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**

verview Interfaces Logical De	evices Security Engine Platform	Settings				System	Tools Help admi
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 しの							
Network Module 1 Image: Sinsole MGMT USB Power 1 - Running Power 2 - Removed							
FAULTS 3(3) 0(0) © CRITICAL ▲ MAJOR	INTERFACES 3 5 OWN (* UP	INSTANCES O O DOWN	1 ⑦ UP	Smart Agent	INVENTORY 1(1) Security Engine	6(6) ☆ Fans a	1(2) Power Supplies
Select All Faults Cancel Selected Faults	Acknowledge				k		
Severity Description			Cause	Occurrence	Time		Acknowledged
CRITICAL FPGA version	lower than 2.00 is detected. A critical upgrad	le from the firmwar	fpga-upgrade-require	ed 1	2022-02-20T22	32:45.641	no 👔
CRITICAL Network Mod	ule 3 removed when in online state. It is recon	mmended to set m	module-suprise-remo	val 1	2022-11-07T09	:03:02.022	no
Successful Login in last 24 hrs - <u>View Details</u> T	Thu Feb 01 2024 at 17:00:55 from - 172.16.0.35						ابیاب cisco

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

Overview Interfaces Logica	al Devices Security Engine	Platform Settings		System	n Tools Help admin
NTP	LDAP RADIUS TACACS				
SSH					
SNMP	Properties				
HTTPS	Timeout:* 5 Secs				
► AAA					
Syslog	Retries:* 1				
DNS	RADIUS Providers				
FIPS and Common Criteria					Add
Access List			a sector	A	
MAC Pool	Hostname	Order	Service	Auth Port	
Resource Profiles					
Network Control Policy					
Chassis URL					
Save Cancel					
					ale ale
8 Successful Login in last 24 hrs - View De	tails Thu Feb 01 2024 at 17:00:55 from	- 172.16.0.35			cisco

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

Overview Interfaces Logi	cal Devices Security Engine	Platform Settings			System Tools Help admin
NTP SSH SNMP HTTPS	LDAP RADIUS TACACS Properties Timeout.* 5 Secs	1			
AAA Syslog DNS FIPS and Common Criteria Access List	Retries:* 1 RADIUS Providers	Add RADIUS Provider Hostname/FQDN/IP Address:* Order:*	172.16.0.12 lowest-available		Add
MAC Pool Resource Profiles Network Control Policy Chassis URL	rostname	Key: Confirm Key: Authorization Port:* Timeout:*	••••••• ••••••• 1812 5	Set: No	
	Save Cancel	Retries.*	1	Cancel	
8 Successful Login in last 24 hrs - <u>View</u>	Details Thu Feb 01 2024 at 17:00:55 fr	om - 172.16.0.35			ոլիսիս cisco

Step 5. Navigate to System > User Management

Overview Interfaces Logic	al Devices Security Engine	Platform Settings		Sys	tem ⁴)Tools Help admir
			Configuratio	on Licensing Upd	ates User Managemen
SSH					_
SNMP	Properties				
HTTPS	Timeout:* 5 Secs				
► AAA	Patriar 1				
Syslog					
DNS	RADIOS Providers				
FIPS and Common Criteria					Add 📀
Access List	Hostname	Order	Service	Auth Port	
MAC POOL	172.16.0.12	1	authorization	1812	28
Network Control Policy					a
Chassis URI					
CHOSSIS ONE					
	2				
	Save Cancel				
	إكستار السار				
					ala al
vascript:void(0) last 24 hrs - View [Details Thu Feb 01 2024 at 17:00:55 fr	rom - 172.16.0.35			cisco

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

Overview Interfaces Logica	al Device	es Security Engine Platform Settings			System	Tools Help admin
			Configuration	Licensing	Updates	User Management
Local Users Settings						
Default Authentication	Local Local	*Local is fallback authentication method				
Console Authentication	RADIUS LDAP	• -				
Remote User Settings	TACACS	;				
Remote User Role Policy	None	No-Login				
Local User Settings						
Password Strength Check	Enab	le				
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 De	<u>etails</u> Thu	Feb 01 2024 at 17:00:55 from - 172.16.0.35				cisco



Note: FCM configuration has finish at this point.

Identity Service Engine

Step 1. Add a new Network Device.

Navigate to the burger icon \equiv 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.

