

Configure FMC and FTD External Authentication with ISE as a RADIUS Server

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[External Authentication for FMC](#)

[External Authentication for FTD](#)

[Network Topology](#)

[Configure](#)

[ISE Configuration](#)

[Add your Network Devices](#)

[Create the Local User Identity Groups and Users](#)

[Create the Authorization Profiles](#)

[Add a New Policy Set](#)

[FMC Configuration](#)

[Add your ISE RADIUS Server for FMC Authentication](#)

[FTD Configuration](#)

[Add your ISE RADIUS Server for FTD Authentication](#)

[Enable the RADIUS Server](#)

[Verify](#)

Introduction

This document describes an example of external authentication configuration for Secure Firewall Management Center and Firewall Threat Defense.

Prerequisites

Requirements

It is recommended to have knowledge of these topics:

- Cisco Secure Firewall Management Center initial configuration via GUI and/or shell.
- Configuring authentication and authorization policies on ISE.
- Basic RADIUS knowledge.

Components Used

The information in this document is based on these software and hardware versions:

- vFMC 7.4.2
- vFTD 7.4.2
- ISE 3.3

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.

Background Information

When you enable external authentication for management and administrative users of your Secure Firewall system, the device verifies the user credentials with a Lightweight Directory Access Protocol (LDAP) or RADIUS server as specified in an external authentication object.

External authentication objects can be used by the FMC and FTD devices. You can share the same object between the different appliance/device types, or create separate objects.

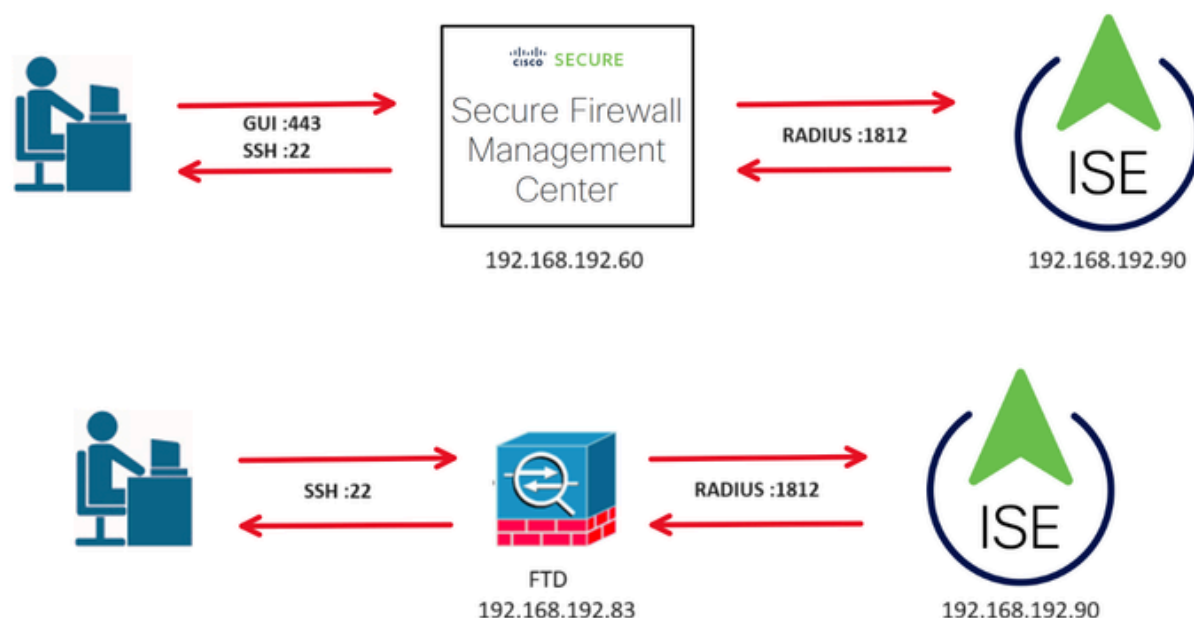
External Authentication for FMC

You can configure multiple external authentication objects for web interface access. Only one external authentication object can be used for CLI or shell access.

External Authentication for FTD

For the FTD, you can only activate one external authentication object.

Network Topology



Configure

ISE Configuration



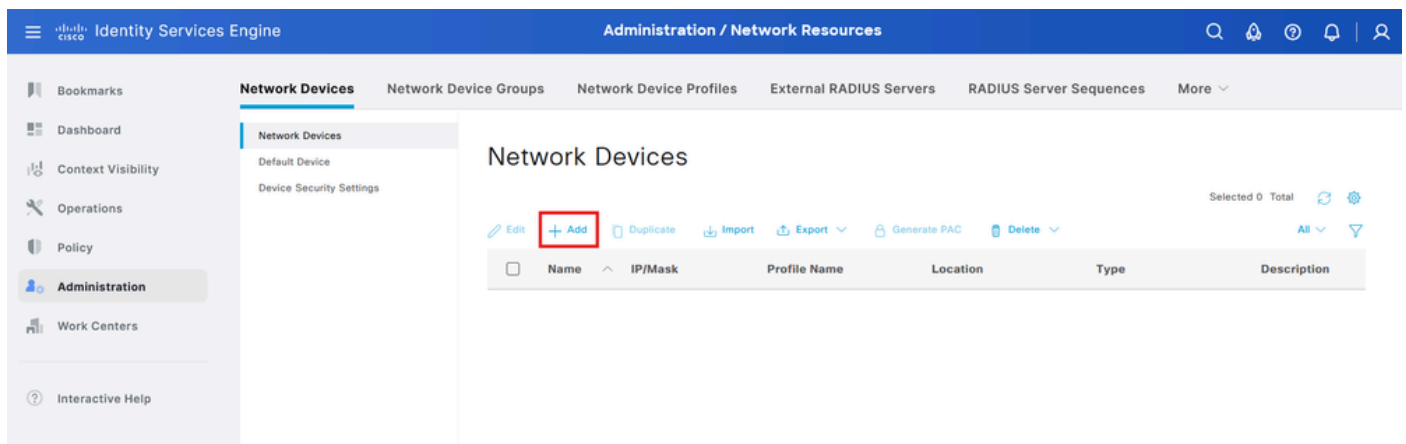
Note: There are multiple ways to setup ISE authentication and authorization policies for Network Access Devices (NAD) such as FMC. The example described in this document is a point of reference in which we create two profiles (one with Admin rights and the other Read-Only) and can be adapted to meet the baselines to access your network. One or more authorization policies can be defined on ISE with returning RADIUS attribute values to the FMC that are then mapped to a local user group defined in the FMC system policy configuration.

Add your Network Devices

Step 1. Navigate to the burger icon



located in the upper left corner >**Administration** > **Network Resources** > **Network Devices** > **+Add**.



Step 2. Assign a **Name** to the network device object and insert the **FMC IP address**.

Check the **RADIUS checkbox** and define a **Shared Secret**.

The same key must be used later to configure the FMC.

Once done, click **Save**.

Identity Services Engine Administration / Network Resources

Network Devices Network Device Groups Network Device Profiles More

Network Devices List > FMC

Network Devices

Name FMC

Description

IP Address * IP : 192.168.192.60 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations Set To Default

IPSEC No 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

Step 2.1. Repeat the same to add the FTD.

Assign a **Name** to the network device object and insert the FTD **IP address**.

Check the **RADIUS checkbox** and define a **Shared Secret**.

Once done, click **Save**.

Identity Services Engine

Administration / Network Resources

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Network Devices

Network Device Groups

Network Device Profiles

More

Network Devices

Default Device

Device Security Settings

Network Devices List > FTD

Network Devices

Name

FTD

Description

IP Address

* IP :

192.168.192.83 / 32

Device Profile

Cisco

Model Name

Software Version

Network Device Group

Location

All Locations

Set To Default

IPSEC

No

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

Step 2.3. Validate both devices are shown under Network Devices.

