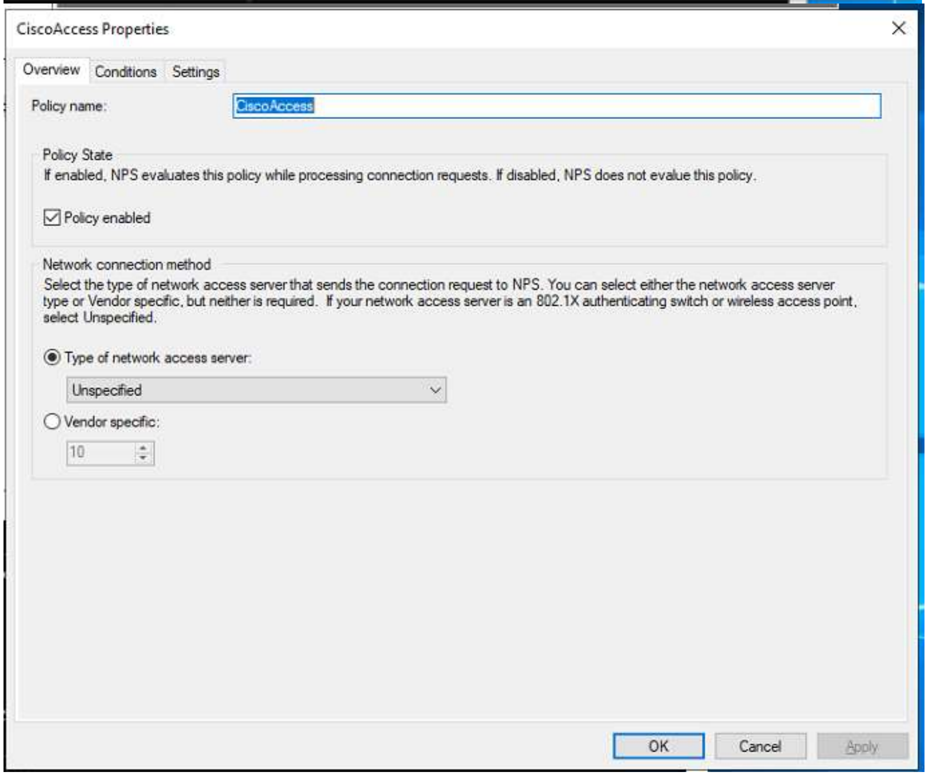
Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

| Policy Name | Status | Processing Order | Source |
|---|---|---|---|
| CiscoAccess | Enabled | 1 | Unspecified |
| Use Windows authentication for all users | Enabled | 999999 | Unspecified |

Conditions - If the following conditions are met:

| Condition | Value |
|---|---|

Settings - Then the following settings are applied:



CiscoAccess Properties

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

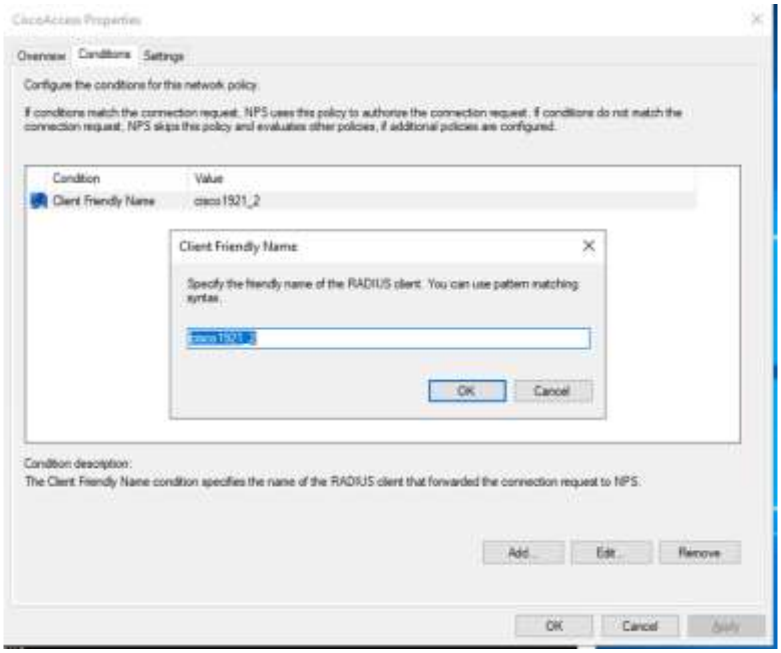
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server:

Unspecified

○ Vendor specific:

10



Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

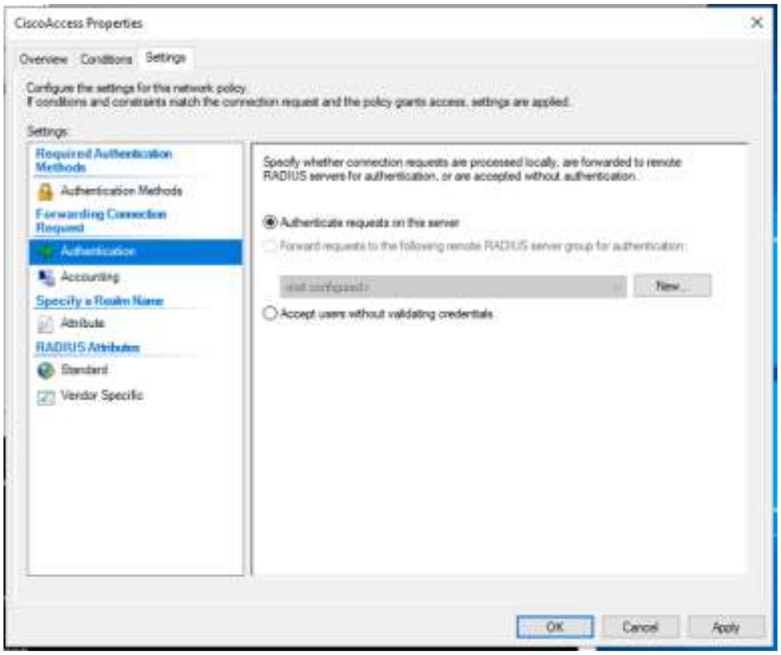
| Condition | Value |
|---|---|
| Client Friendly Name | cisco1921_2 |

Client Friendly Name

Specify the friendly name of the RADIUS client. You can use pattern matching syntax.

cisco1921_2

Condition description:
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

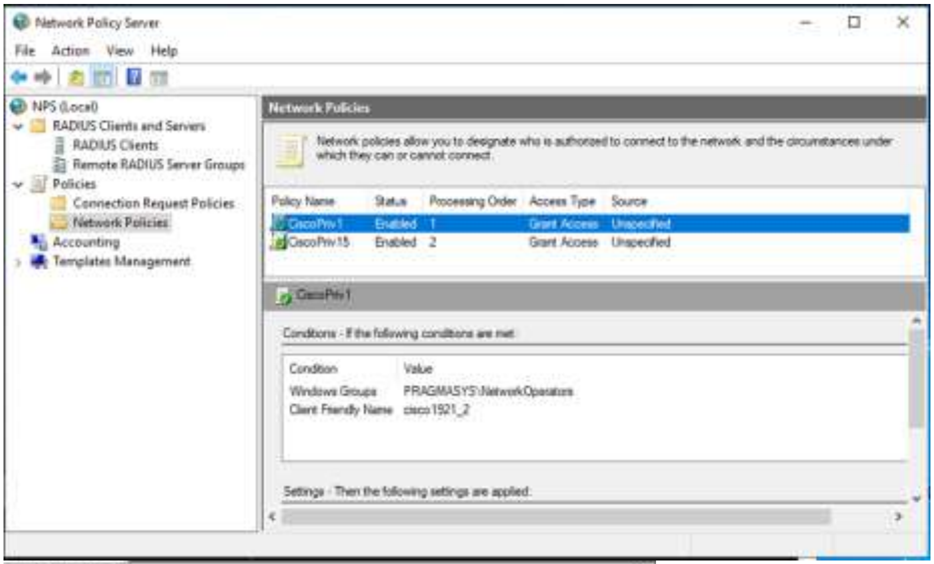
● Authenticate requests on this server

○ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

○ Accept users without validating credentials

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).



Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

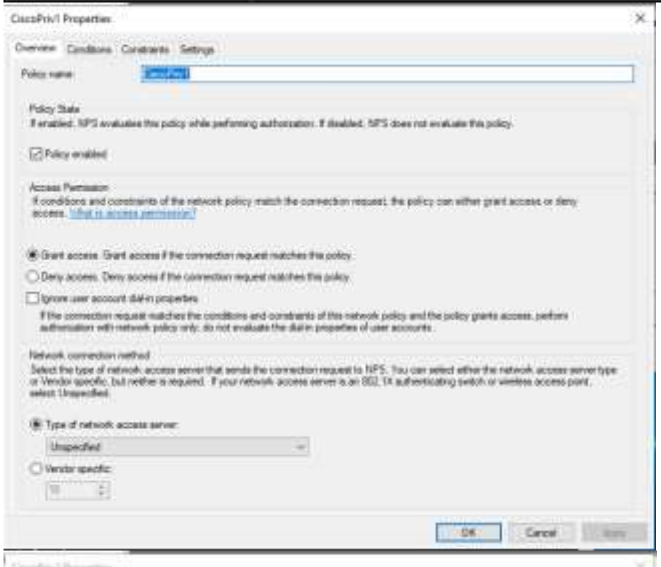
| Policy Name | Status | Processing Order | Access Type | Source |
|---|---|---|---|---|
| CiscoPriv1 | Enabled | 1 | Grant Access | Unspecified |
| CiscoPriv15 | Enabled | 2 | Grant Access | Unspecified |

CiscoPriv1

Conditions - If the following conditions are met:

| Condition | Value |
|---|---|
| Windows Groups | PRAGMASYS\NetworkOperators |
| Client Friendly Name | cisco1921_2 |

Settings - Then the following settings are applied:



Policy name: CiscoPriv1

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

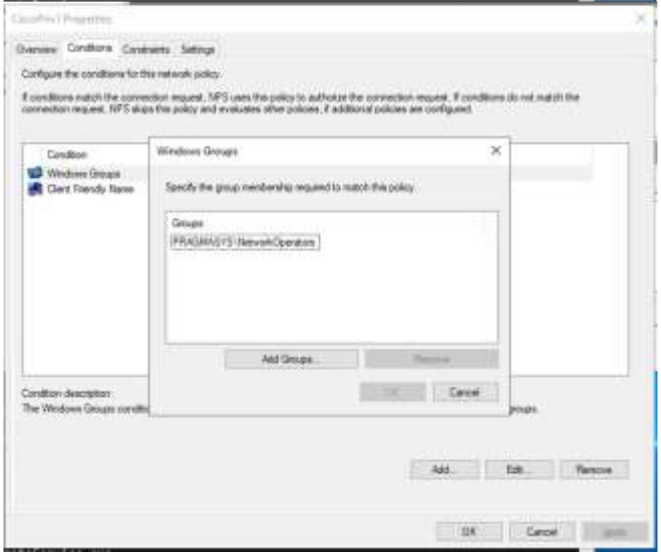
○ Deny access. Deny access if the connection request matches this policy.

□ Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

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



Configure the conditions for this network policy.

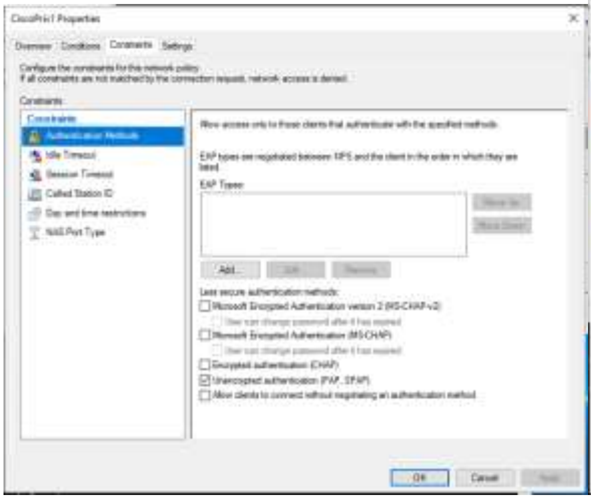
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

| Condition |
|---|
| Windows Groups |
| Client Friendly Name |

Condition description:
The Windows Groups conditi[illegible] groups.