🔳 Cisco ISE	Administration - Network Resources	A Evaluation Mode 18 Days	9.0	58 Q	- 1
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM pxOrid Direct Connectors Location Services				
Network Devices Default Device Device Security Settings	Network Devices List > New Network Device Notwork: Devices				
	Name 799-4110 Description				
	H Address ∨ *P: 122.16.6.130 I 32 O				
	Device Protise 🕮 Cisco 👻 🕐				
	Model Name 596-4110 V				
	Software Version 2.12 V				
	Location All Locations 🗸 Set To Default				
	IPSEC Is IPSEC Device v Set To Default				
	Device Types V Set To Default				
	RADIUS Authentication Settings				
	RADIUS UDP Settings				
	Protocol RADIUS				
	Shared Secret				
	Second Shared Show				

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

	Administration - Network Resources			A Evaluation Mode 18 Days Q	Ø 6
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Serve	Sequences NAC Managers	External MDM	pxGrid Direct Connectors More \vee	
Network Devices					
Default Device	Network Devices				
Device Security Settings				Selected 0 Total 1 🧭	٢
	🖉 Edit 🕂 Add 🚺 Duplicate 🕁 Import 🏝 Export 🗸 🛆 Generate PAC 🌘 Delete 🗸			At 🗸	∇
	□ Name ∧ IP/Mask Profile Name Location Typ	B Description			
	□ FPR-4110 172.16.0	Jevice 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

E Cisco ISE	Administration - Identity Management	🔺 Evaluation Mode 18 Days 🔍 🕥 👼 🗔
Identities Groups External Iden	tity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 12 0		Selected 0 Total 9 😥 💿
> Endpoint Identity Groups	🖉 Edit 🕂 Add 🚺 Delete 🗸 🕁 Import 🖒 Export 🗸	All \sim $~$ ∇
> 🛅 User Identity Groups	Name Description	
	C & ALL_ACCOUNTS (default) Default ALL_ACCOUNTS (default) User Group	
	Default Employee User 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 Exte	Innal Identity Sources Identity Source Sequences Settings	
SQ < SB > Endpoint identity Groups > User identity Groups	Ver ldentity Groups > New User Identity Group User Group for Administrator. Description	Cancel

5.1 Repeat the same process for ReadOnly users.

=	Cisco ISE	Administration - Identity Management	🛦 Evaluation Mode 18 Days Q 💿 🕫 🔅
Ide	ntities Groups External Iden	tity Sources Identity Source Sequences Settings	
	SQ C SS C SS	User Identity Groups > New User Identity Group Identity Group * Name FPR-4110-ReadOnly User Group for Read Only Users. Description	Submit

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

E Cisco ISE	Administration - Identity Management	🛕 Evaluation Mode 18 Days Q 🛞 🖽 🕻
Identities Groups External Ide	ntity Sources Identity Source Sequences Settings	
Identity Groups	User Identity Groups	
< 12 O		Selected 0 Total 11 📿 🔕
> 🛅 Endpoint Identity Groups	🖉 Edit 🕂 Add 🏮 Delete 🗸 🕁 Import 🖒 Export 🗸	$_{ m All}$ \sim γ
> 🛅 User Identity Groups	Name Description	
	ALL_ACCOUNTS (defauit) Defauit ALL_ACCOUNTS (defauit) User Group	
	Default Employee User Group	
	C & FPR-4110-Admin User Group for Administrator.	
	KFR-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	
	destType_SocialLogin (default) Identity group mirroring the guest type	
	CuestType_Weekly (default) Identity group mirroring the guest type	
	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.



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.

E Cisco ISE		Administration - Identity Management	🛦 Evaluation Mode 18 Days Q. 💿 🕼 💿
Identities Groups Ext	ernal Identity Sources Identity Source Sequences Settings		
Ukrat	V Network Access User Usename Usename Cisco_admin Status Cisco_admin Acceut Name Alas Cisco Acceut Name Alas Cisc		
	Passeoid Re-Enter Passeoid Login Passeoid	Generate Pasaword Image: Constrate Pasaword Image: Constrate Pasaword Image: Constrate Pasaword	

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.