Identity Services Engine

Administration / Network Resources

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server Sequences

More

Network Devices

Default Device

Device Security Settings

Network Devices

Selected 0 Total 2

Edit

Add

Duplicate

Import

Export

Generate PAC

Delete

All

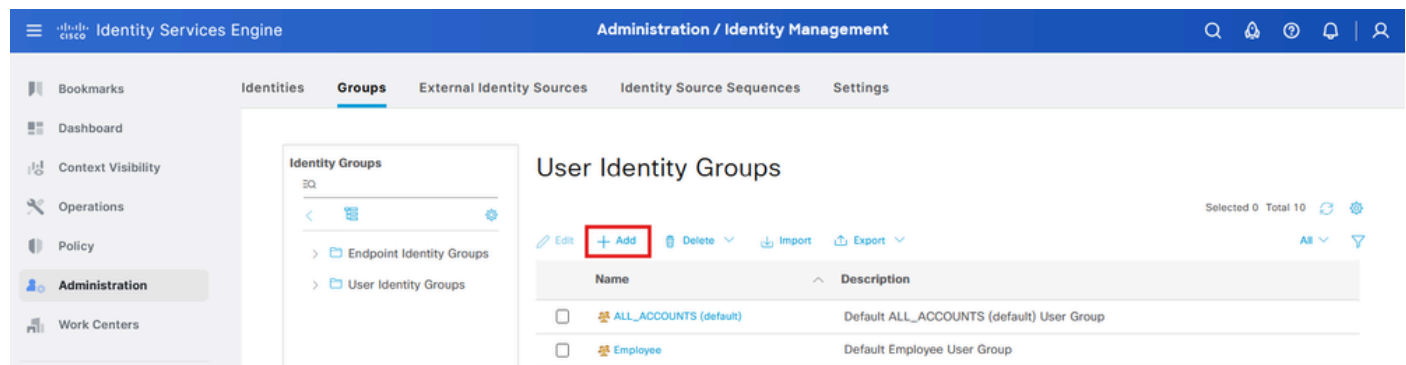
	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	FMC	192.168.192.60/32	Cisco	All Locations	All Device Types	
<input type="checkbox"/>	FTD	192.168.192.83/32	Cisco	All Locations	All Device Types	

Create the Local User Identity Groups and Users

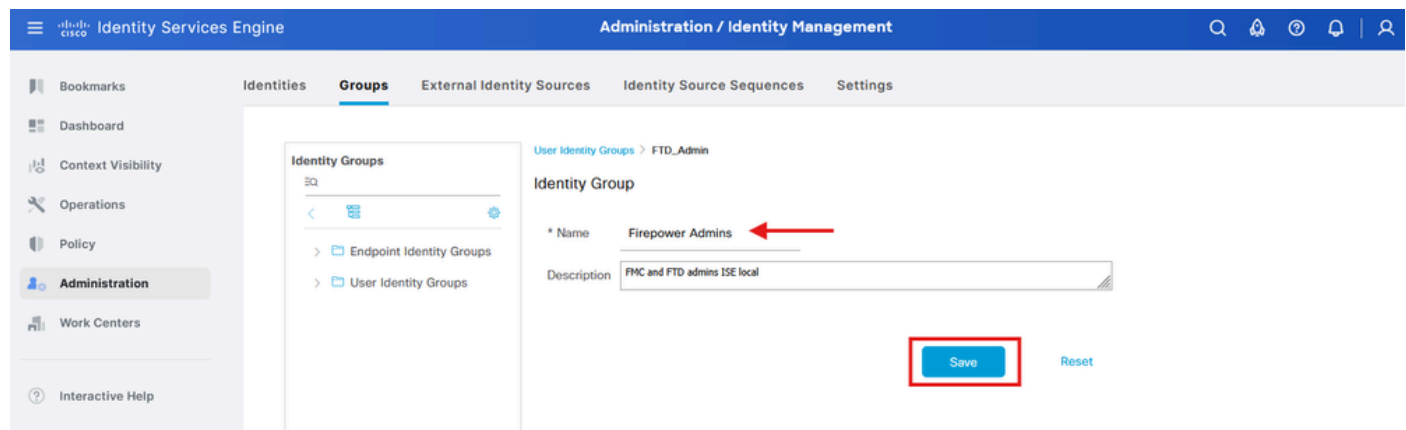
Step 3. Create the required User Identity Groups. Navigate to the burger icon



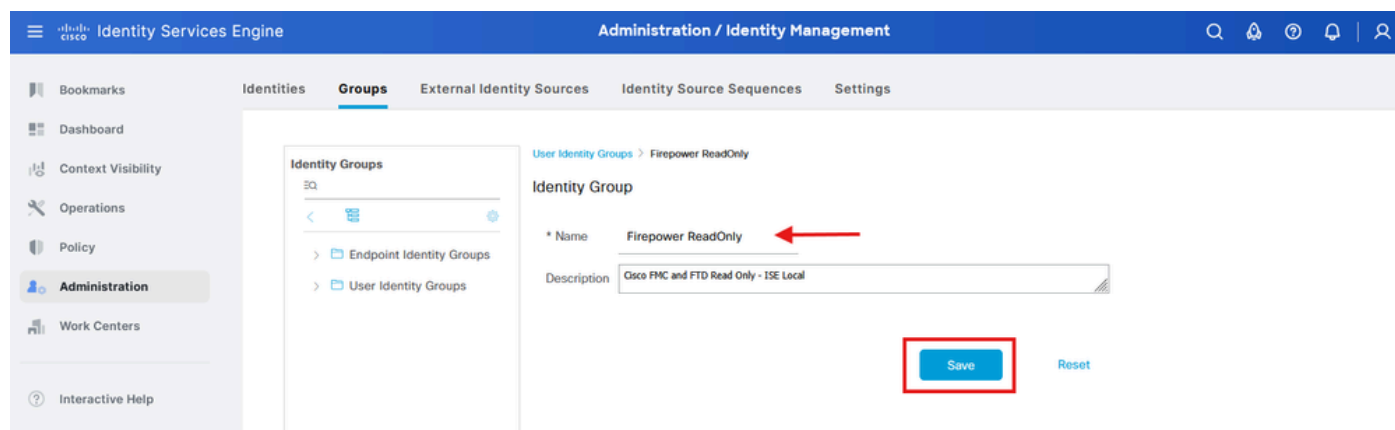
located in the upper left corner > **Administration > Identity Management > Groups > User Identity Groups > + Add**



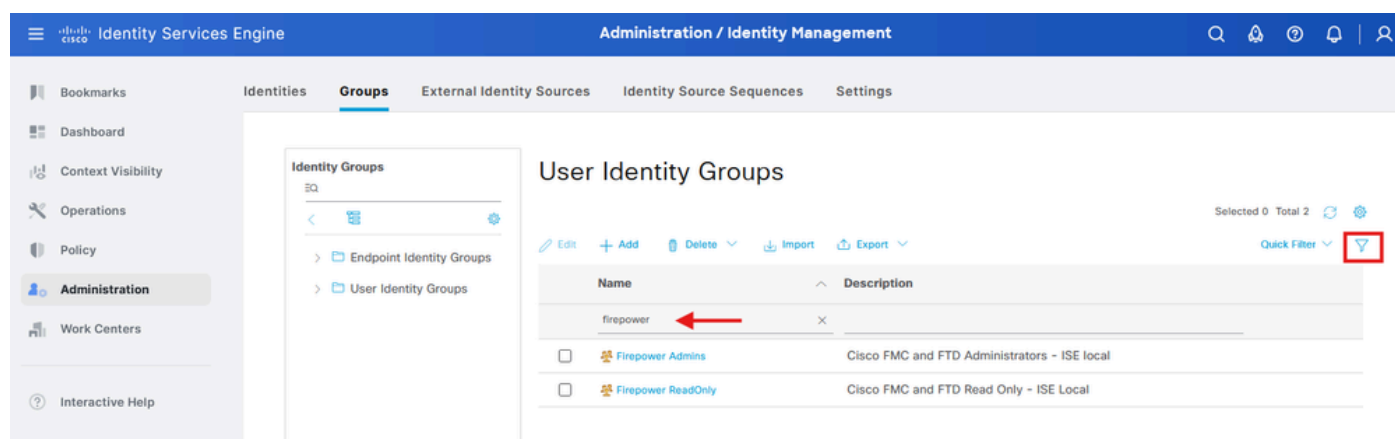
Step 4. Give each group a name and Save individually. In this example we are creating a group for Administrator users and another one for Read-Only users. First, create the group for the user with Administrator rights.



