Configure ISE Radius Authentication for Secure Firewall Chassis Manager (FCM)

Contents

Introduction

This document describes the process of how to configure Radius Authorization/Authentication access for Secure Firewall Chasiss Manager with ISE.

Prerequisites

Requirements

Cisco recommends having knowledge of the following topics:

- Secure Firewall Chassis Manager (FCM)
- Cisco Identity Services Engine (ISE)
- Radius Authentication

Components Used

- Cisco Firepower 4110 Security Appliance FXOS v2.12
- Cisco Identity Services Engine (ISE) v3.2 patch 4

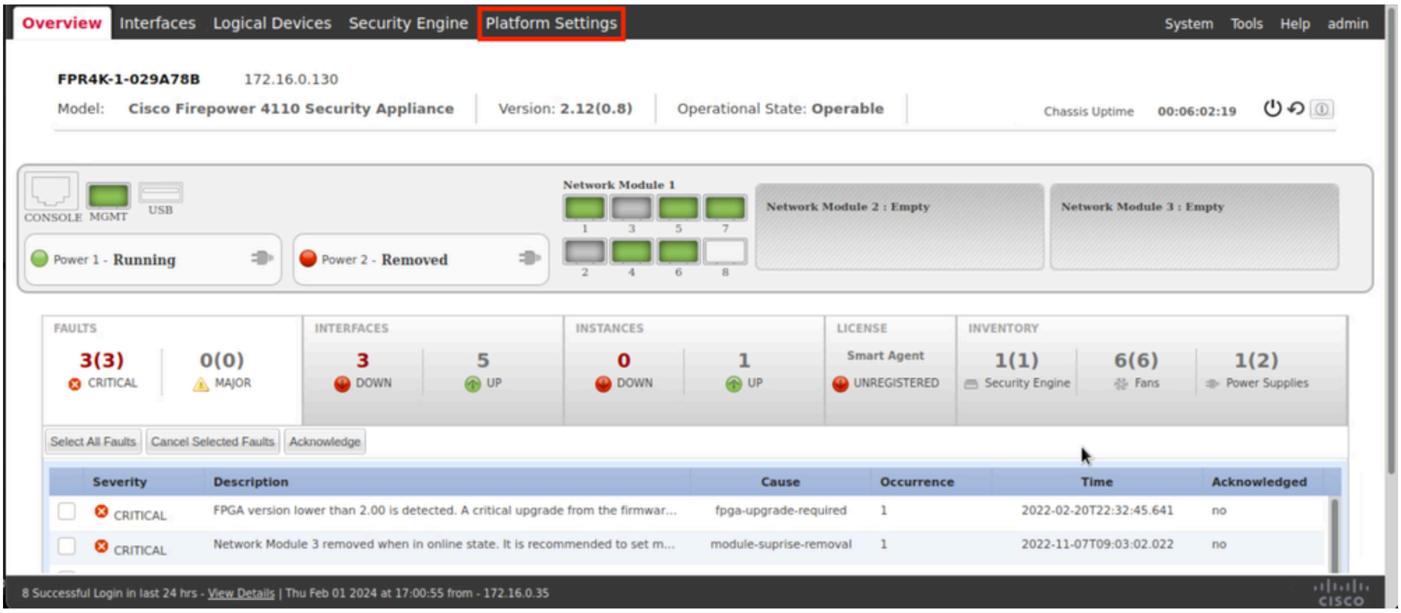
  The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Configurations

Secure Firewall Chasiss Manager

Step 1. Log into the Firepower Chassis Manager GUI.
Step 2. Navigate to **Platform Settings**



FPR4K-1-029A78B 172.16.0.130

Model: Cisco Firepower 4110 Security Appliance | Version: 2.12(0.8) | Operational State: Operable | Chassis Uptime 00:06:02:19

Power 1 - Running

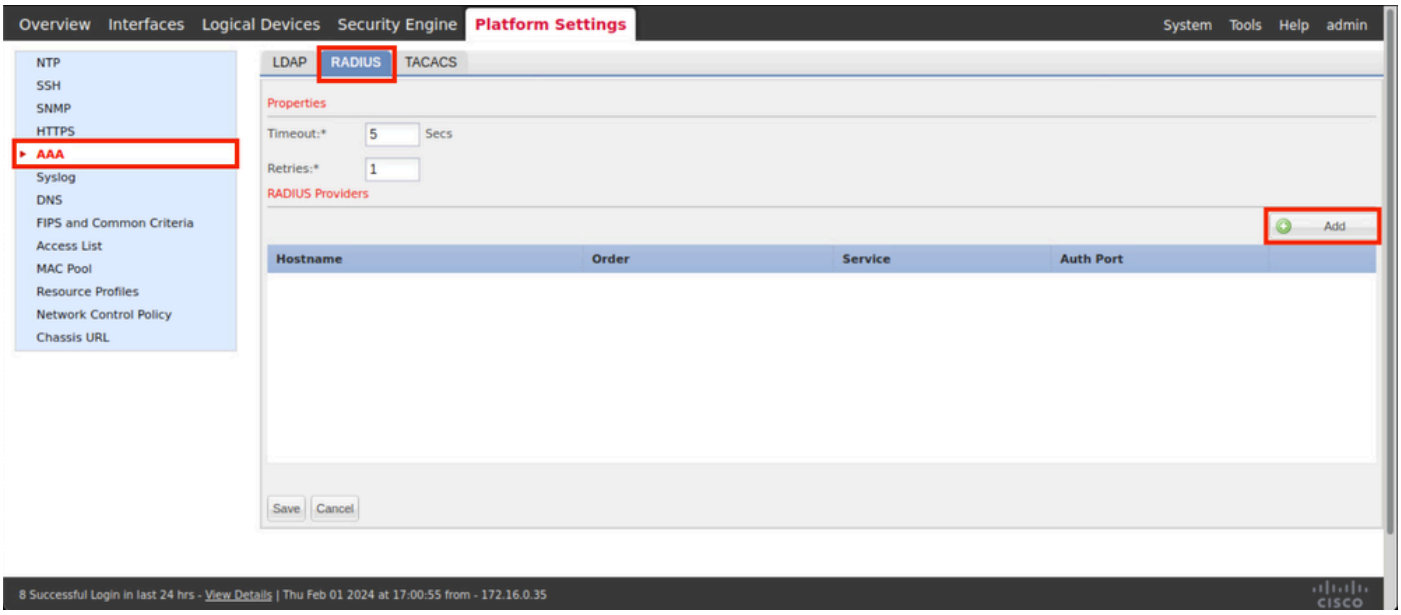
Power 2 - Removed

FAULTS		INTERFACES		INSTANCES		LICENSE	INVENTORY		
3(3)	0(0)	3	5	0	1	Smart Agent	1(1)	6(6)	1(2)
CRITICAL	MAJOR	DOWN	UP	DOWN	UP	UNREGISTERED	Security Engine	Fans	Power Supplies

	Severity	Description	Cause	Occurrence	Time	Acknowledged
□	CRITICAL	FPGA version lower than 2.00 is detected. A critical upgrade from the firmwar...	fpga-upgrade-required	1	2022-02-20T22:32:45.641	no
□	CRITICAL	Network Module 3 removed when in online state. It is recommended to set m...	module-suprise-removal	1	2022-11-07T09:03:02.022	no

8 Successful Login in last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Step 3. From the left menu click over **AAA.** Select Radius and **Add** a new RADIUS provider.



Properties

Timeout:* 5 Secs

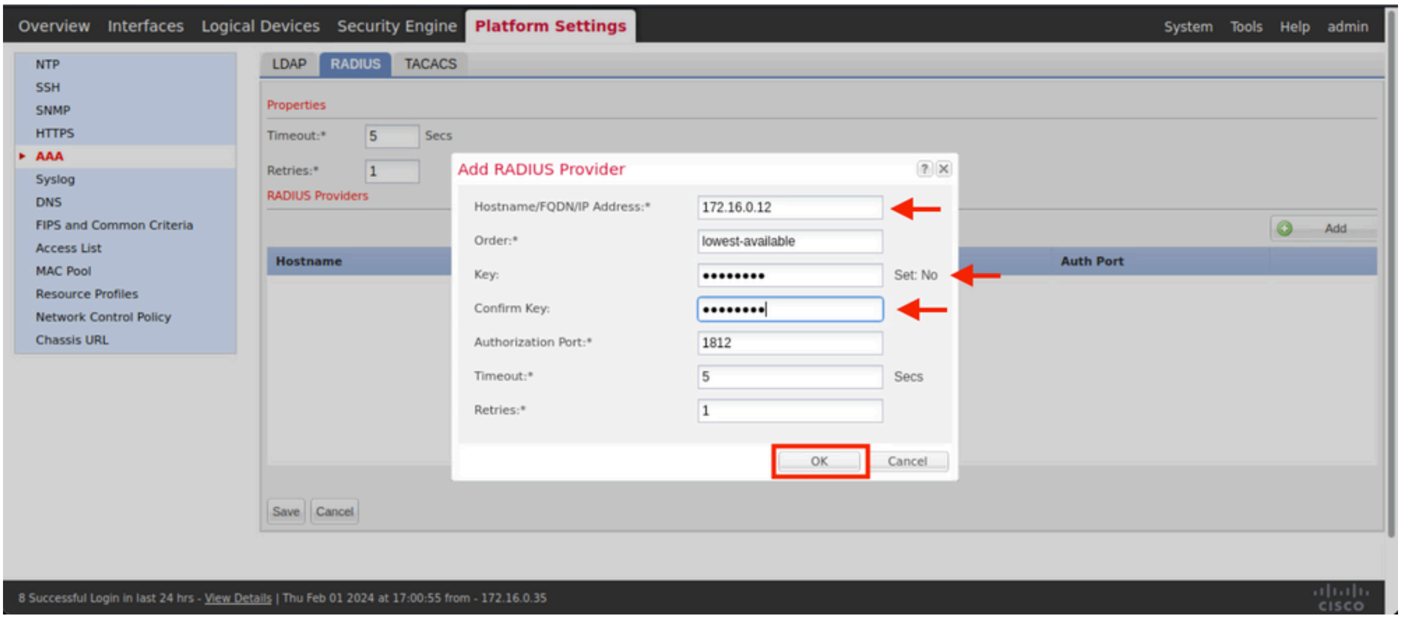
Retries:* 1

RADIUS Providers

Hostname	Order	Service	Auth Port

8 Successful Login in last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Step 4. Fill the prompt menu with the requested information of the Radius Provider. Click **OK**.