Specify the group membership required to match this policy.

Groups
PRAGMASYS\NetworkOperators



CiscoPriv1 Properties

Overview | Conditions | **Constraints** | Settings

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

- Constraints
  - Authentication Methods
  - Idle Timeout
  - Session Timeout
  - Called Station ID
  - Day and time restrictions
  - NAS Port Type

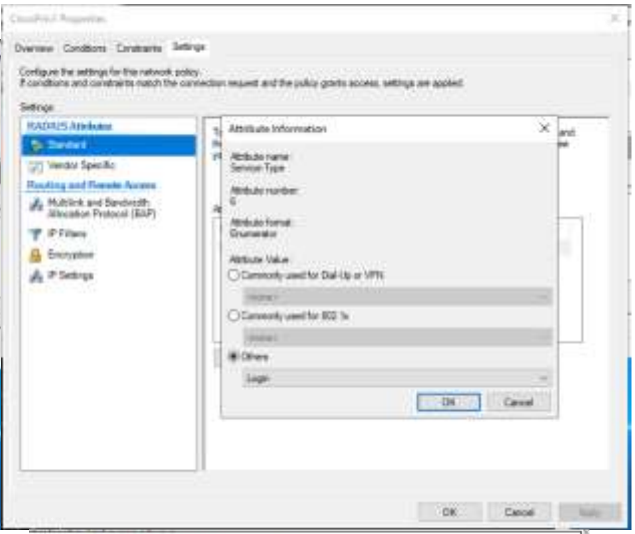
Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

- □ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  - □ User can change password after it has expired
- □ Microsoft Encrypted Authentication (MS-CHAP)
  - □ User can change password after it has expired
- □ Encrypted authentication (CHAP)
- ☑ Unencrypted authentication (PAP, SPAP)
- □ Allow clients to connect without negotiating an authentication method



CiscoPriv1 Properties

Overview | Conditions | Constraints | **Settings**

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes
  - Standard
  - Vendor Specific
- Routing and Remote Access
  - Multilink and Bandwidth Allocation Protocol (BAP)
  - IP Filters
  - Encryption
  - IP Settings

Attribute Information

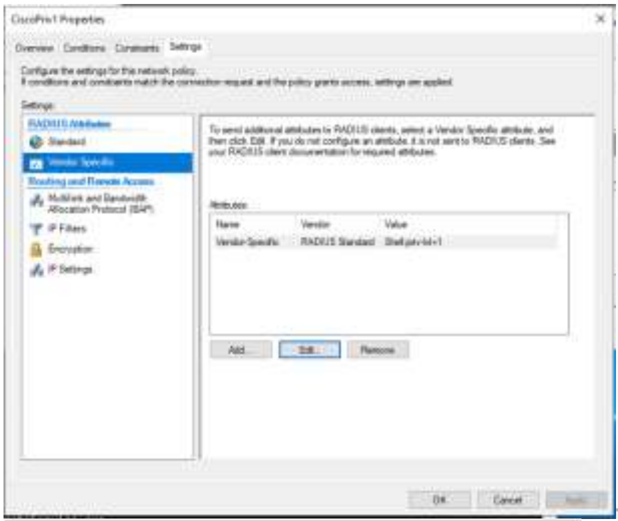
Attribute name:
Service Type

Attribute number:
6

Attribute format:
Enumerator

Attribute Value:

- ○ Commonly used for Dial-Up or VPN
  - <none>
- ○ Commonly used for 802.1x
  - <none>
- ● Others
  - Login