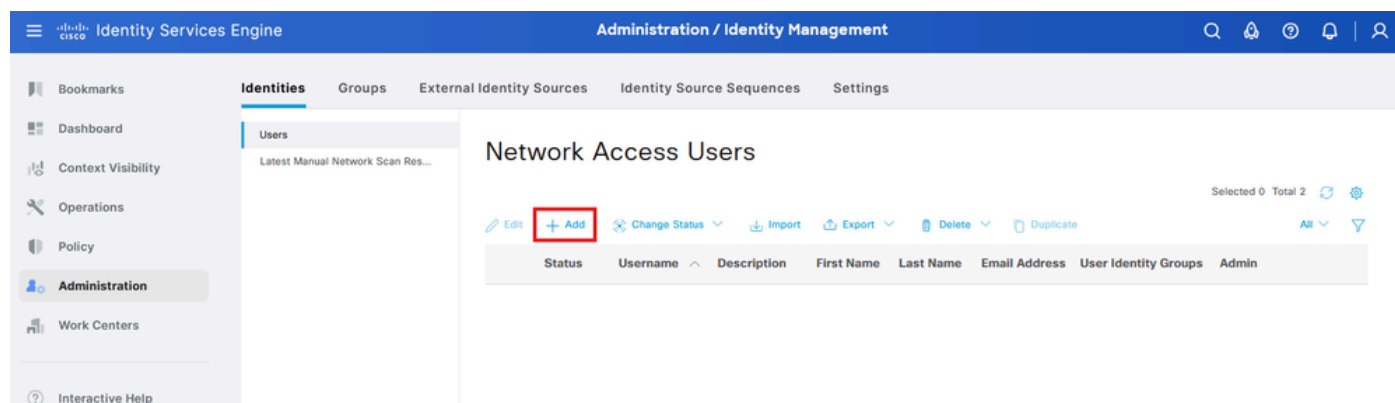
Step 4.1. Create the second group for the ReadOnly user.



Step 4.2. Validate both groups are shown under the User Identity Groups List. Use the filter to find them easily.



Step 5. Create the local users and add them to their correspondent group. Navigate to > **Administration > Identity Management > Identities > + Add.**



Step 5.1. First create the user with Administrator rights. Assign a name to it, password and the group **Firepower Admins**.

Identity Services Engine

Administration / Identity Management

Search

Alerts

Help

Logout

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Identities

Groups

External Identity Sources

Identity Source Sequences

Settings

Users

Network Access Users List

Latest Manual Network Scan Res...

Network Access User

* Username

firewall_admin

Status

Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

With Expiration

Never Expires

Password

* Login Password

Re-Enter Password

Enable Password

Generate Password

Generate Password

User Information

Account Options

Account Disable Policy

User Groups

Firepower Admins

Save

Reset

Step 5.2. Add the user with ReadOnly rights. Assign a name, password and the group **Firepower ReadOnly**.

Identity Services Engine Administration / Identity Management

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Identities Groups External Identity Sources Identity Source Sequences Settings

Users [Network Access Users List](#)

Latest Manual Network Scan Res...

Network Access User

* Username **firewall_readuser**

Status ☒ Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime:

☐ With Expiration

☒ Never Expires

Password

* Login Password

Re-Enter Password

Generate Password

Generate Password

User Information

Account Options

Account Disable Policy

User Groups

Firepower ReadOnly

Save Reset

Create the Authorization Profiles

Step 6. Create the Authorization Profile for the FMC Web Interface Admin user.

Navigate to



> **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** > +Add.

Define a name for the **Authorization Profile**, leave Access Type as **ACCESS_ACCEPT**.

Under Advanced Attributes Settings add a **Radius > Class--[25]** with the value **Administrator** and click **Submit**.

Identity Services Engine

Policy / Policy Elements

Search

Alerts

Help

Logout

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Dictionary

Conditions

Results

Authentication

Authorization

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

FMC_GUI_Admin

Description

Administrator Access FMC Web Interface

* Access Type

ACCESS_ACCEPT

Network Device Profile

Cisco

Service Template

☐

Track Movement

☐

Agentless Posture

☐

Passive Identity Tracking

☐

> Common Tasks

Advanced Attributes Settings

Radius:Class

*

Administrator

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit

Cancel

Step 6.1. Repeat the previous step to create the Authorization Profile for the FMC Web Interface ReadOnly User. Create the Radius Class with the value **ReadUser** instead Administrator this time.

Identity Services Engine

Policy / Policy Elements

Search

Alerts

Help

Logout

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Dictionary

Conditions

Results

Authentication

Authorization

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles

New Authorization Profile

Authorization Profile

* Name

FMC_GUI_ReadOnly

Description

Read Only Access FMC Web Interface

* Access Type

ACCESS_ACCEPT

Network Device Profile

Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Advanced Attributes Settings

Radius:Class

*

ReadUser

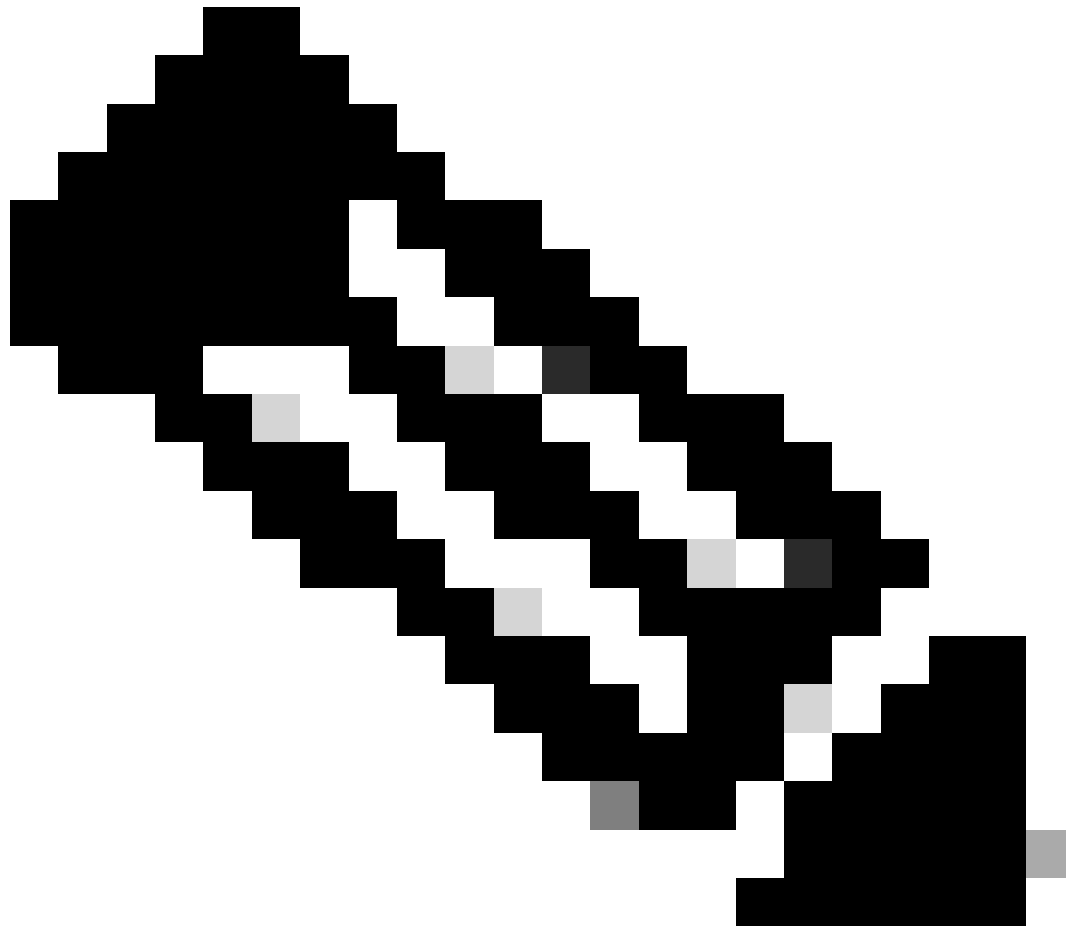
Attributes Details

Access Type = ACCESS_ACCEPT

Class = ReadUser

Submit

Cancel



Note: For FMC (all versions) and FTD (6.2.3 and 6.3), you must define users for Command Line Interface (CLI) access in the FMC External Authentication Object, which I show in Step 4 under the FMC Configuration procedure. For FTD 6.4 and later, we recommend defining users on the RADIUS server as I show you in the next step.