Properties

Timeout:* 5 Secs

Retries:* 1

RADIUS Providers

Hostname	Auth Port

Add RADIUS Provider

Hostname/FQDN/IP Address:* 172.16.0.12

Order:* lowest-available

Key: •••••••• Set: No

Confirm Key: ••••••••

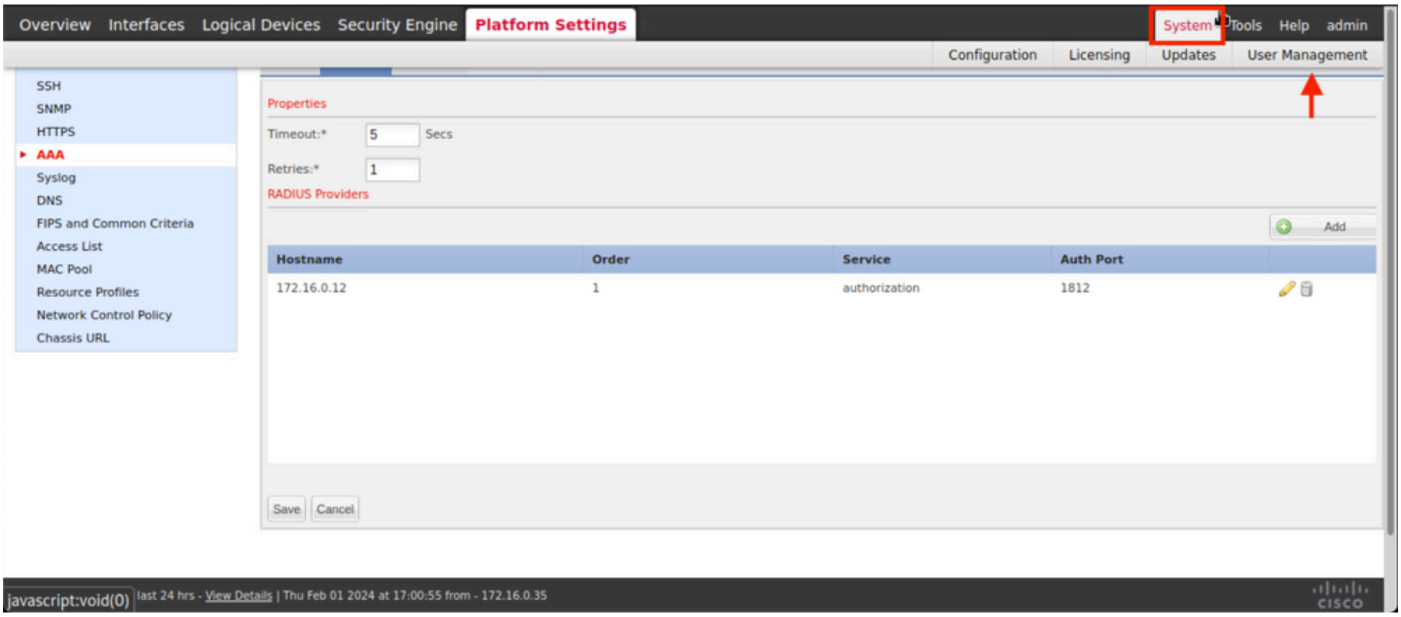
Authorization Port:* 1812

Timeout:* 5 Secs

Retries:* 1

8 Successful Login in last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Step 5. Navigate to **System > User Management**



Properties

Timeout:* 5 Secs

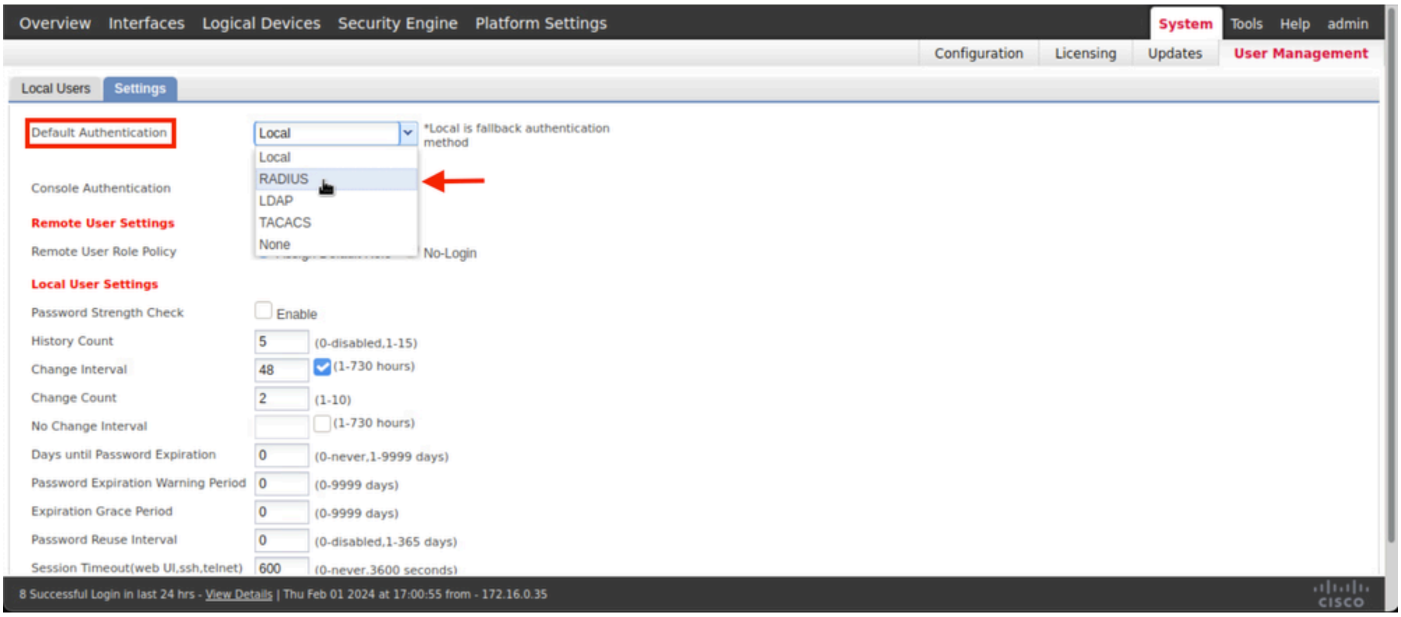
Retries:* 1

RADIUS Providers

Hostname	Order	Service	Auth Port
172.16.0.12	1	authorization	1812

javascript:void(0) last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Step 6. Click on Settings tab and set Default Authentication from the drop down menu to Radius, then, scroll down and Save the configuration.



Default Authentication: Local *Local is fallback authentication method

Console Authentication

Remote User Settings

Remote User Role Policy: No-Login

Local User Settings

Password Strength Check: □ Enable

History Count: 5 (0-disabled,1-15)

Change Interval: 48 ☑ (1-730 hours)

Change Count: 2 (1-10)

No Change Interval: □ (1-730 hours)

Days until Password Expiration: 0 (0-never,1-9999 days)

Password Expiration Warning Period: 0 (0-9999 days)

Expiration Grace Period: 0 (0-9999 days)

Password Reuse Interval: 0 (0-disabled,1-365 days)

Session Timeout(web UI,ssh,telnet): 600 (0-never,3600 seconds)

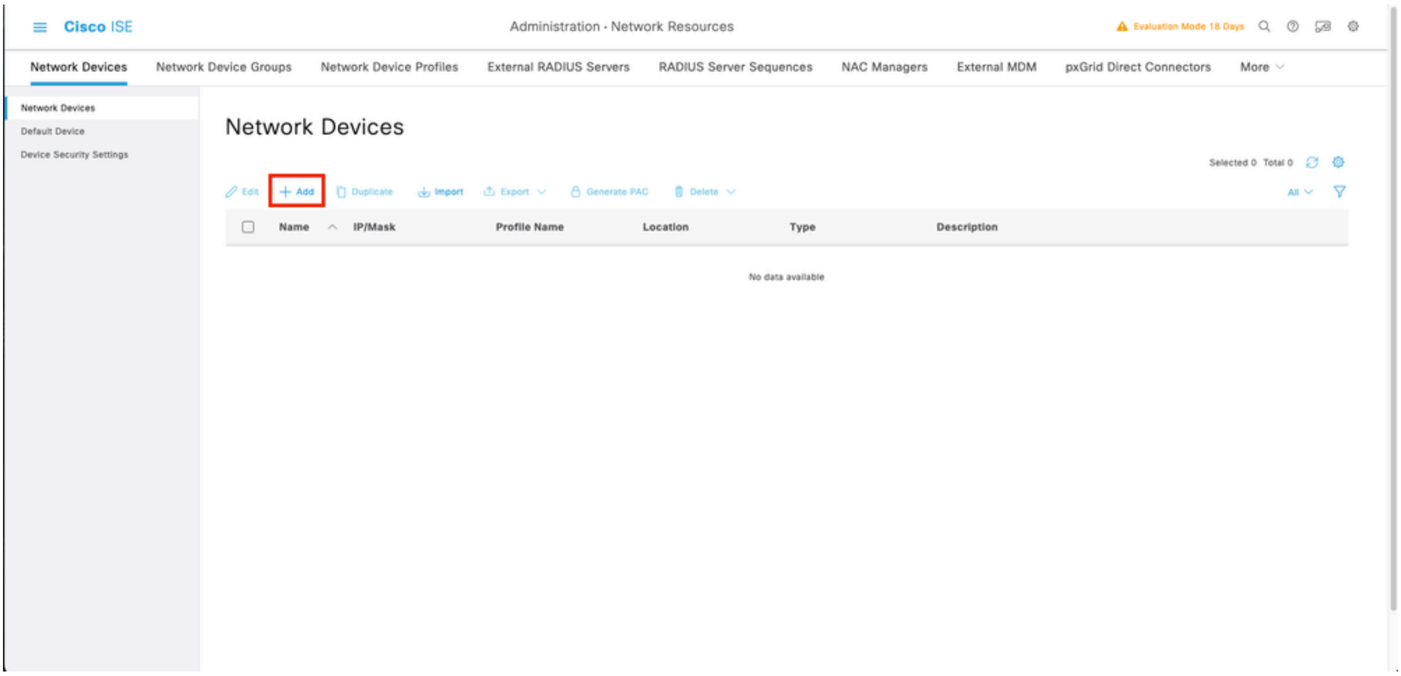
8 Successful Login in last 24 hrs - View Details | Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35

Note: FCM configuration has finish at this point.

Identity Service Engine

Step 1. Add a new Network Device.

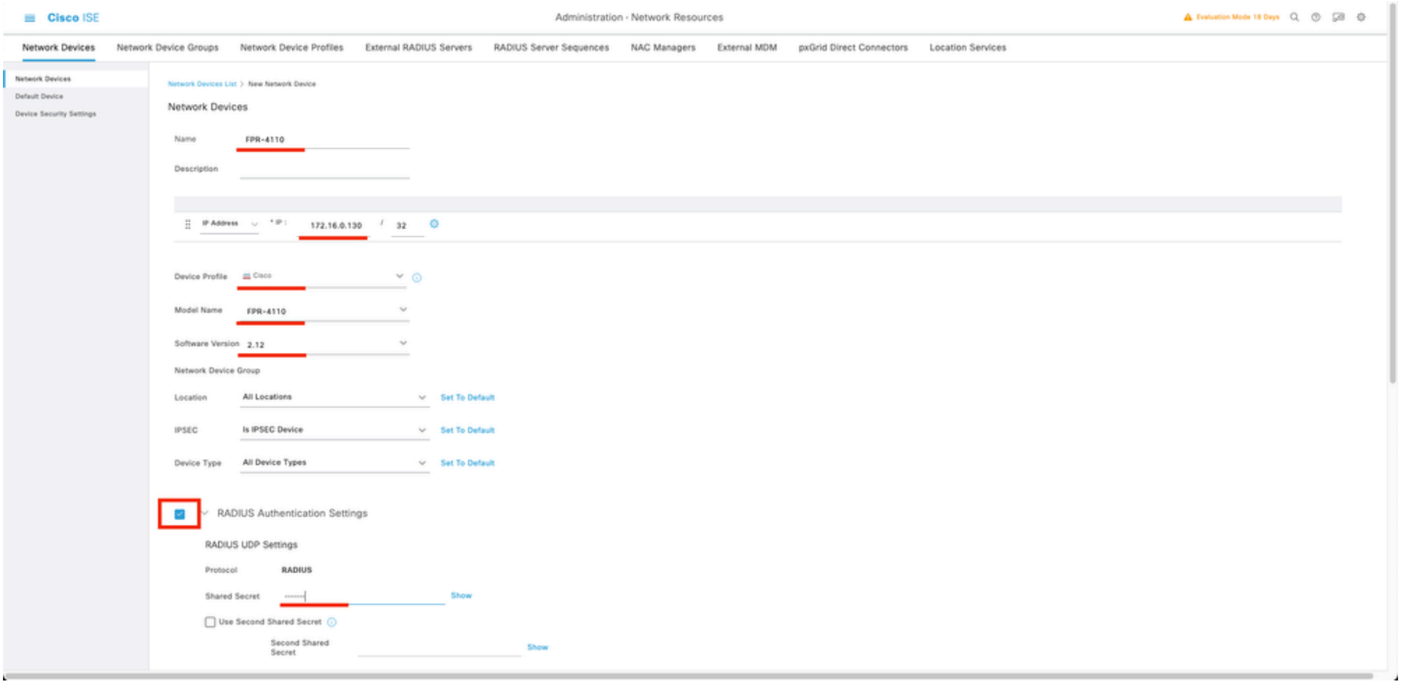
Navigate to the burger icon ≡ located in the upper left corner > Administration > Network Resources > Network Devices > +Add.