CiscoPriv1 Properties

Overview | Conditions | Constraints | **Settings**

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

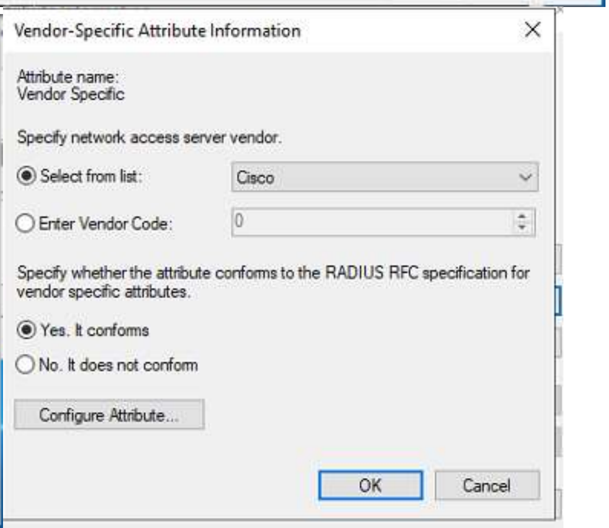
Settings:

- RADIUS Attributes
  - Standard
  - Vendor Specific
- Routing and Remote Access
  - Multilink and Bandwidth Allocation Protocol (BAP)
  - IP Filters
  - Encryption
  - IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

| Name | Vendor | Value |
|---|---|---|
| Vendor-Specific | RADIUS Standard | Shell:priv-lvl=1 |



Vendor-Specific Attribute Information

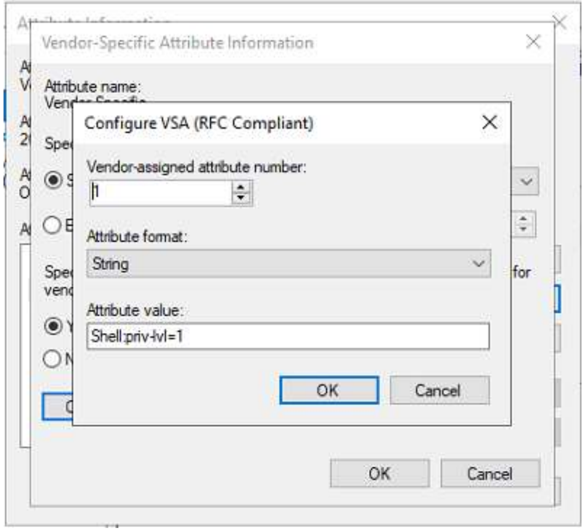
Attribute name:
Vendor Specific

Specify network access server vendor.

- ● Select from list: Cisco
- ○ Enter Vendor Code: 0

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

- ● Yes. It conforms
- ○ No. It does not conform



Attribute Information

Vendor-Specific Attribute Information

Attribute name:
Vendor Specific

Configure VSA (RFC Compliant)

Vendor-assigned attribute number:
1

Attribute format:
String

Attribute value:
Shell:priv-lvl=1

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):*** **https://www.pragmasys.com/ssh-client/download**

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

**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
!
! Last configuration change at 18:06:11 UTC Fri Dec 8 2023 by pragmasys\admin
!
version 15.5
hostname cisco1921_2
!
boot-start-marker
boot system usbflash0:c1900-universalk9-mz.SPA.155-3.M6a.bin
boot-end-marker
!
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
!

ip domain name pragmasys.local
ip name-server 10.0.1.8
ip name-server 10.0.1.6
!
crypto pki trustpoint CA2
 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
            quit
```

```
license udi pid CISCO1921/K9 sn FJC1939E3B7
!
username cisco privilege 15 secret 5 $1$Fi9T$dVcIJOZTCtdbkq51ZHMn20
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
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
!
ip default-gateway 10.0.1.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
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
!
control-plane
no vstack
!
line con 0
line aux 0
line vty 0 4
 privilege level 15
 password cisco
 transport input ssh
line vty 5 15
 privilege level 15
 transport input telnet ssh
!
scheduler allocate 20000 1000
ntp server 192.5.41.40
!
end
```