E Cisco ISE	Administration - Identity Management	🛦 Evaluation Mode 18 Days Q. 🛞 🕼 🕼
Identities Groups External Identity Sources Identity Source Sequences Settings		
Users Network Access User Usersame Usersame Cisco,readonty Account Name Alas Email Email 		
Vever Expires Never Expires Never Expires		
Passend Re-Enter Passend * Login Passend * Login Passend * Login Passend * Login Passend * User Information > User Information > Account Options > Account Disable Policy	Osciente Password O Osciente Password O	
✓ User Groups E #PR-4110-ReadOny <> ③ ●		

7.3 Validate the users are under Network Access Users.

	Adr.	nicistration - Identity Management	A Featurities Mode 18 Days O	0.02.0
L CISCO ISE	Phot	minasassi - soning minageninin	-	, 90 Q
Identities Groups Exte	nal Identity Sources Identity Source Sequences Settings			
Users				
Latest Manual Network Scan Res	Network Access Users			
			Selected 0 Total 2	0 0
	🖉 Em 🕂 Add 🛞 Change Status 🗸 🦽 Import 🖄 Export 🗸 🐧 Depters 🖉 Depters		A4	~ V
	Status Username	tress User Identity Groups Admin		
	Enabled 1 cisco_admin	FPR-4110-Admin		
	Enabled 1 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**.

= Cisco ISE	Policy - Policy Elements	Evaluation Mode 17 Day	• Q (2 50	٥
Dictionaries Conditions	Results				
Authentication >	Authorization Profile Authorization Profile				
Authorization Profiles	* Name EOB_d110_Admine				
Downloadable ACLs	Description				
Profiling >					
Posture	ACCESS_ACCEPT V				
Client Provisioning	Network Device Profile				
	Service Template				
	Agenties Posture				
	Passive identity Tracking 🗌 🕜				
					_
	ACL IPv6 (Fitter-ID)				
	Advanced Attributes Settings				
	Ecisco.cisco-av-pair v * sheit.roles**admin* v = +				
	Attributes Details				
	Acces type + ACCES, JACCEPT dtcp-tw-par + sh-dtrides*admet*				
		Submit		Cancel	

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.

Cisco ISE	Policy - Policy Elements	Evaluation Mode 18 Days	105	2 ¢
Dictionaries Conditions	Results			
Authentication	Authorization Profile > New Authorization Profile Authorization Profile			
Authorization Profiles Downloadable ACLs	* Name FPR-4110-ReadOnly			
Profiling >	Description			
Posture >	* Access Type ACCESS_ACCEPT ~			
Client Provisioning	Network Device Profile Service Template Track Movement Agentiess Posture Passive Identity Tracking O			
	ACL IPv6 (Fitter-ID)			
	Advanced Attributes Settings			
	E <u>Cisco:cisco-av-pair</u> v * shelt:roles=*read-only* v = +			
	- Attributes Details Acces Type = ACCES, ACCEPT dece-ar-par = dedicades="read-only"			
		Submit	Cance	a

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 \equiv > Policy > Policy Sets >Add icon sign at the upper left corner.

=	Cisco I	SE			Policy · Policy Sets	A Evaluation Mode	17 Days	۵ ۵	9 ¢
Polic	cy Sets					Reset Reset Policyset	Hitcounts		Save
۲	Status	Policy Set Name	Description	Conditions		Allowed Protocols / Server Sequence	Hits	Actions	View
0	Q Search								
					+				
	٥	Default	Default policy set			Default Network Access 🧳 🖉 +	58		>
							Reset		Save

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

Q. Search				
New Policy Set 1	n list 🥒 🕂		<u>ې</u>	•
Default Default palicy set	twork Access 🥒 🚽	58	\$	>

Save

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

Library	Editor										53 Ø
Search by Name ● □ ● □ □ ● □ □ ● □ □ ● □ □ ● □ □ ● □ □ ● □ □ ● □ □ ● □	0	Radius-NAS-IP-Address Equals v Attri	Sele	ct attribute for conditio	0					8	lave
∷ 🖪 5G 📀		Cot to 'le cot'	•	0 0 9 8	8 8 8 C	T	0 E	₹	Wrong value		View
: [] Catalyst_Switch_Local_Web_Authentication		Set to is not		Dictionary	Attribute	ID	Info		Dupicace		
# 🗄 Radius 🛈				All Dictionaries ~	Attribute MS-User-IPv4-Address	1D					<u> </u>
: E Switch_Local_Web_Authentication			•	Network Access	ISE Host Name		0				<u> </u>
: B Switch_Web_Authentication			۰	Radius	DNS-Server-IPv6-Address	169	0				
# E Wired_802.1X			۰	Radius	Framed-IP-Address	8	0				Save
: 🔋 Wired_MAB 📀			۰	Radius	Framed-IPv6-Address	168	0				
: E Wireless_802.1X O			•	Radius	NAS+IP+Address	4	0	η.			
# E Wireless_Access			•	Radius	Stateful-IPv6-Address-Pool	172	0				
# E Wireless_MAB											
E WLC_Web_Authentication											