Step 2. Fill the paramaters requested about the new Network Devices information.

2.1 Check the RADIUS checkbox
2.2 Configure the same Shared Secret key as in the FCM Radius Configuration.

2.1 Scroll down and click Submit.



Network Devices

Name FPR-4110

Description

IP Address * IP : 172.16.0.130 / 32

Device Profile Cisco

Model Name FPR-4110

Software Version 2.12

Network Device Group

Location All Locations Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type All Device Types Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

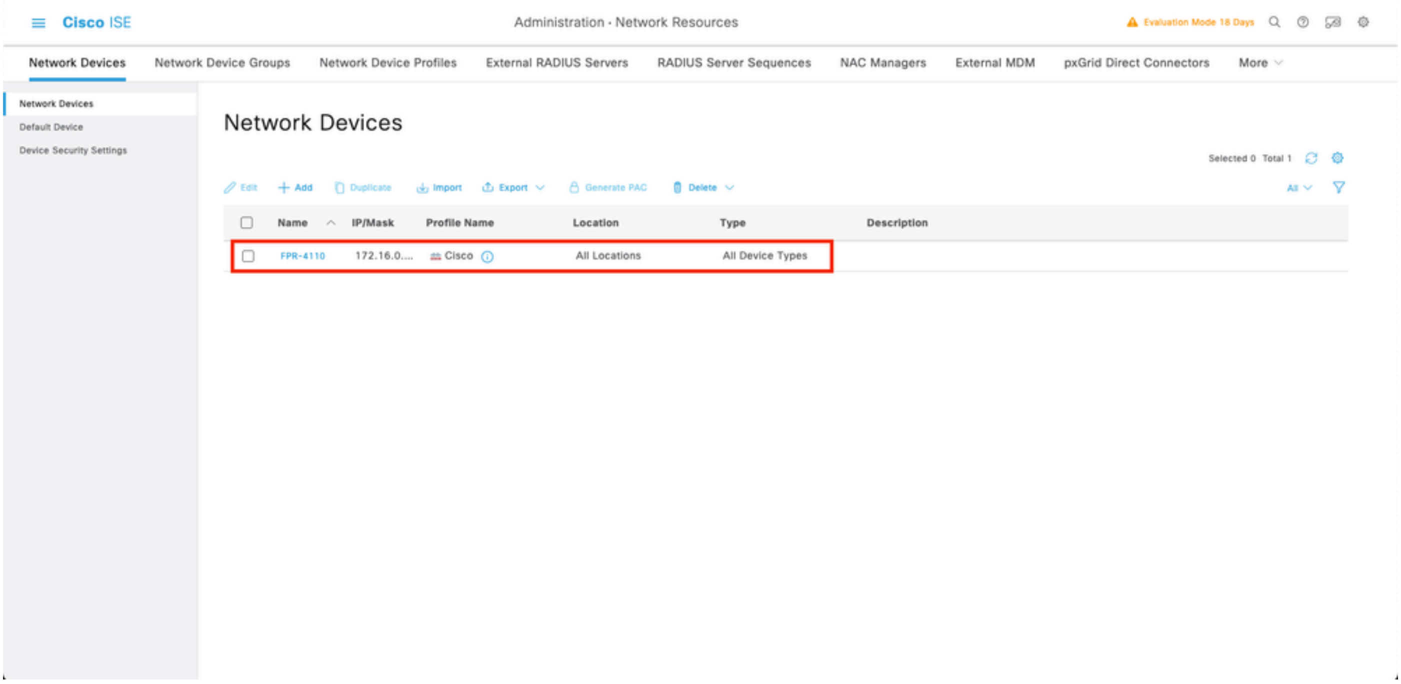
Protocol RADIUS

Shared Secret ······· Show

□ Use Second Shared Secret

Second Shared Secret Show

Step 3. Validate the new device is shown under Network Devices.

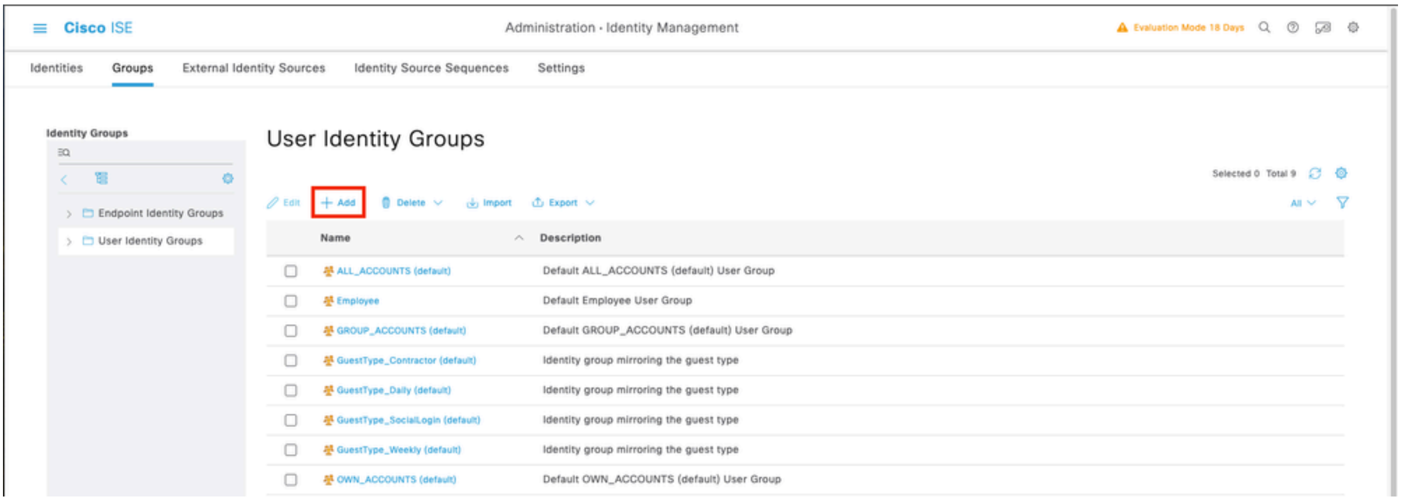


Network Devices

Selected 0 Total 1

□	Name	IP/Mask	Profile Name	Location	Type	Description
□	FPR-4110	172.16.0....	Cisco	All Locations	All Device Types	

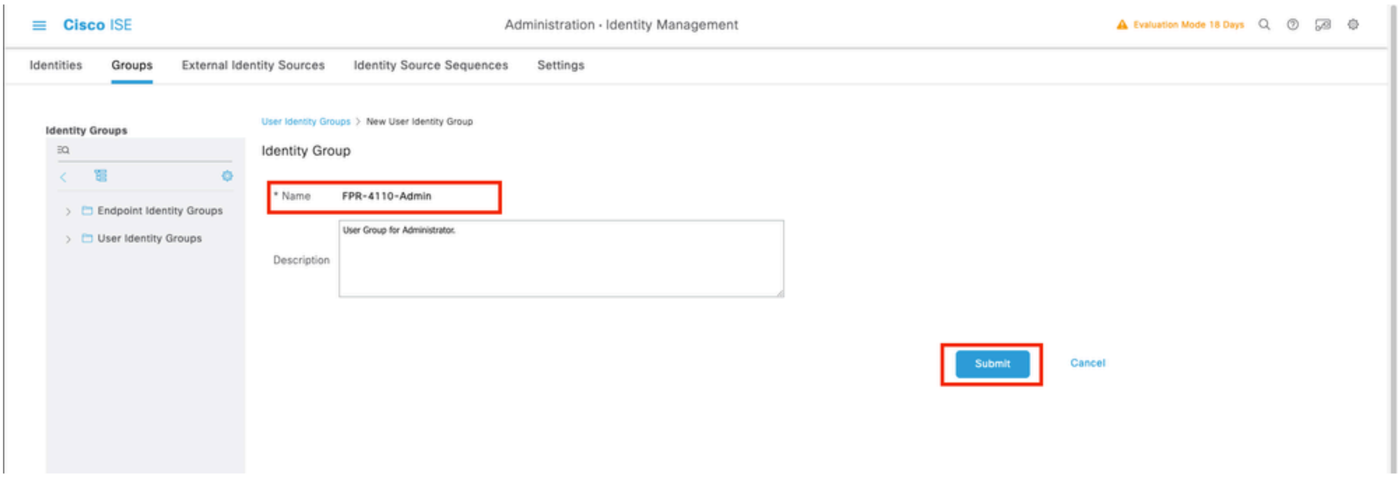
Step 4. Create the required User Identity Groups. Navigate to the burger icon ≡ located in the upper left corner > Administration > Identity Management > Groups > User Identity Groups > + Add



User Identity Groups

	Name	Description
□	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
□	Employee	Default Employee User Group
□	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
□	GuestType_Contractor (default)	Identity group mirroring the guest type
□	GuestType_Daily (default)	Identity group mirroring the guest type
□	GuestType_SocialLogin (default)	Identity group mirroring the guest type
□	GuestType_Weekly (default)	Identity group mirroring the guest type
□	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Step 5. Set a name for the Admin User Identity Group and click Submit in order to save the configuration.

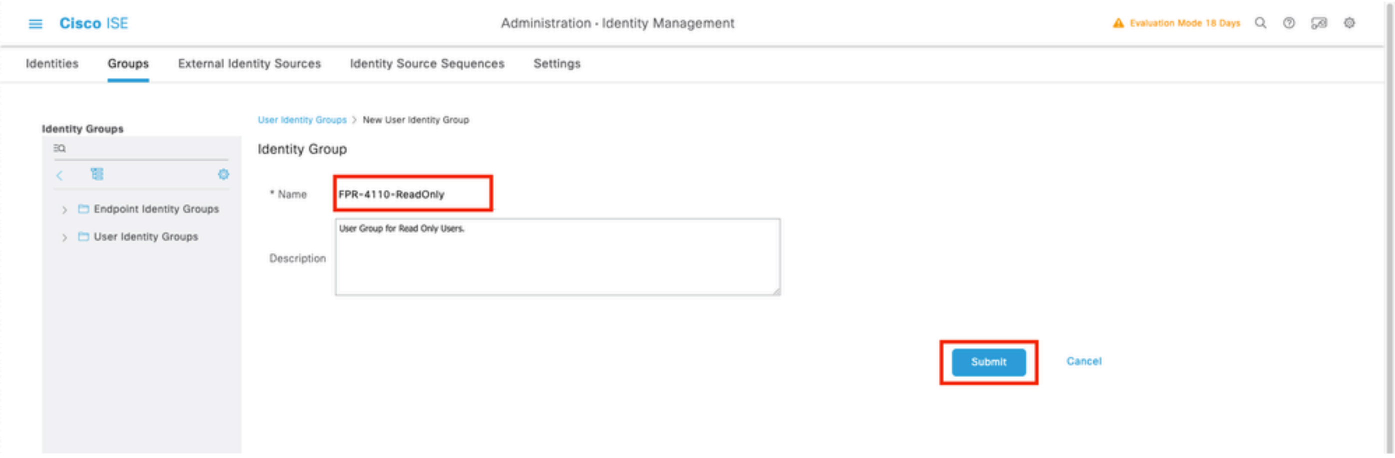

Cisco ISE
Administration · Identity Management
Evaluation Mode 18 Days
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > New User Identity Group
Submit
Cancel

Identity Group

* Name FPR-4110-Admin

Description User Group for Administrator.