Step 7. Create the Authorization Profile for the FTD CLI user with Administrator rights.

Navigate to



> **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles** > +Add.

Define a name for the **Authorization Profile**, leave Access Type as **ACCESS_ACCEPT**.

Under Advanced Attributes Settings add a **Radius > Service-Type--[6]** with the value **Administrative** and click **Submit**.

Identity Services Engine Policy / Policy Elements

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

Dictionary Conditions Results

Authentication Authorization Authorization Profiles Downloadable ACLs Profiling Posture Client Provisioning

Authorization Profiles > FTD_CLI_Admin

Authorization Profile

* Name FTD_CLI_Admin

Description Administrator Access FTD Command Line Interface

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

> Common Tasks

> Advanced Attributes Settings

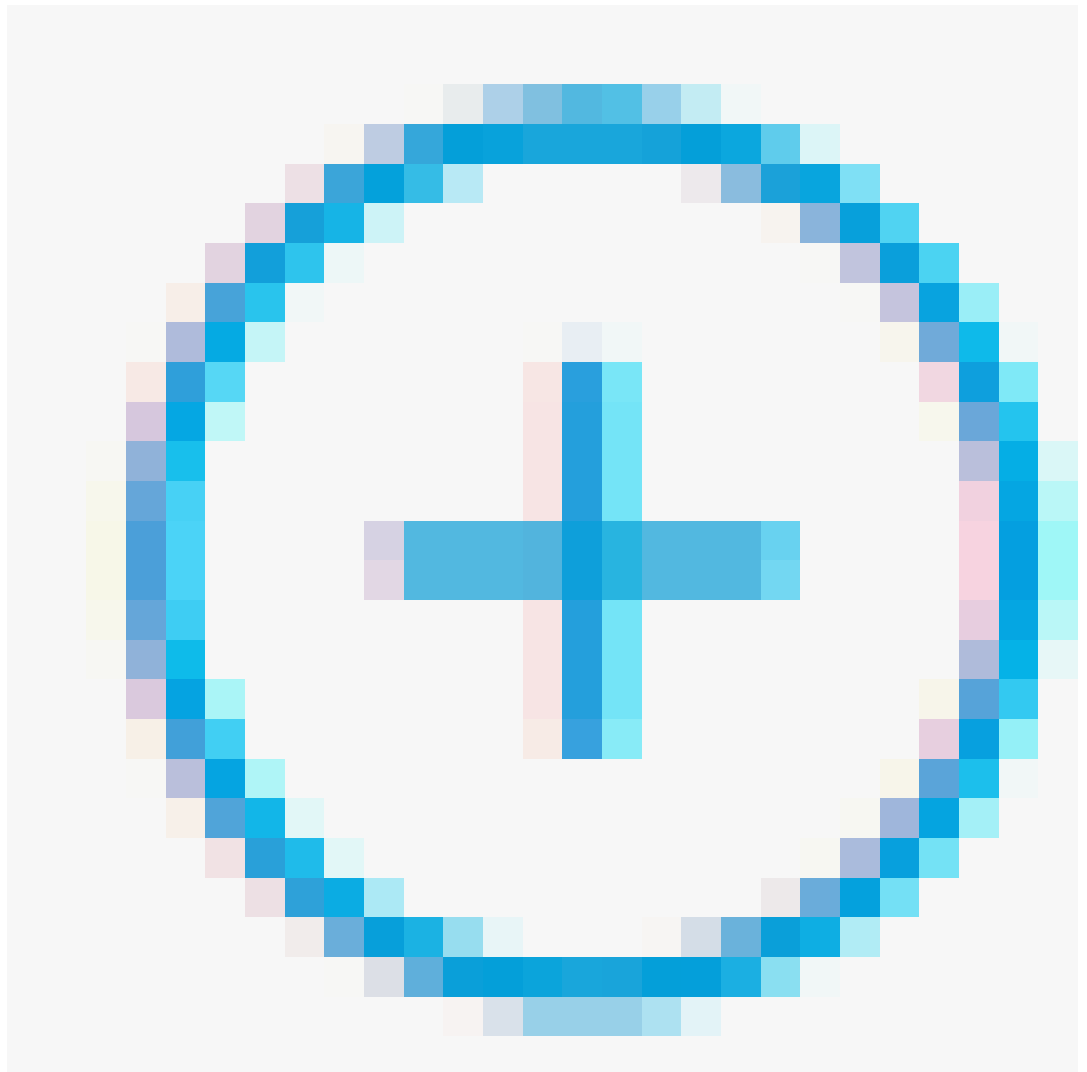
Radius:Service-Type * Administrative

> Attributes Details

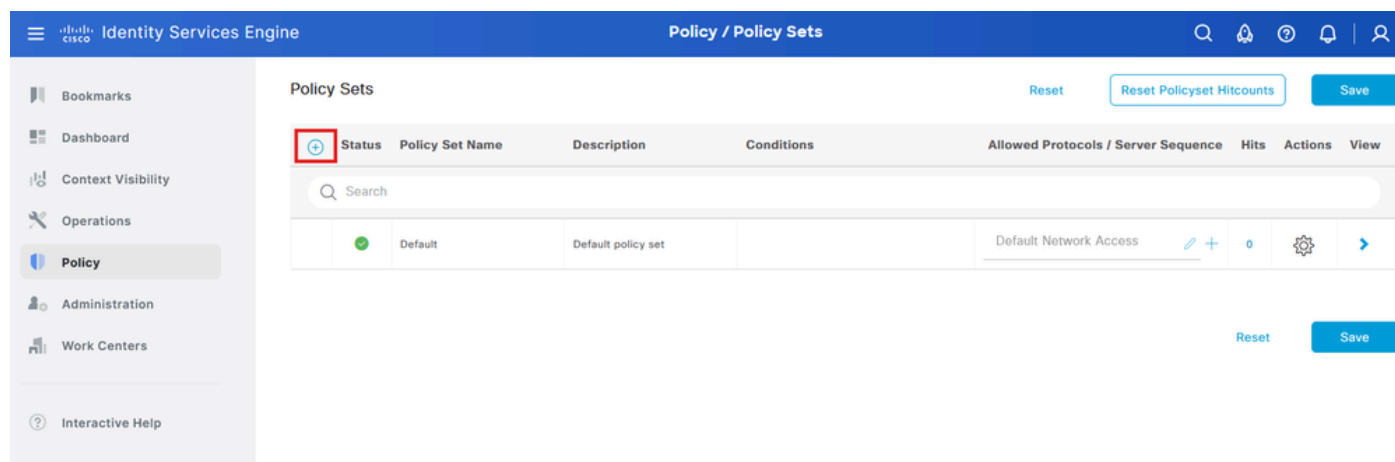
Access Type = ACCESS_ACCEPT
Service-Type = 6

Save Reset

Step 7.1. Repeat the previous step to create the Authorization Profile for the FTD CLI ReadOnly User. This time create the **Radius > Service-Type--[6]** with the value **NAS Prompt** instead.



icon placed at the upper left corner.