Library	Editor			
Search by Name		Radius-NAS-IP-Address		8
• •	۰	Equals v 172.16.0.130		
∷ 🖪 5G 💿		Set to 'Is not'	Duplicate	Save
:: [] Catalyst_Switch_Local_Web_Authentication		NEW AND OR		
🗄 🖹 Radius 🕕				
:: [] Switch_Local_Web_Authentication				
: [] Switch_Web_Authentication				
:: E Wired_802.1X ()				
: E Wired_MAB ()				
: [] Wireless_802.1X ()				
: B Wireless_Access				
E Wireless_MAB				
: [] WLC_Web_Authentication ①				
			Close	Use

9.3 Once completed, click Save.

≡ C	isco IS	SE		Policy - Policy Sets		A Evaluation N	iode 17 Dr	/ays ()	ک ک	6 R
Policy	Sets				Reset	Reset Policy	set Hitco	ounts		Save
۲	Status	Policy Set Name	Description	Conditions	Allowed Protoco	ls / Server Sequ	ence F	Hits A	Actions	View
Q	Search									
	۰	New Policy Set 1		Radius NAS-IP-Address EQUALS 172.16.0.130	Default Networ	k Access 🛛 🛇	×+		(2)	>
	۰	Default	Default policy set		Default Network	Access 🥖	+ ,	58	②	>
							R	leset		Save



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			Reset Policyset Hitcounts		Save
(+) Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence Hits	Actions	View
Q Search					
New Policy Set 1		Radius NAS-IP-Address EQUALS 172.16.0,130	Default Network Access 🛛 🗸 +	٥	>

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

\vee	Authorization R	Policy (1)						
					Results			
	 Status 	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
	Q Search							
	۰	Authorization Rule 1		+	Select from list	+ Select from list	0 +	(2)

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**.

Library		Editor									
Search by Name			Identity	iroup-Na	me						
) 10 E T	*	Equals	Sele	ct attribute for condition	on		×			
:: 🕑 56			Set to 'Is	•	3 0 • 9 9	Q 8 8 8 8	0 1	О Е 🕈		Duplicate	Save
🗄 🔡 BYOD_is_Registered					Dictionary	Attribute	ID	Info			
# Catalyst_Switch_Local_Web_Authentication					All Dictionaries V	Attribute	ID				
: Compliance_Unknown_Devices				-	IdentityGroup	Description		0			
E Compliant_Devices					IdentityGroup	Name		0			
EAP-MSCHAPv2					InternalUser	IdentityGroup		0			
🗄 📑 EAP-TLS					PassiveID	PassiveID_Groups		0			
🗄 📋 Guest_Flow				•	administrator	ExternalGroups		0			
🗄 📑 MAC_in_SAN											
E Network_Access_Authentication_Passed											
E Non_Cisco_Profiled_Phones											
Non_Compliant_Devices											
🗄 📋 Radius											
Switch_Local_Web_Authentication											

Co. 195			Dollar: Dollar: Cote A C-1 stores		
Conditions Studio				0	×
Library		Editor			
Search by Name			IdentityGroup Name	۲	- 1
 ♥ ♥	£ 🕈		Equals Vuer Identity Groups:FPR-4110- + Admin		
ii 🗄 sa		-			
H BYOD_is_Registered			Set to 'is not' Duplicate	Save	
# Catalyst_Switch_Local_Web_Authentication			NEW AND OR		
E Compliance_Unknown_Devices					
# 🕑 Compliant_Devices					
EAP-MSCHAPv2					
🗄 🖪 EAP-TLS					
: Duest_Flow					10
II 🗄 MAG_In_SAN					1
Intwork_Access_Authentication_Passed					
: [] Non_Cisco_Profiled_Phones					
Ison_Compliant_Devices					
🗄 [] Radius					
I Switch_Local_Web_Authentication	0				_
			Close	Use	
1					_

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

under Profiles.