5.1 Repeat the same process for ReadOnly users.

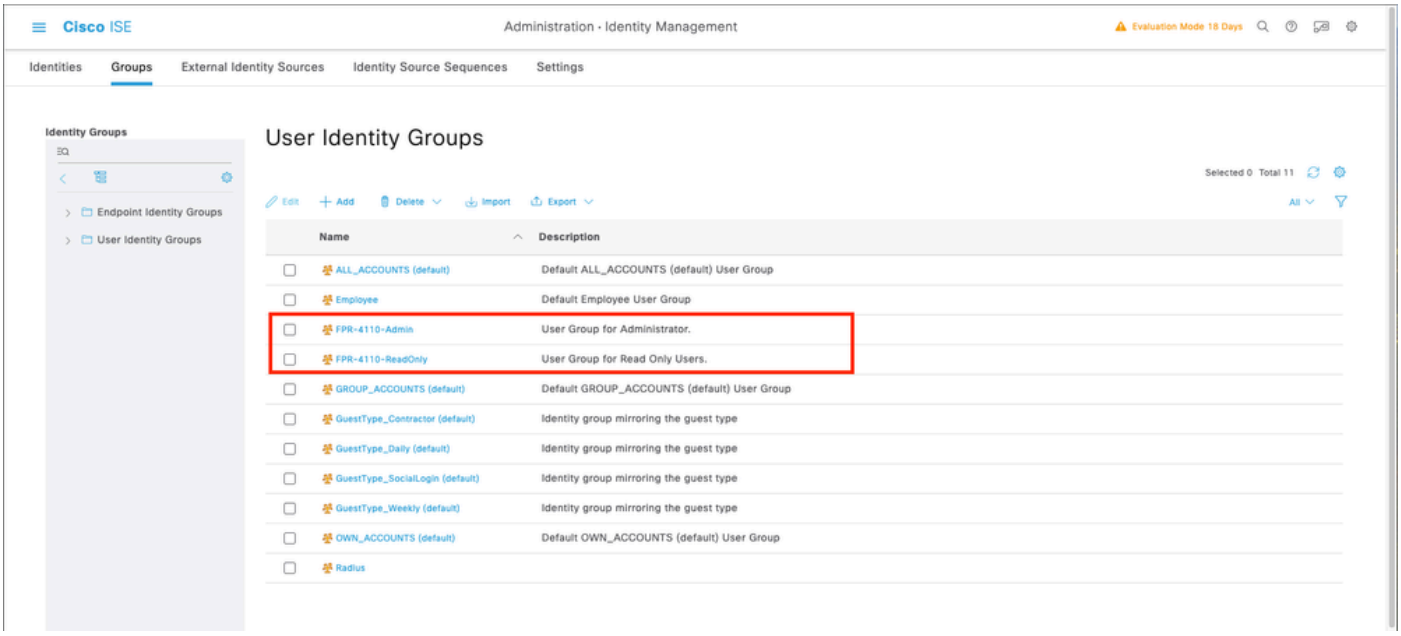

Cisco ISE
Administration · Identity Management
Evaluation Mode 18 Days
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > New User Identity Group
Submit
Cancel

Identity Group

* Name FPR-4110-ReadOnly

Description User Group for Read Only Users.

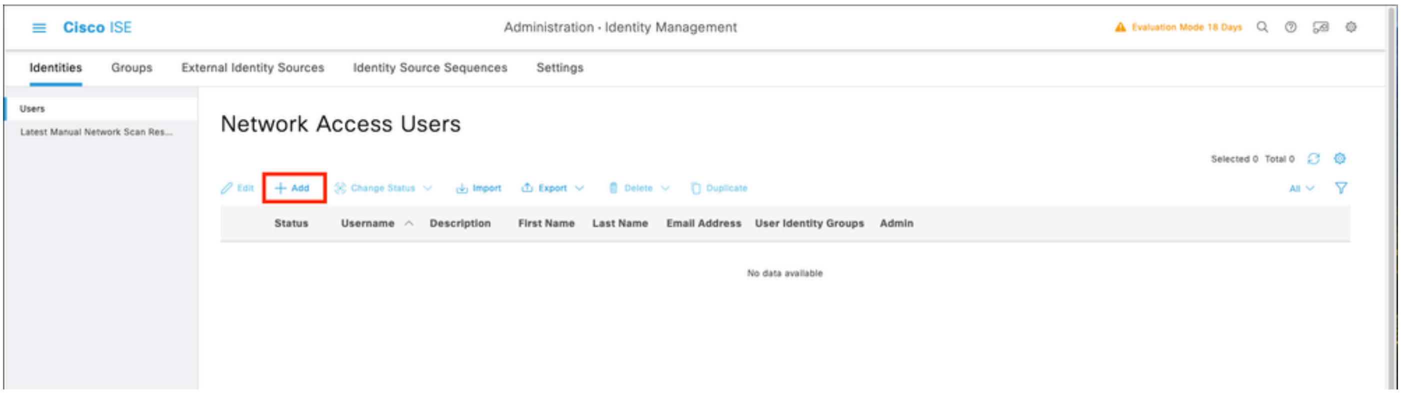
Step 6. Validate the new Users Groups are showing under User Identity Groups.



User Identity Groups

Name	Description
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
Employee	Default Employee User Group
FPR-4110-Admin	User Group for Administrator.
FPR-4110-ReadOnly	User Group for Read Only Users.
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
GuestType_Contractor (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_SocialLogin (default)	Identity group mirroring the guest type
GuestType_Weekly (default)	Identity group mirroring the guest type
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
Radius	

Step 7. Create the local users and add them to their correspondent group. Navigate to the burger icon ≡ **> Administration > Identity Management > Identities > + Add.**

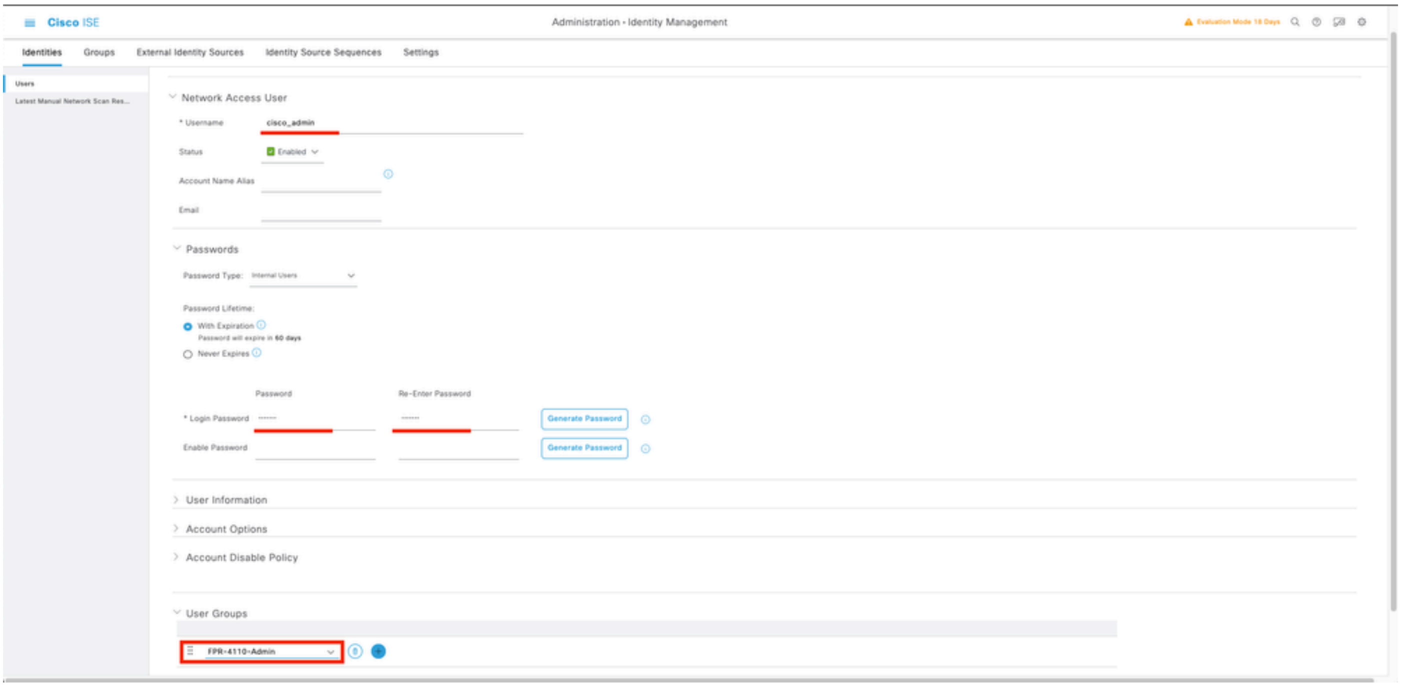


Network Access Users

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin

No data available

7.1 Add the user with Administrator rights. Set a name, password, and assign it to **FPR-4110-Admin,** scroll down and click **Submit** to save the changes.



Cisco ISE
Administration • Identity Management
Evaluation Mode 18 Days
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...

Network Access User

* Username: cisco_admin

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime:

● With Expiration
Password will expire in **60 days**

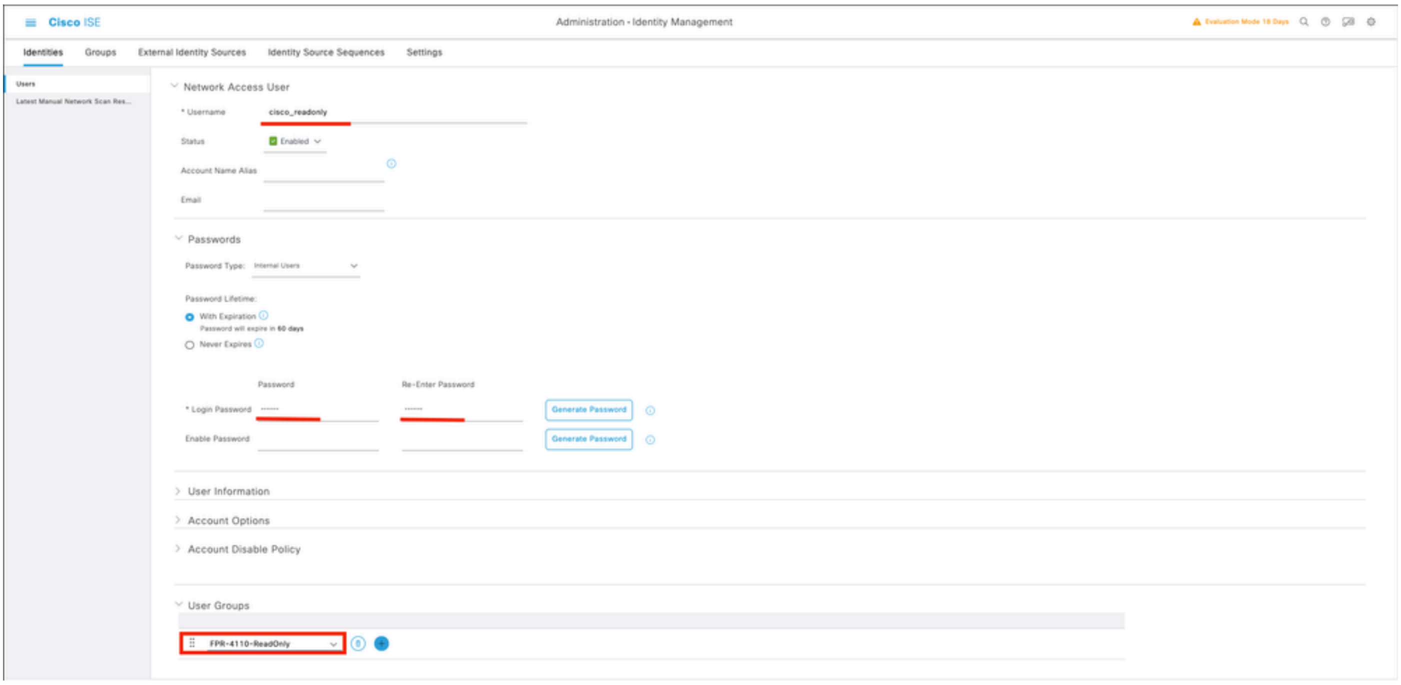
○ Never Expires

	Password	Re-Enter Password
* Login Password	•••••••	•••••••
Enable Password		

User Groups

FPR-4110-Admin

7.2 Add the user with ReadOnly rights. Set a name, password and assign it to **FPR-4110-ReadOnly,** scroll down and click **Submit** to save the changes.



Cisco ISE
Administration • Identity Management
Evaluation Mode 18 Days
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...