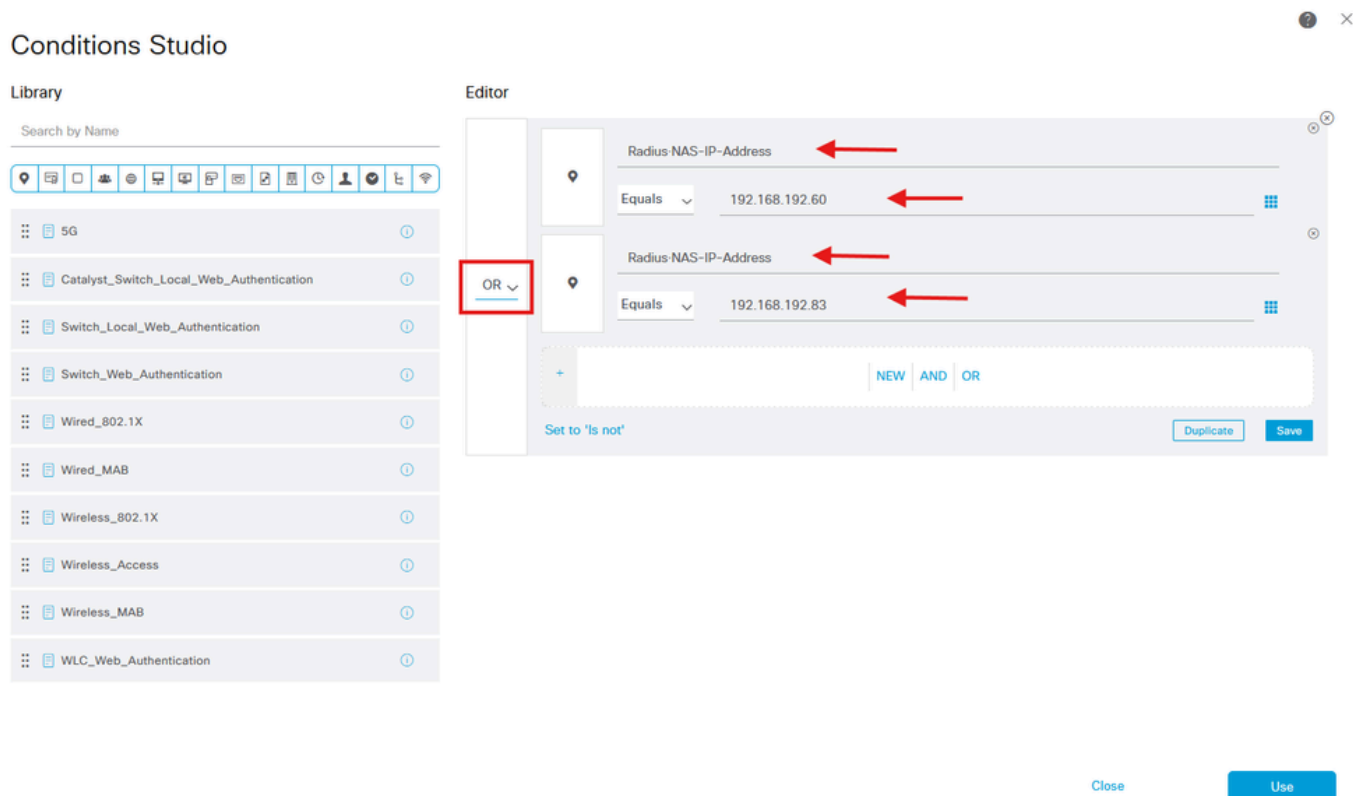


Step 8.1. A new line is placed at the top of your Policy Sets.

Name the new policy and add a top condition for **RADIUS NAS-IP-Address** attribute matching the FMC IP address.

Add a second condition with **OR** conjunction to include the IP address of the FTD.

Click **Use** to keep the changes and exit the editor.



Step 8.2. Once completed hit **Save**.

Identity Services Engine

Policy / Policy Sets

Search

Reset

Reset Policyset Hitcounts

Save

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Policy Sets

Reset

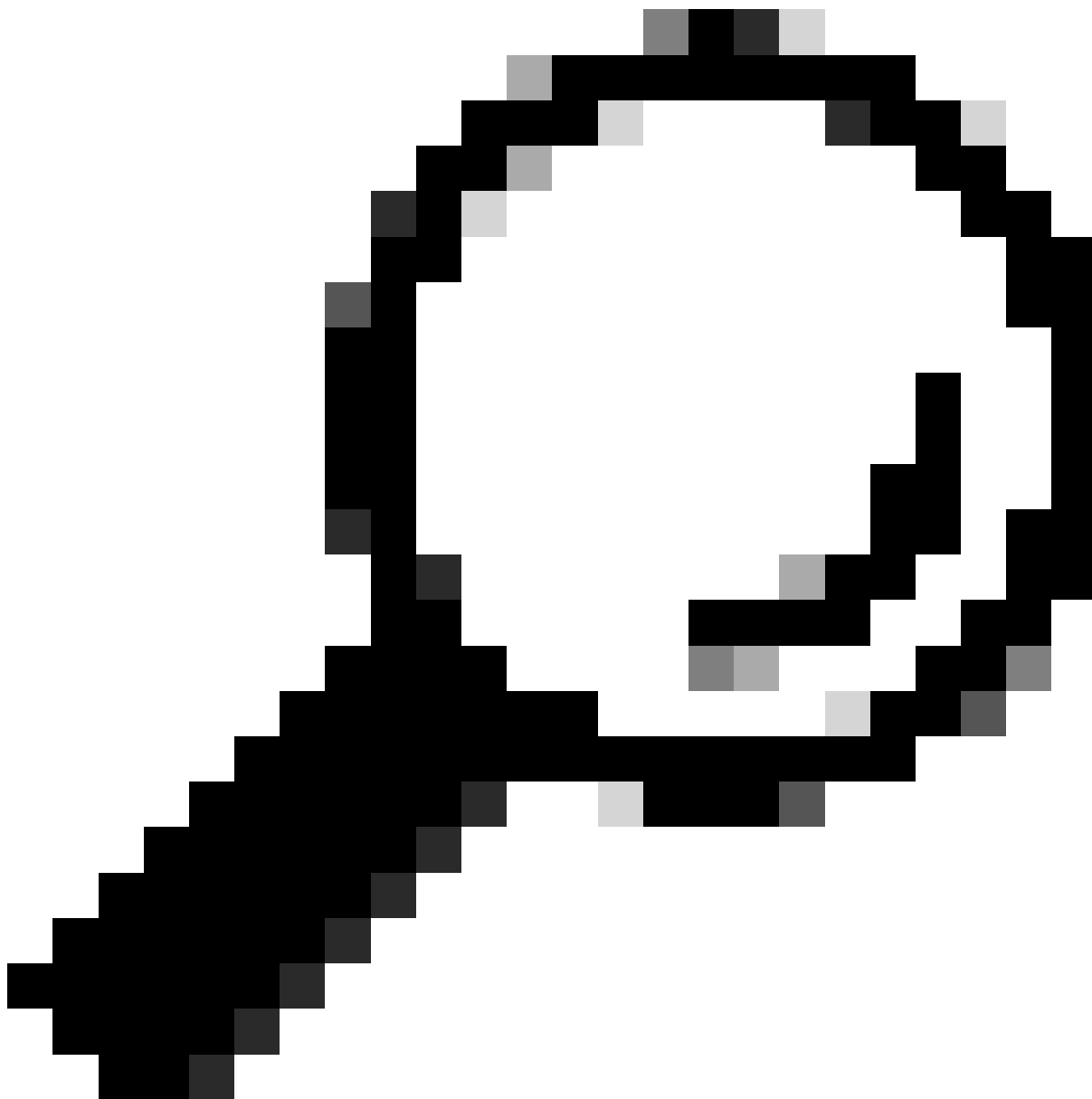
Reset Policyset Hitcounts

Save

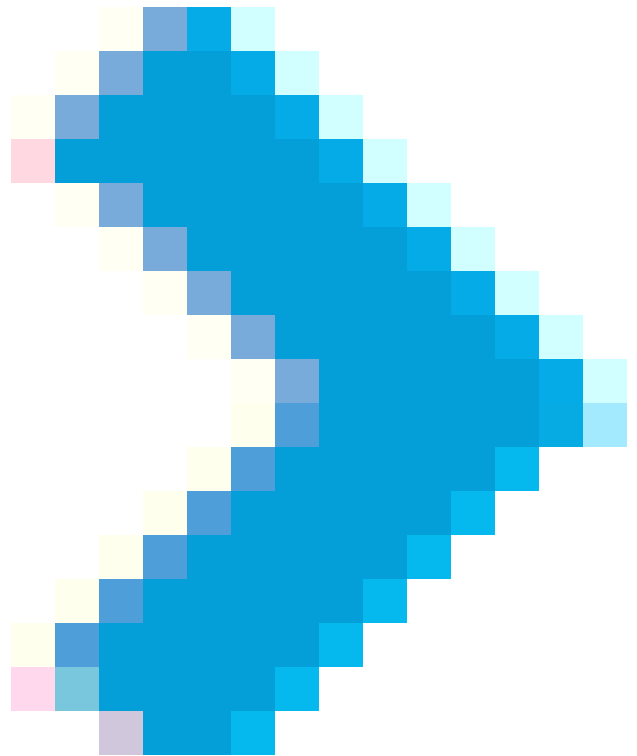
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<div></div>	FMC and FTD Access	Management Access	OR <div><div>Radius-NAS-IP-Address EQUALS 192.168.192.60</div><div>Radius-NAS-IP-Address EQUALS 192.168.192.83</div></div>	Default Network Access		<div></div>	<div></div>
<div></div>	Default	Default policy set		Default Network Access		<div></div>	<div></div>