\sim Authorization Policy (1)					
		Results			
• Status Rule Name	Conditions	Profiles	Security Groups	Hit	s Actions
Q Search					
Authorization Rule 1	R IdentityGroup Name EQUALS User Identity Groups:FPR-4110-Admin	FPR-4110-Admins \times	+ Select from list	+	٨
O Default		DenyAccess	+ Select from list	+ •	\$

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 \equiv > **Operations** > **Radius** > **Live logs**.
- 3. The information displayed shows if a user logged successfully.

=	Cisco ISE		Operations - RADIUS									A Evaluation N	lode 17 Days	9.0	58 Ø						
Live L	ogs Live Sessions																				
	Aisconfigured Supplicants 🕕				Misconfigure	d Network Devices 🕕				RADIUS Droj	• 0			c	lient Stopped Resp	onding 🕕				Repeat Co	anter 🕜
	0					0				1					0					0	
6	3 15 Reset Repeat Counts (🖞 Export To 🗸														Refre Nev	њ 17 — "	Latest 20 (records 🗸	Within Last 3 hour Filter 🗸	•
	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
	×			<u>~</u>	Identity	Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	~	Network Devic	Device Port	Identity Group	Posture Sta	Server	Mdm Serve	IMEISV		Usecase
Г (Feb 03, 2024 01:51:51.0	2	ò		cisco_readonly			New Polic	New Polic	FPR-4110			FPR-411D		User Identity Group		marpatinISE				
	Feb 03, 2024 01:50:48.9	8	ò		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.

≡ Cisco ISE	Op	perations - RADIUS	🛕 Evaluation Mod	e 18 Days Q 🛞 🕫 🖗
Live Logs Live Sessions				
Misconfigured Supplicants 🕓	Misconfigured Network Devices 🕕	RADIUS Drops 💿	Client Stopped Responding 🕕	Repeat Counter 🕕
0	1	1	0	3
ව් 🖯 Reset Repeat Counts 🕁 Disport To 🗸			Refeat. Show Show Latest 20 rec	rords v Huthin Last 3 hours v Filter v 0
Time Status	Details Repea Identity Endpoint ID	Endpoint Authenti Authoriz IP a	Address Network De Device Port Identity Group Postu	re Server Mdm Sei
×	V Identity Endpoint ID	Endpoint Pr Authenticat Authorizatic Authorizatic IP	Address 🗸 Network Device Device Port Identity Group Postur	e Sta Server Mdm Ser
Feb 02, 2024 07:32:18.8	a cisco_admin	Default >> Default	FPR-4110 User Identity Group:	marpatinISE
Feb 02, 2024 07:23:20.1	G cisco_readonly	Default >> Default >> PermitAcc	FPR-4110 User identity Group:	marpatinISE
Feb 02, 2024 07:15:32.2	G 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 \equiv > **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.



2.2 Select and Start the capture.

E Cisco ISE	Operations - Troubleshoot										🛦 Evaluation Mode 17 Days Q 💿 🗔 🔘	
Diagnostic Tools Download	d Logs	s Debug Wizard										
General Teels	The	TCP Dump utility page is to n	nonitor the contents of pack	ets on a network interface ar	nd troubleshoot problems on	the network as	they appe	ar				
RADIUS Authentication Troubl												Rows(Page 1 → < < 1 / 1 > > Ge 1 Total Rows
Execute Network Device Com Evaluate Configuration Validat	ø	A00 / Edt () Truck	Start OStop	E. Download								mer 🗸 – O
Posture Troubleshooting		Host Name	Network Interface	Filter	File Name	Reposito	File S	Number of	Time Limit	Promiscuous M	Status	
Agentiess Posture Troublesho EndPoint Debug		marpatin/SE.marpatin.com	GigabitEthemat 0 [Up, Run	ip host 172.16.0.130	marpatinISE_GigabitEthemet		10	1	5	false	RUNNING	
TCP Dump												
Session Trace Tests												
TrustSec Tools												

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 initial request.

	🕽 🔴 🔮 🧖 🖉 marpatinISE_GigabitEthernet 2.pcap									
4	🥖 🙆 🚞 🚞 🖉 🤇	🗢 🗢 😫 🕢	🖢 📃 🔍 ବ୍ ବ୍ ବ୍							
📘 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				