Network Access User

* Username: cisco_readonly

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime:

● With Expiration
Password will expire in **60 days**

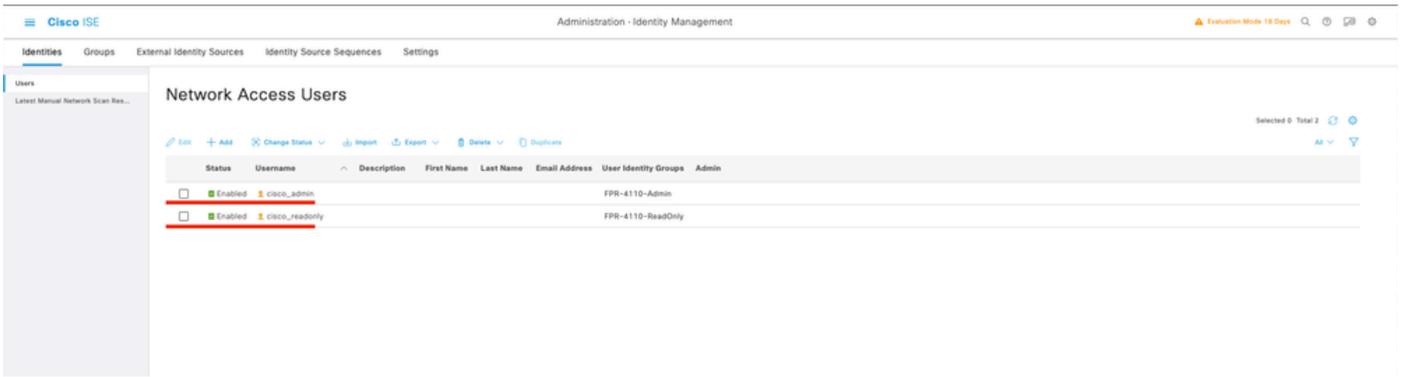
○ Never Expires

	Password	Re-Enter Password
* Login Password	••••••	••••••
Enable Password		

User Groups

FPR-4110-ReadOnly

7.3 Validate the users are under **Network Access Users.**



Network Access Users

	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	Enabled	cisco_admin					FPR-4110-Admin	
□	Enabled	cisco_readonly					FPR-4110-ReadOnly	

Step 8. Create the Authorization Profile for the Admin user.

The FXOS chassis includes the these User Roles:

- Administrator - Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.
- Read-Only - Read-only access to system configuration with no privileges to modify the system state.
- Operations - Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.
- AAA - Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system

Attribuites for each role:

cisco-av-pair=shell:roles="admin"

cisco-av-pair=shell:roles="aaa"

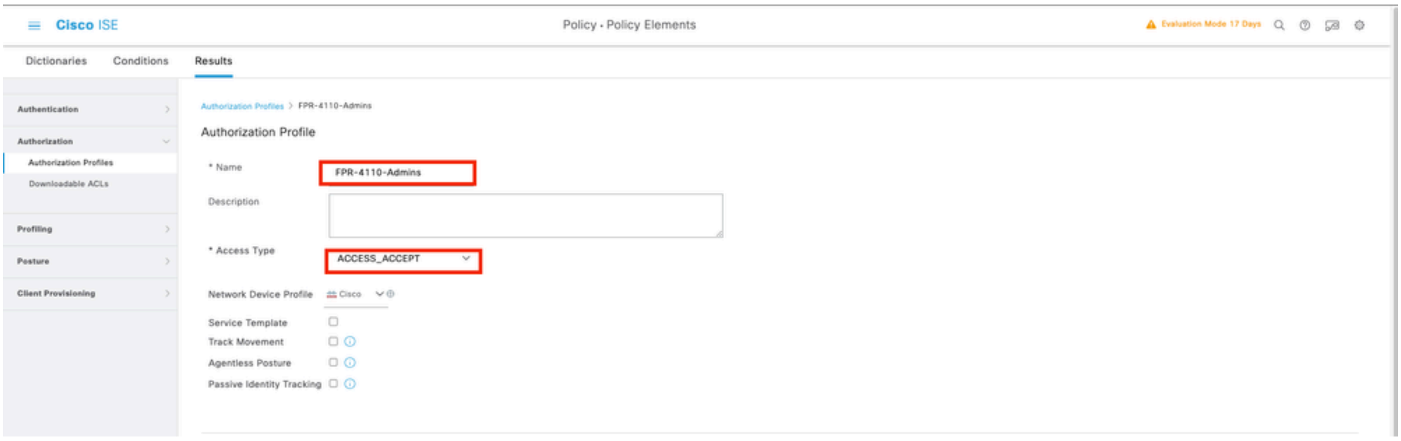
cisco-av-pair=shell:roles="operations"

cisco-av-pair=shell:roles="read-only"

Note: This documentation only defines admin and read-only attributes.

Navigate to burger icon ≡ > **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** > **+Add.**

Define a name for the **Authorization Profile**, leave Access Type as **ACCESS_ACCEPT** and under **Advanced Attributes Settings** add **cisco-av-pair=shell:roles="admin"** with and click **Submit.**



Authorization Profiles > FPR-4110-Admins

Authorization Profile

* Name: FPR-4110-Admins

Description:

* Access Type: ACCESS_ACCEPT

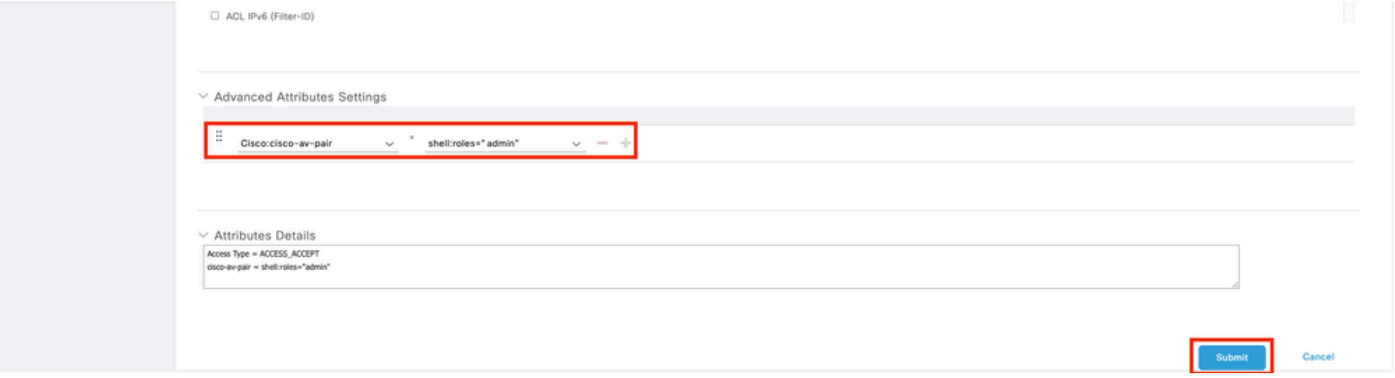
Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □



□ ACL IPv6 (Filter-ID)

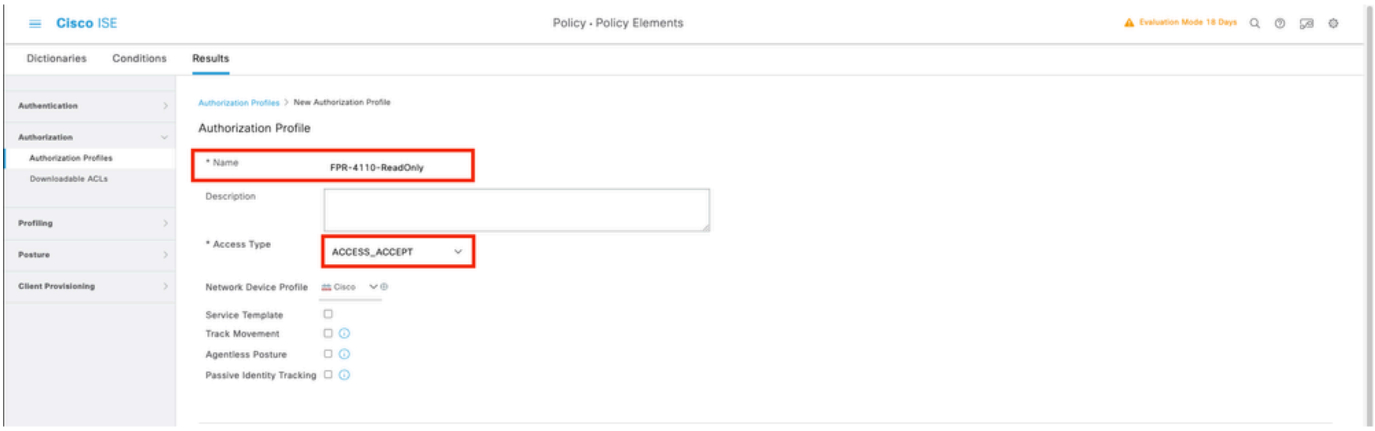
Advanced Attributes Settings

Cisco:cisco-av-pair = shell:roles="admin"

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:roles="admin"
```

8.1 Repeat the previous step to create the Authorization Profile for the ReadOnly User. Create the Radius Class with the value **read-only**instead Administrator this time.



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: FPR-4110-ReadOnly

Description:

* Access Type: ACCESS_ACCEPT

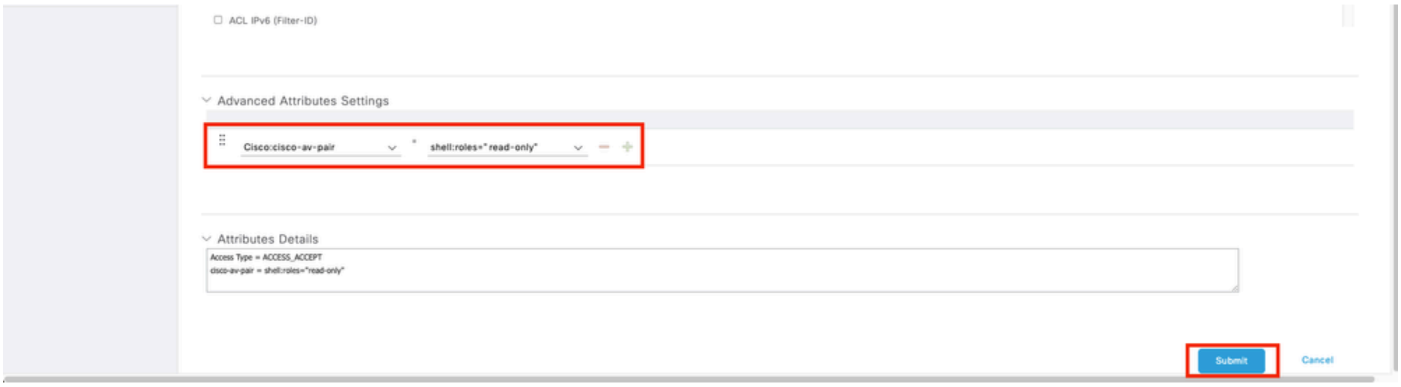
Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □



□ ACL IPv6 (Filter-ID)

Advanced Attributes Settings

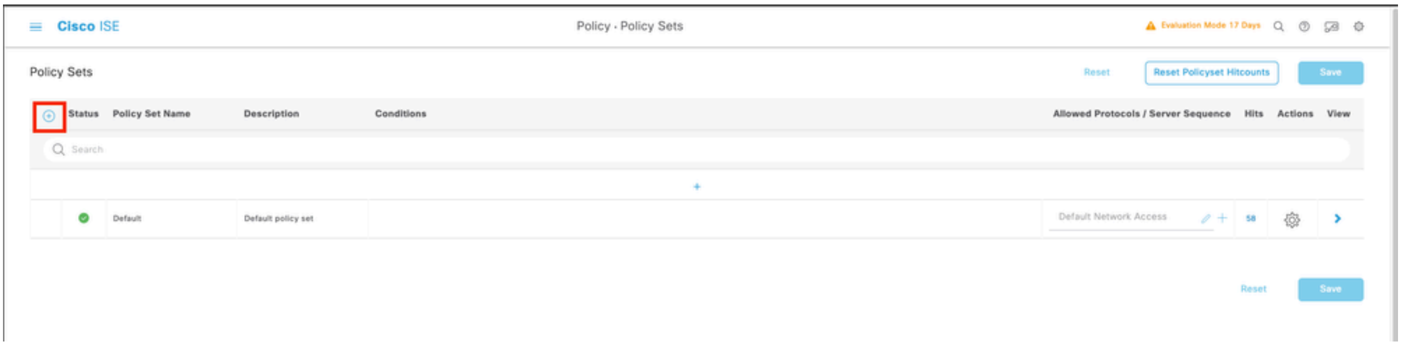
Cisco:cisco-av-pair = shell:roles="read-only"

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = shell:roles="read-only"
```

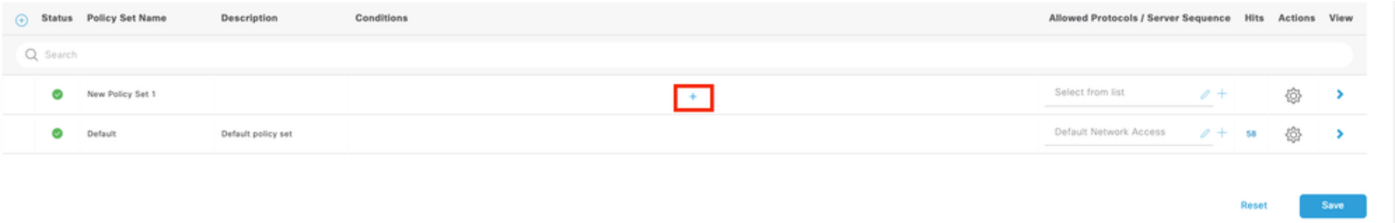
Step 9. Create a Policy Set matching the FMC IP address. This is to prevent other devices from granting access to the users.