Reset

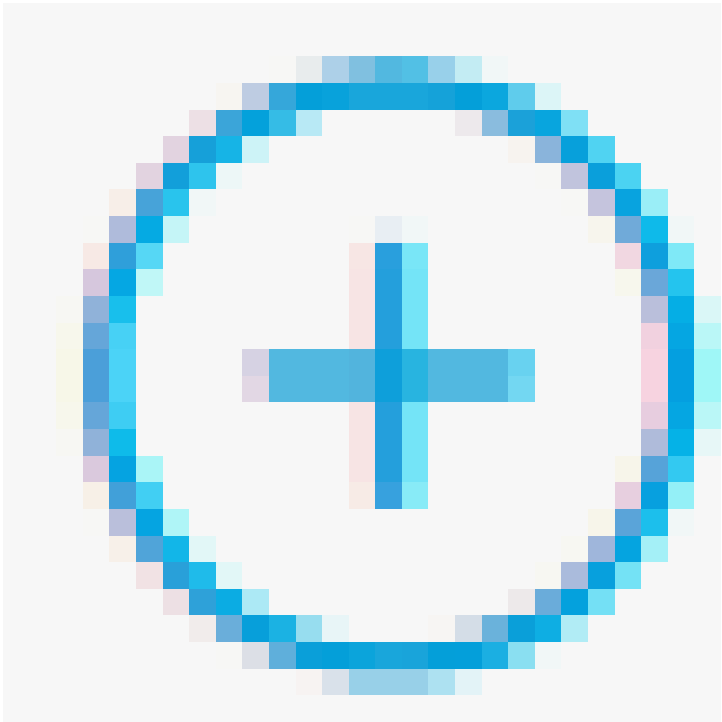
Save



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 9. View the new Policy Set by hitting the icon placed at the end of the row.



Expand the Authorization Policy menu and push the icon to add a new rule to allow the access to the user with admin rights.

Give it a name.

Set the conditions to match the Dictionary **Identity Group** with Attribute **Name Equals** and choose **User Identity Groups: Firepower Admins** (the group name created in Step 4) and click **Use**.

Conditions Studio

Library

Search by Name



5G	
BYOD_is_Registered	
Catalyst_Switch_Local_Web_Auth entication	
Compliance_Unknown_Devices	
Compliant_Devices	
EAP-MSCHAPv2	
EAP-TLS	
Guest_Flow	
MAC_in_SAN	

Editor

IdentityGroup-Name

Equals

User Identity Groups:Firepower
Admins

Set to 'Is not'

Duplicate

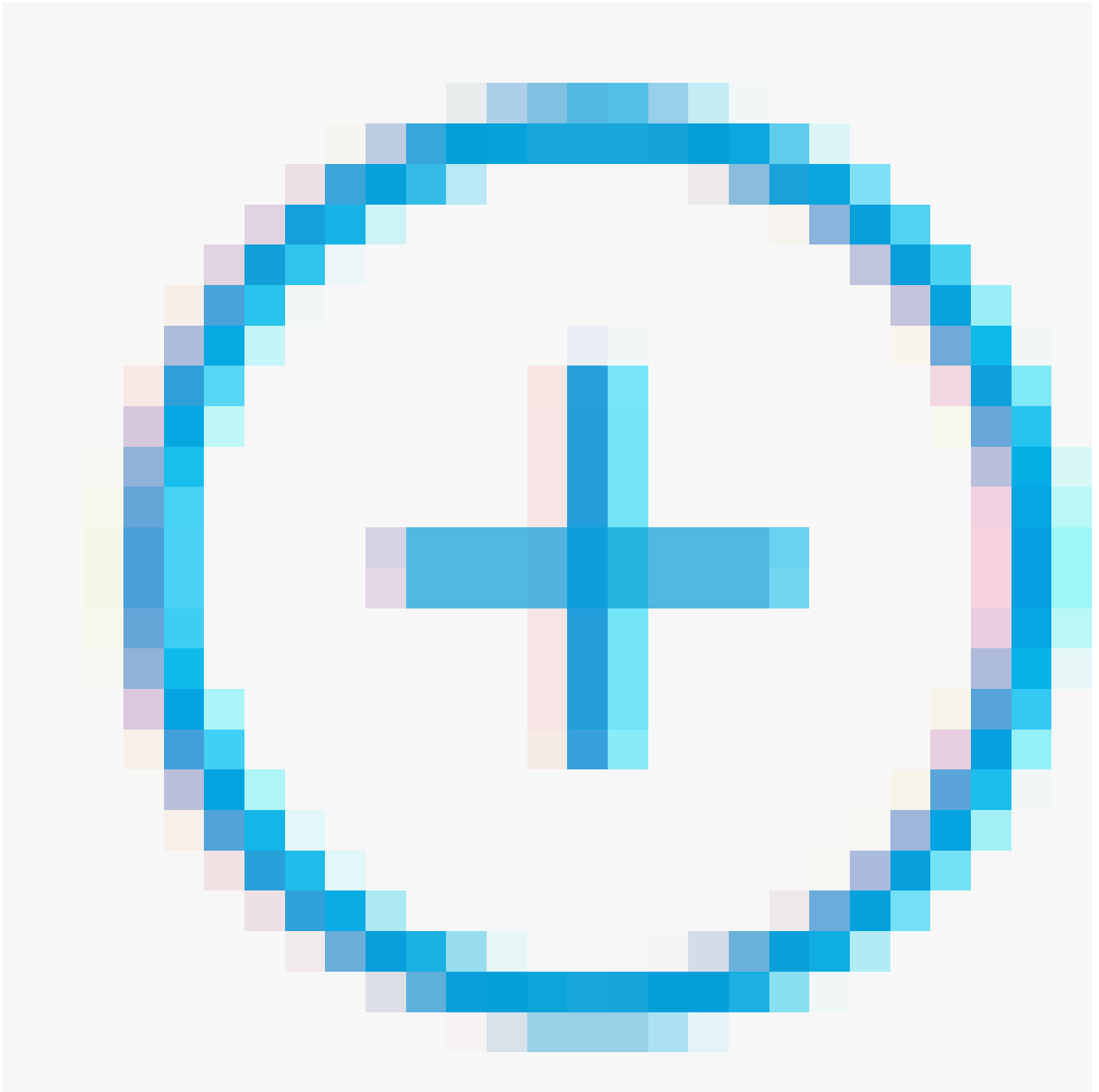
Save

NEW AND OR

Close

Use

Step 10. Click the










































icon to add a second rule to allow the access to the user with read-only rights.

Give it a name.

Set the conditions to match the Dictionary **Identity Group** with Attribute **Name Equals User Identity Groups: Firepower ReadOnly** (the group name created in Step 4.1) and click **Use**.

?

Editor

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																

IdentityGroup-Name

Equals

User Identity Groups:Firepower

ReadOnly

Set to 'Is not'

Duplicate Save

NEW AND OR

Close

Use

Use

Policy / Policy Sets

Policy Sets → FMC and FTD Access Reset Reset Policyset Hittcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	FMC and FTD Access	Management Access	OR <ul style="list-style-type: none"> Radius-NAS-IP-Address EQUALS 192.168.192.60 Radius-NAS-IP-Address EQUALS 192.168.192.83 	Default Network Access ✎ +	0

> Authentication Policy(1)

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

▼ Authorization Policy(3)

	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
	FMC and FTD Read Access	IdentityGroup-Name EQUALS User Identity Groups:Firepower ReadOnly	FMC_GUI_ReadOnly ✕ + FTD_CLI_RO ✕ +	Select from list ✎ +	0		
	FMC and FTD Admin Access	IdentityGroup-Name EQUALS User Identity Groups:Firepower Admins	FMC_GUI_Admin ✕ + FTD_CLI_Admin ✕ +	Select from list ✎ +	0		
	Default		DenyAccess ✎ +	Select from list ✎ +	0		

Reset Save

FMC Configuration

Add your ISE RADIUS Server for FMC Authentication

Step 1. Create the External Authentication Object under **System > Users > External Authentication > + Add External Authentication Object**.