Navigate to ☰ > **Policy** > **Policy Sets** >**Add icon sign** at the upper left corner.



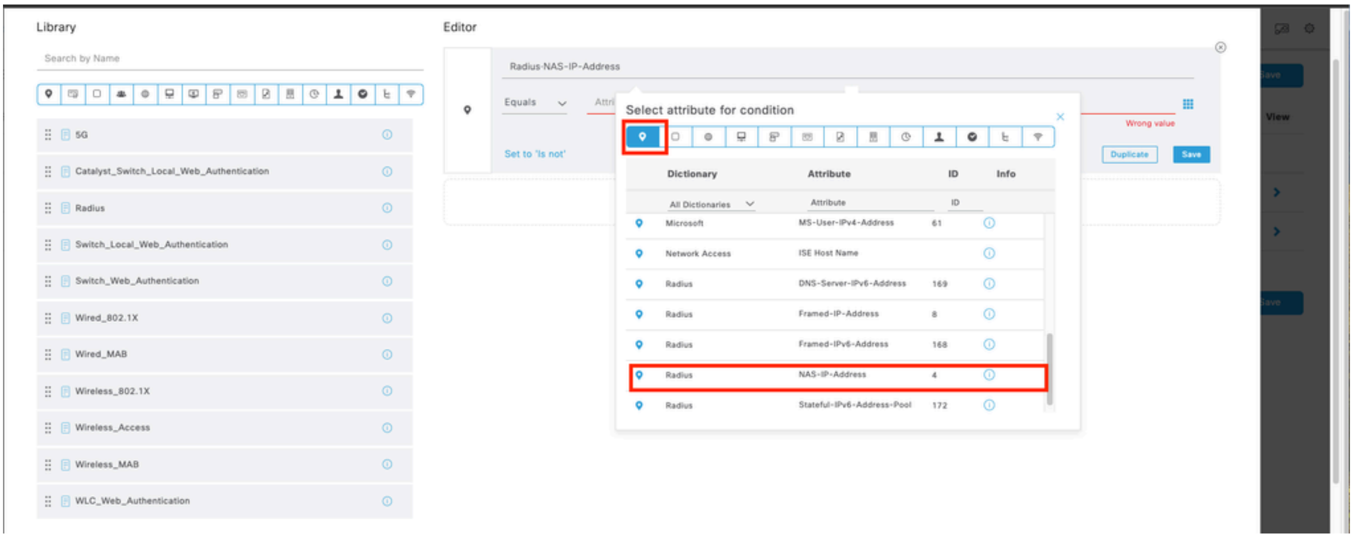
	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	●	Default	Default policy set		Default Network Access	58	⚙	>

9.1 A new line is placed at the top of your Policy Sets. Click the **Add icon** to configure a new condition.

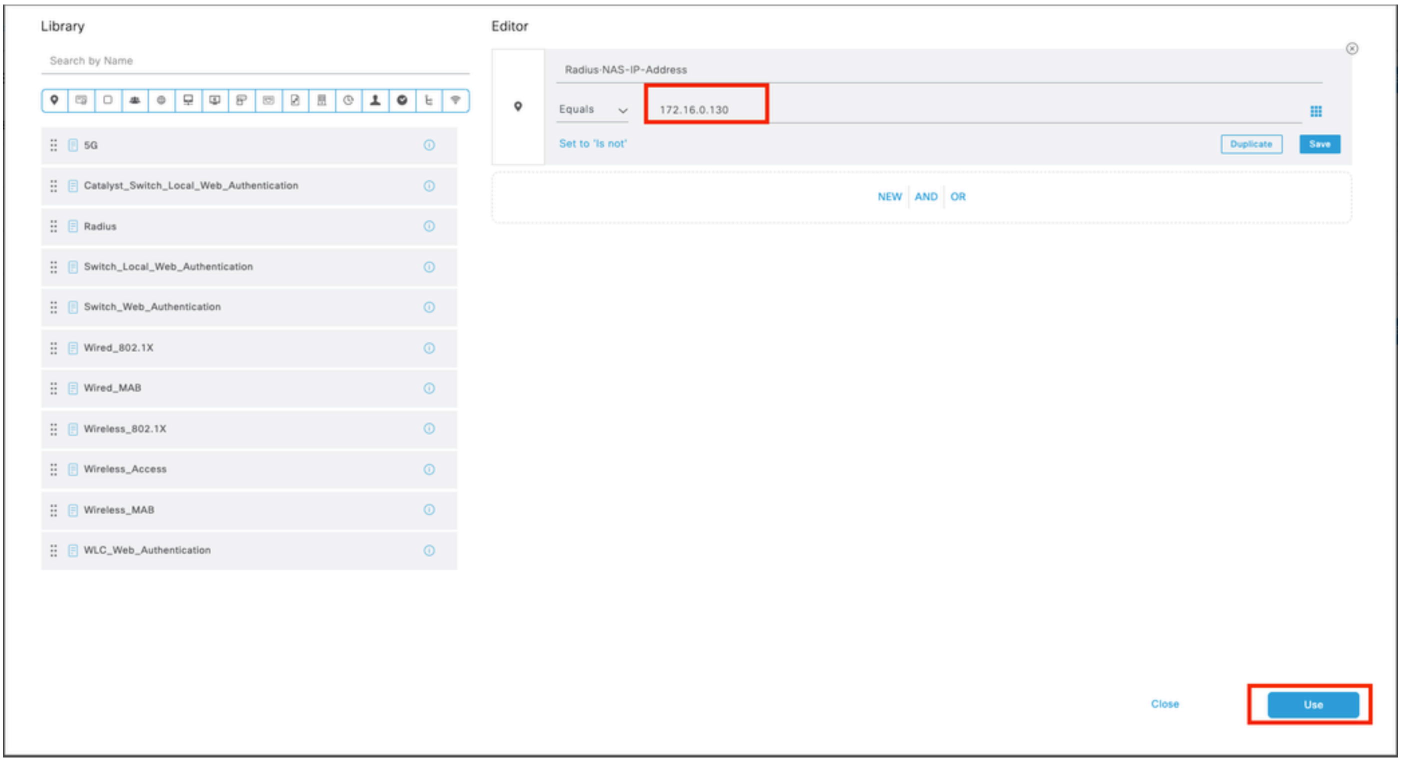


	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	●	New Policy Set 1		+	Select from list		⚙	>
	●	Default	Default policy set		Default Network Access	58	⚙	>

9.2 Add a top condition for**RADIUS NAS-IP-Address**attribute matching the FCM IP address, then click **Use.**



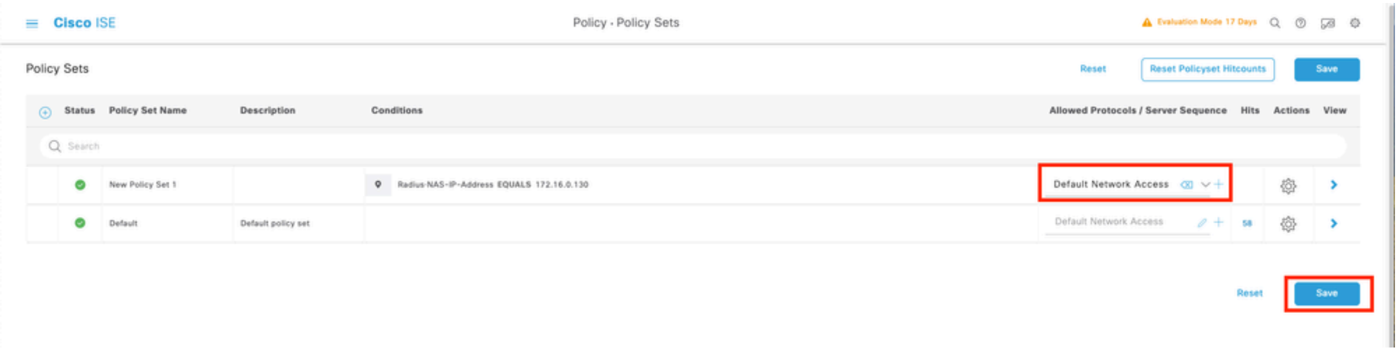
Dictionary	Attribute	ID	Info
Microsoft	MS-User-IPv4-Address	61	ⓘ
Network Access	ISE Host Name		ⓘ
Radius	DNS-Server-IPv6-Address	169	ⓘ
Radius	Framed-IP-Address	8	ⓘ
Radius	Framed-IPv6-Address	168	ⓘ
Radius	NAS-IP-Address	4	ⓘ
Radius	Stateful-IPv6-Address-Pool	172	ⓘ



5G
Catalyst_Switch_Local_Web_Authentication
Radius
Switch_Local_Web_Authentication
Switch_Web_Authentication
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_Access
Wireless_MAB
WLC_Web_Authentication

Radius·NAS-IP-Address
Equals 172.16.0.130

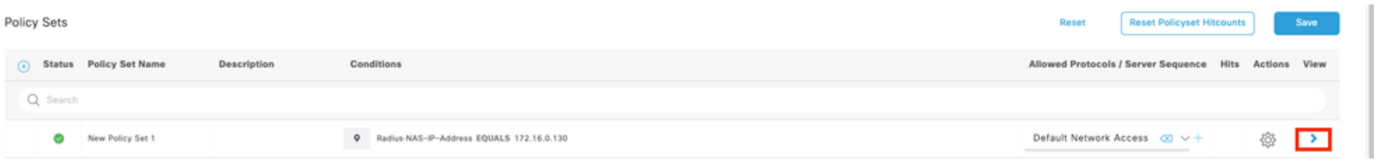
9.3 Once completed, click **Save**.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	New Policy Set 1		Radius·NAS-IP-Address EQUALS 172.16.0.130	Default Network Access		⚙	>
●	Default	Default policy set		Default Network Access	58	⚙	>

Tip: For this exercise we have allowed the Default Network Access Protocols list. You can create a new list and narrow it down as needed.

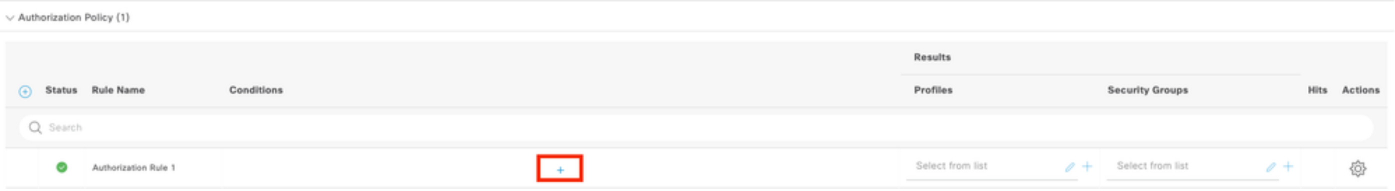
Step 10. View the new Policy Set by hitting the >icon placed at the end of the row.



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	New Policy Set 1		Radius-NAS-IP-Address EQUALS 172.16.0.130	Default Network Access		⚙	>

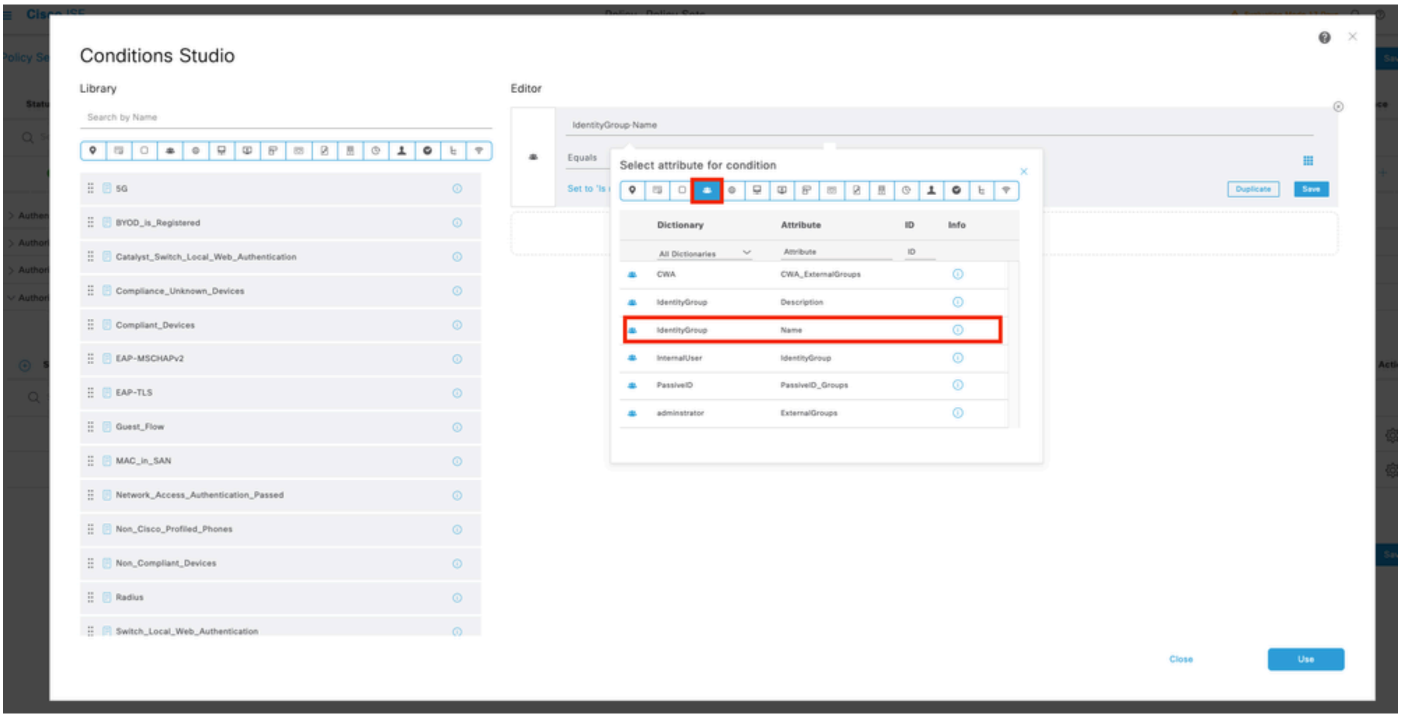
10.1 Expand the **Authorization Policy** menu and click in **(+)** to add a new condition.



Authorization Policy (1)

	Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
	●	Authorization Rule 1	+	Select from list	Select from list		⚙

10.2 Set the conditions to match the Dictionary**Identity Group**with Attribute**Name Equals User Identity Groups: FPR-4110-Admins**(the group name created in Step 7) and click**Use**.



Conditions Studio

Library

Editor

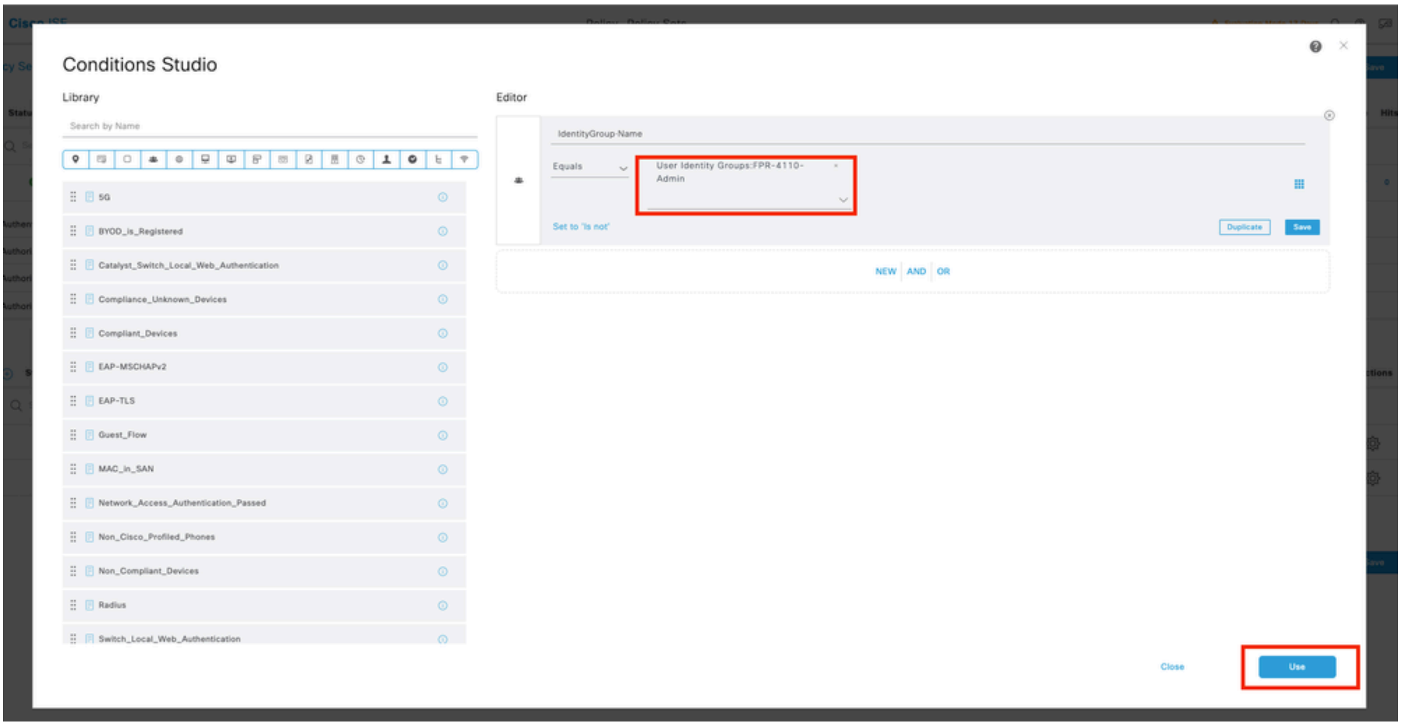
IdentityGroup·Name

Equals

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
CWA	CWA_ExternalGroups		ⓘ
IdentityGroup	Description		ⓘ
IdentityGroup	Name		ⓘ
InternalUser	IdentityGroup		ⓘ
PassiveID	PassiveID_Groups		ⓘ
adminstrator	ExternalGroups		ⓘ

Search by Name
5G
BYOD_is_Registered
Catalyst_Switch_Local_Web_Authentication
Compliance_Unknown_Devices
Compliant_Devices
EAP-MSCHAPv2
EAP-TLS
Guest_Flow
MAC_in_SAN
Network_Access_Authentication_Passed
Non_Cisco_Profiled_Phones
Non_Compliant_Devices
Radius
Switch_Local_Web_Authentication
Duplicate
Save
Close
Use



Conditions Studio

Library

Editor

IdentityGroup·Name

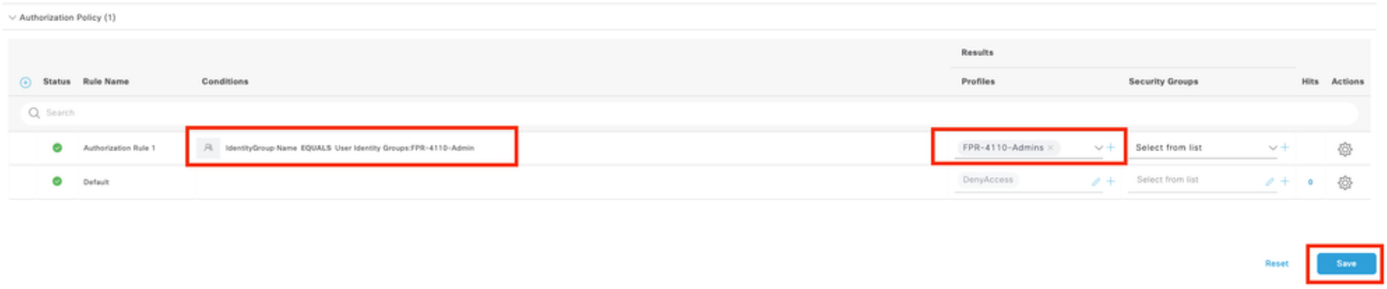
Equals

User Identity Groups:FPR-4110-Admin

Set to 'Is not'

Search by Name
5G
BYOD_is_Registered
Catalyst_Switch_Local_Web_Authentication
Compliance_Unknown_Devices
Compliant_Devices
EAP-MSCHAPv2
EAP-TLS
Guest_Flow
MAC_in_SAN
Network_Access_Authentication_Passed
Non_Cisco_Profiled_Phones
Non_Compliant_Devices
Radius
Switch_Local_Web_Authentication
Duplicate
Save
NEW
AND
OR
Close
Use

Step 10.3 Validate the new condition is configured in the **Authorization policy**, then add a User profile under **Profiles.**



Authorization Policy (1)

Status	Rule Name	Conditions	Results Profiles	 Security Groups	Hits	Actions
✓	Authorization Rule 1	IdentityGroup·Name EQUALS User Identity Groups:FPR-4110-Admin	FPR-4110-Admins	Select from list		
✓	Default		DenyAccess	Select from list	0	

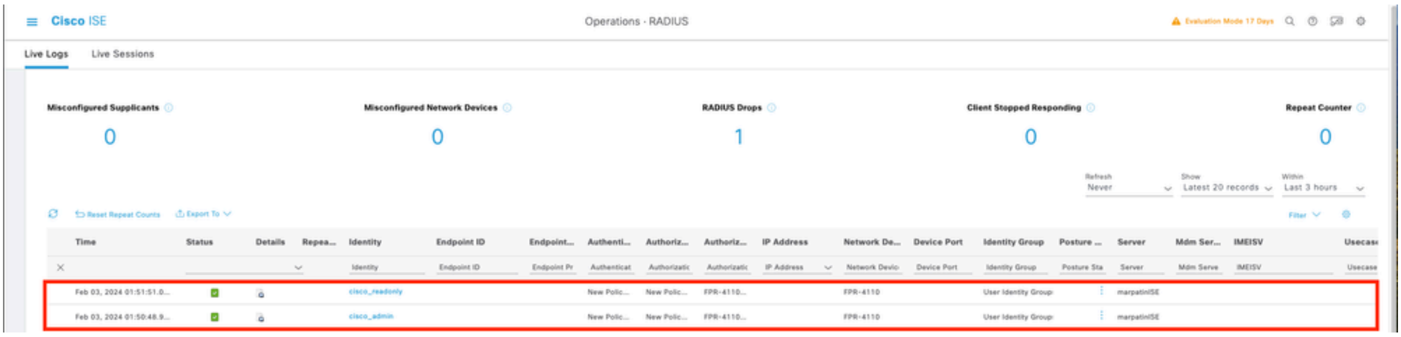
Step 11. Repeat the same process in **step 9** for **Read-only** Users and click **Save.**