Firewall Management Center
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration Deploy

Users User Roles External Authentication Single Sign-On (SSO)

Save Cancel Save and Apply

Default User Role: None Shell Authentication: Disabled

+ Add External Authentication Object

Name	Method	Enabled
No data to Represent		

Step 2. Select **RADIUS** as Authentication Method.

Under **External Authentication Object** give a **Name** to the new object.

Next, in **Primary Server** setting insert the ISE **IP address** and the same **RADIUS Secret Key** you used on Step 2 of your ISE configuration.

Firewall Management Center
System / Users / Create External Authentication Object

Overview Analysis Policies Devices Objects Integration Deploy

Users User Roles External Authentication Single Sign-On (SSO)

External Authentication Object

Authentication Method: RADIUS

Name: ISE-RADIUS-FMC

Description: RADIUS Auth for FMC

Primary Server

Host Name/IP Address: 192.168.192.90

Port: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address:

Port: 1812

RADIUS Secret Key:

Step 3. Insert the **RADIUS Class** attributes values that were configured on Steps 6 and 7 of ISE Configuration: Administrator and ReadUser for firewall_admin and firewall_readuser respectively.

RADIUS-Specific Parameters

Timeout (Seconds)

30

Retries

3

Access Admin

Administrator

Class=Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

Security Analyst (Read Only)

Class=ReadUser

Security Approver

Threat Intelligence Director (TID) User

Default User Role

Access Admin

Administrator

Discovery Admin

External Database User

To specify the default user role if user is not found in any group

Step 4. Populate the **Administrator CLI Access User List** under CLI Access Filter with the user name that must have CLI access to the FMC.

Click **Save** once done.

CLI Access Filter

(For Firewall Management Center (all versions) and Firewall Threat Defense (6.2.3 and 6.3), define users for CLI access. For Firewall Threat Defense 6.4 and later, we recommend defining users on the RADIUS server. Click [here](#) for more information)

Administrator CLI Access User List

firewall_admin

ex. user1, user2, user3 (lowercase letters only).

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

Cancel

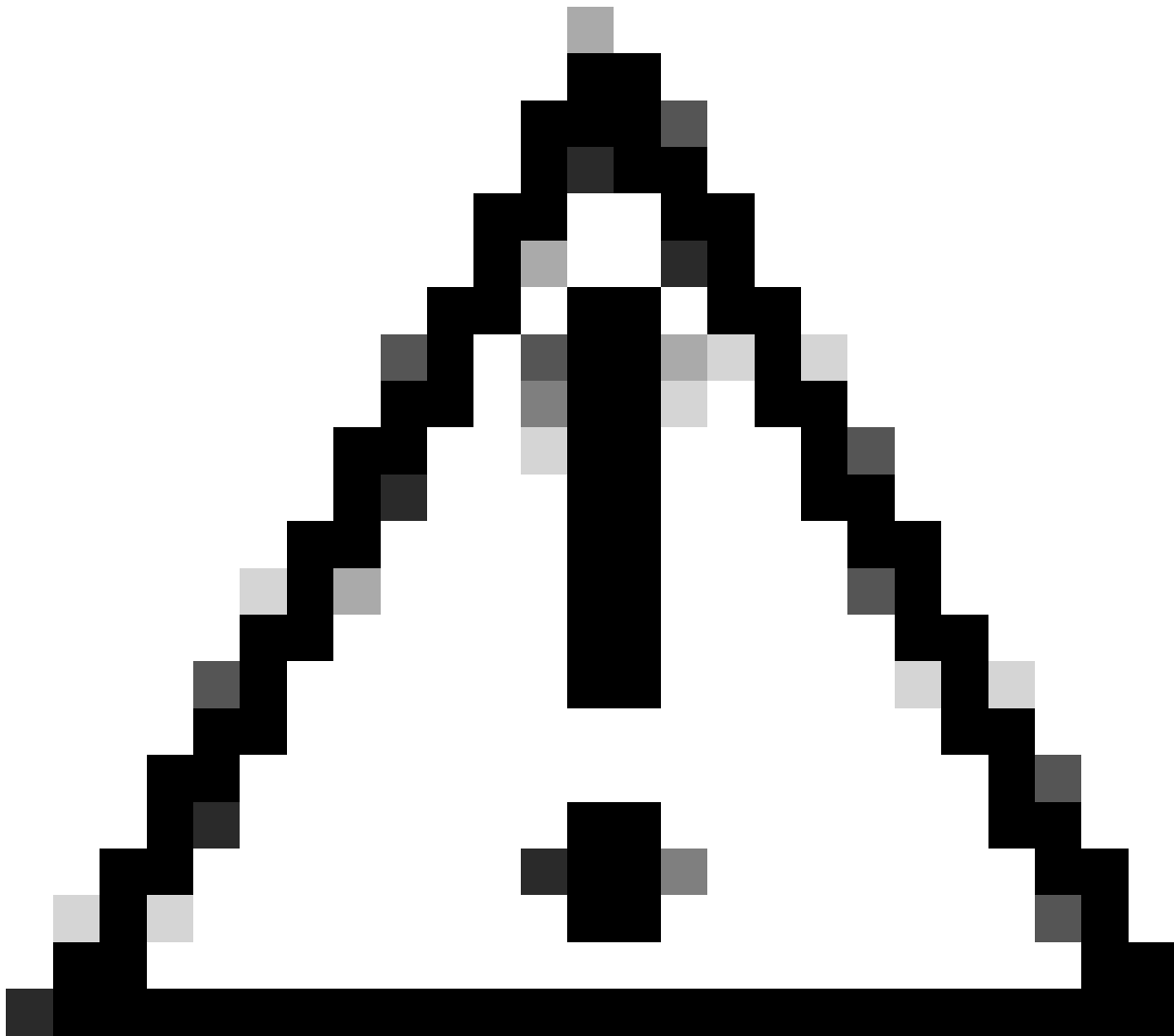
Test

Save



Note: In this procedure we define users on the RADIUS server using the Service-Type attribute to prevent ReadOnly users from getting CLI access to the FTD with expert rights.

For FMC CLI access you must use this user list.



Caution: Any user with CLI access to the FMC can gain Linux shell access with the expert command. Linux shell users can obtain root privileges, which can present a security risk. Make sure that you restrict the list of users with CLI or Linux shell access.

Step 5. Enable the new Object. Set it as the Shell Authentication method for FMC and click Save and Apply.

Firewall Management Center

System / Users / External Authentication

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

Users

User Roles

External Authentication

Single Sign-On (SSO)