Verify

1. Attempt to log into the FCM GUI using the new Radius credentials

2. Navigate to burger icon ☰ > **Operations** > **Radius** > **Live logs**.

3. The information displayed shows if a user logged successfully.

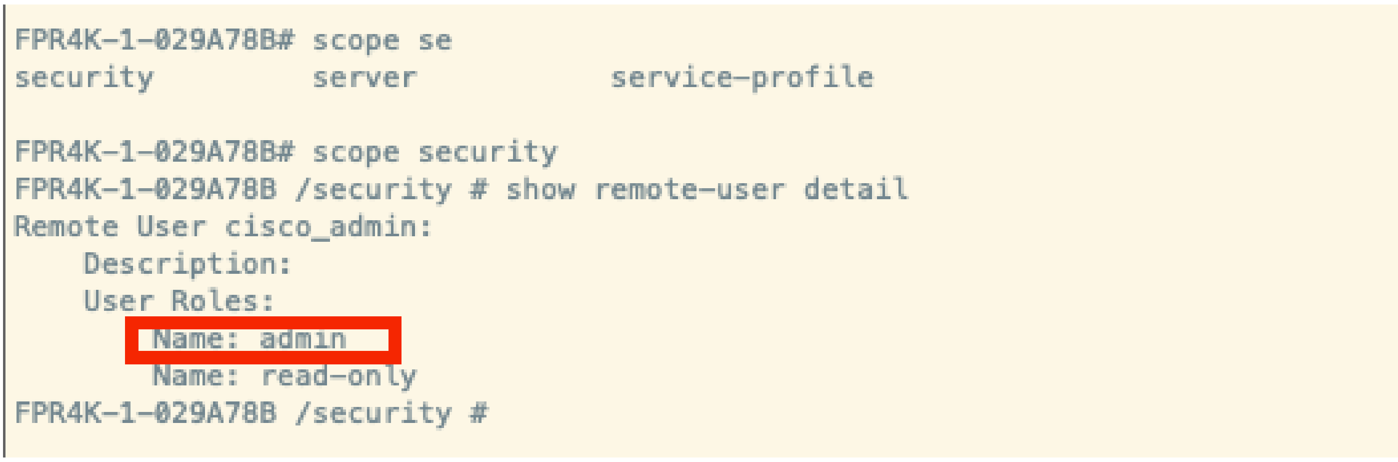


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	1	0	0

Refresh: Never · Show: Latest 20 records · Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Ser...	IMEISV	Usecase
Feb 03, 2024 01:51:51.0...	✓			cisco_readonly			New Polic...	New Polic...	FPR-4110...		FPR-4110		User Identity Group		marpatinISE			
Feb 03, 2024 01:50:48.9...	✓			cisco_admin			New Polic...	New Polic...	FPR-4110...		FPR-4110		User Identity Group		marpatinISE			

4. Validate Logged users role from Secure Firewall Chassis CLI.



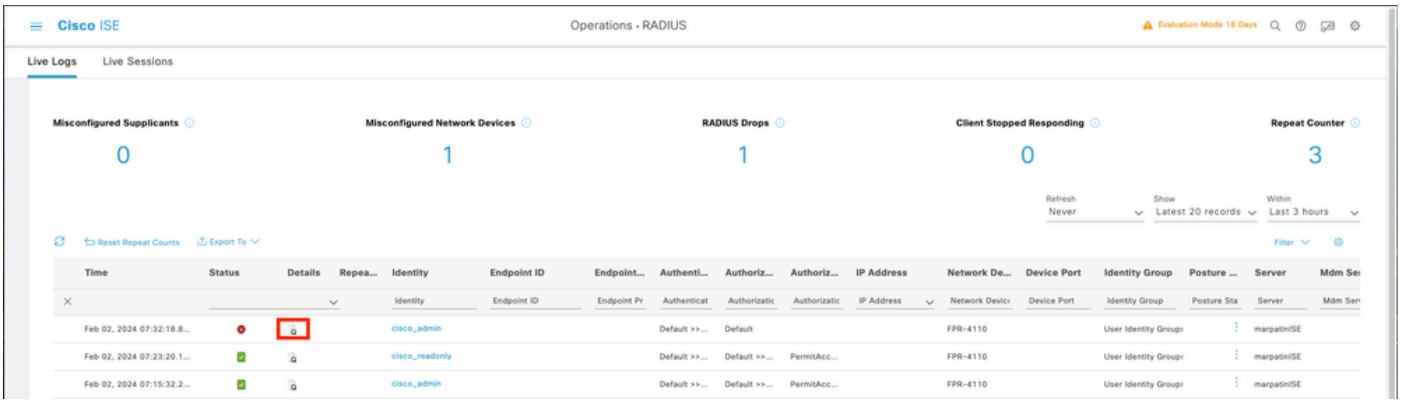
```
FPR4K-1-029A78B# scope se
security          server            service-profile

FPR4K-1-029A78B# scope security
FPR4K-1-029A78B /security # show remote-user detail
Remote User cisco_admin:
    Description:
    User Roles:
        Name: admin
        Name: read-only
FPR4K-1-029A78B /security #
```

Troubleshoot

1. Over ISE GUI , Navigate to burger icon **≡ > Operations > Radius > Live logs.**

1.1 Validate if the log session request is reaching to the ISE node.
1.2 For failed status review the details of the session.



Misconfigured Supplicants: 0
Misconfigured Network Devices: 1
RADIUS Drops: 1
Client Stopped Responding: 0
Repeat Counter: 3

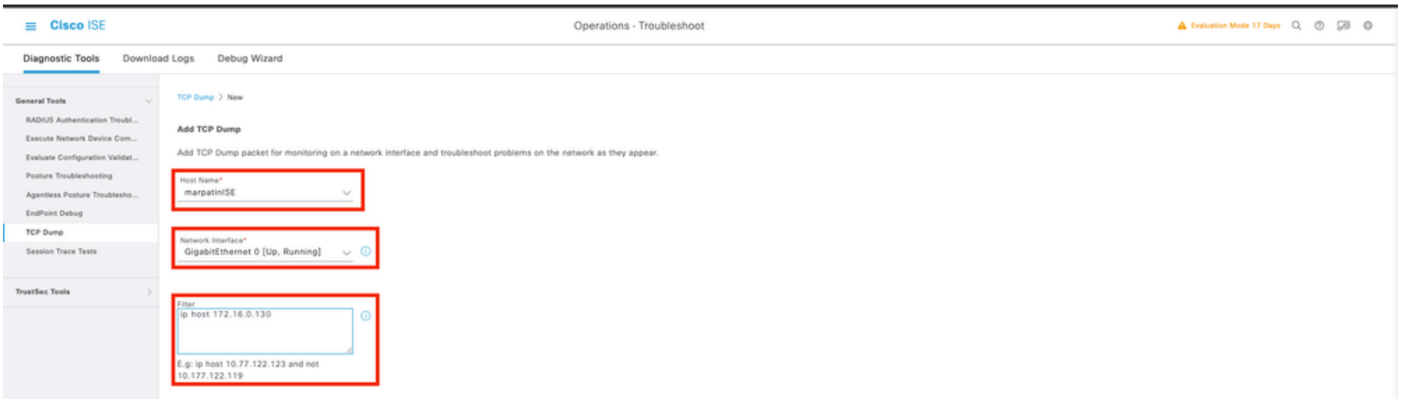
Refresh: Never
Show: Latest 20 records
Within: Last 3 hours

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server	Mdm Se
Feb 02, 2024 07:32:18.8...	✖			cisco_admin			Default >>...	Default			FPR-4110		User Identity Group:	⋮	marpatinISE	
Feb 02, 2024 07:23:20.1...	✓			cisco_readonly			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group:	⋮	marpatinISE	
Feb 02, 2024 07:15:32.2...	✓			cisco_admin			Default >>...	Default >>...	PermitAcc...		FPR-4110		User Identity Group:	⋮	marpatinISE	

2. For requests not showing in Radius Live logs , review if UDP request is reaching the ISE node through a packet capture.

Navigate to burger icon ≡ > **Operations** > **Troubleshoot** > **Diagnostic Tools** > **TCP dump**. Add a new capture and download the file to your local machine in order to review if the UDP packets are arriving to the ISE node.

2.1 Fill the requested information, scroll down and click **Save.**



Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

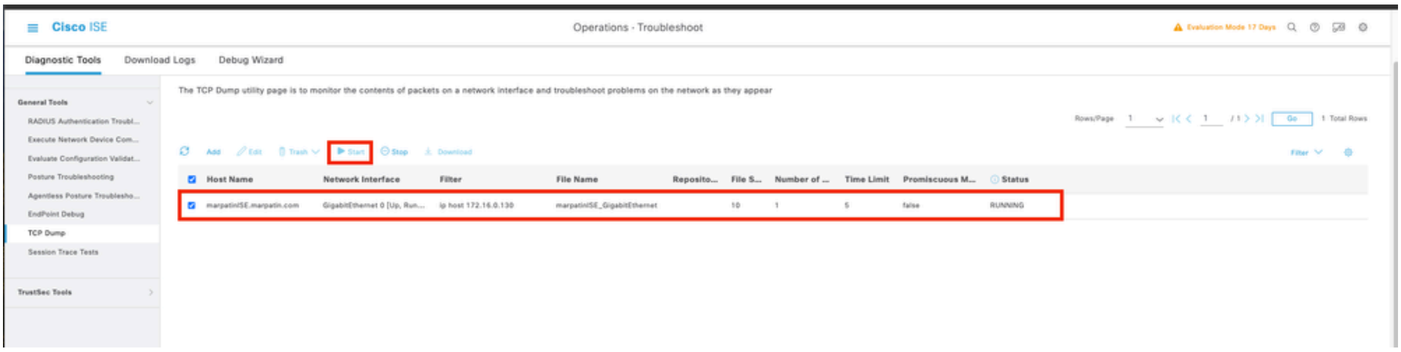
Host Name*: marpatinISE

Network Interface*: GigabitEthernet 0 [Up, Running]

Filter: ip host 172.16.0.130

E.g: ip host 10.77.122.123 and not 10.177.122.119

2.2 Select and Start the capture.



The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

☑	Host Name	Network Interface	Filter	File Name	Reposito...	File S...	Number of ...	Time Limit	Promiscuous M...	Status
☑	marpatinISE.marpatin.com	GigabitEthernet 0 [Up, Run...	ip host 172.16.0.130	marpatinISE_GigabitEthernet		10	1	5	false	RUNNING

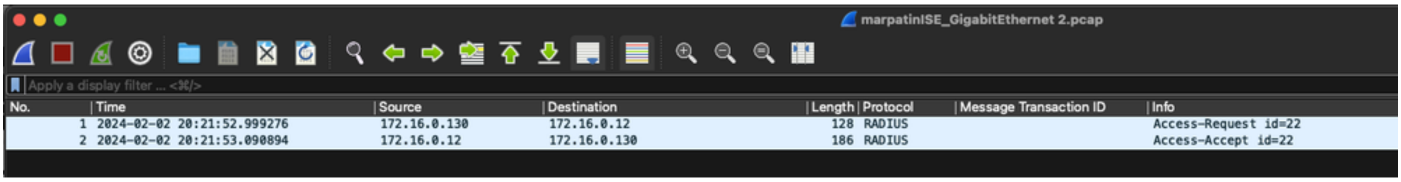
2.3 Attempt to log to the Secure Firewall Chassis while the ISE capture is running

2.4 Stop the TCP Dump in ISE and download the file to a local machine.

2.5 Review traffic output.

Expected output:

Packet No1. Request from the Secure Firewall to the ISE server through Port 1812 (RADIUS)
Packet No2. ISE server reply accepting the inital request.


marpatinISE_GigabitEthernet 2.pcap
Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Length	Protocol	Message Transaction ID	Info
1	2024-02-02 20:21:52.999276	172.16.0.130	172.16.0.12	128	RADIUS		Access-Request id=22
2	2024-02-02 20:21:53.090894	172.16.0.12	172.16.0.130	186	RADIUS		Access-Accept id=22