Save



Cancel

Save and Apply

Default User Role: Administrator

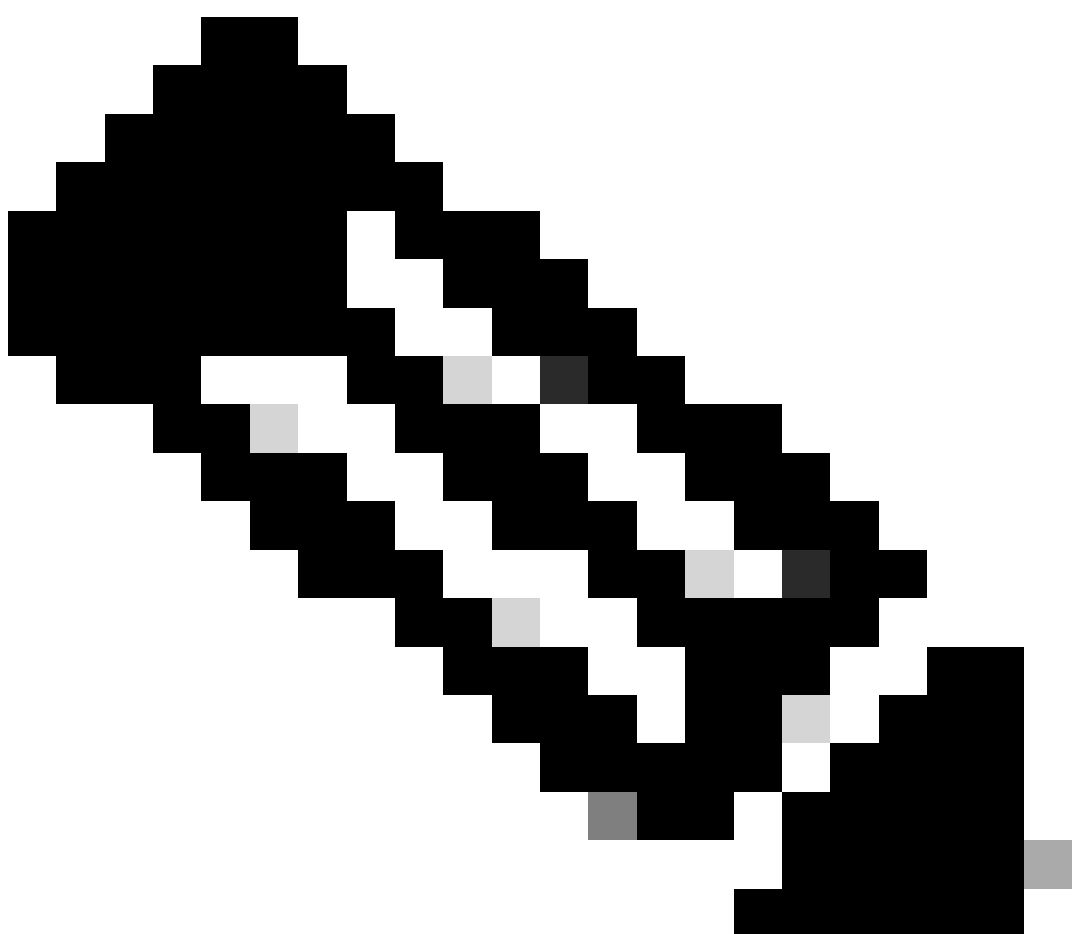
Shell Authentication Enabled (ISE-RADIUS-FMC)

+ Add External Authentication Object

Name	Method	Enabled	
1. ISE-RADIUS-FMC RADIUS Auth for FMC	RADIUS	<input checked="" type="checkbox"/>	 

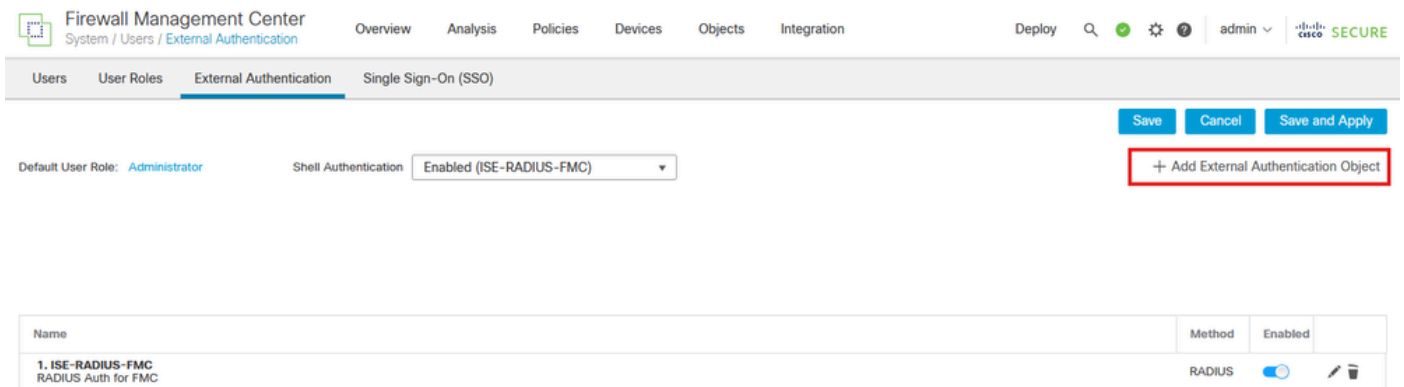
FTD Configuration

Add your ISE RADIUS Server for FTD Authentication



Note: You can share the same object between the management center and devices or create separate objects depending on where you want to define your users and the authorization level they must have. In this scenario we are defining our users on the RADIUS server, so we need to create separate objects for the threat defense and the management center.

Step 1. Same as you did for the FMC, create the External Authentication Object under **System > Users > External Authentication > + Add External Authentication Object**.



Firewall Management Center
System / Users / External Authentication

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Users User Roles External Authentication Single Sign-On (SSO)

Save Cancel Save and Apply

Default User Role: Administrator Shell Authentication: Enabled (ISE-RADIUS-FMC)

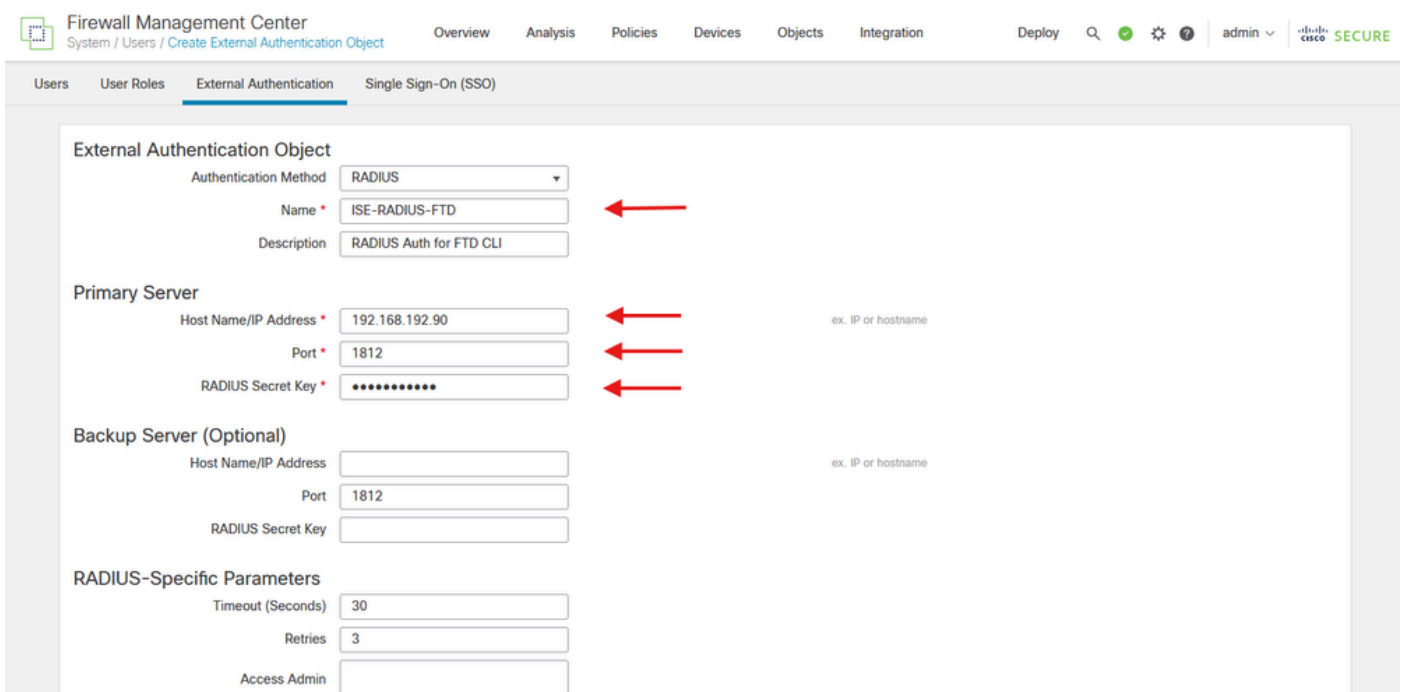
+ Add External Authentication Object

Name	Method	Enabled
1. ISE-RADIUS-FMC RADIUS Auth for FMC	RADIUS	<input checked="" type="checkbox"/>

Step 2. Select **RADIUS** as Authentication Method.

Under **External Authentication Object** give a **Name** to the new object.

Next, in **Primary Server** setting insert the ISE **IP address** and the same **RADIUS Secret Key** you used on Step 2.1 of your ISE configuration. Click **Save**



Firewall Management Center
System / Users / Create External Authentication Object

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⓘ admin ▾

Users User Roles External Authentication Single Sign-On (SSO)

External Authentication Object

Authentication Method: RADIUS

Name: ISE-RADIUS-FTD

Description: RADIUS Auth for FTD CLI

Primary Server

Host Name/IP Address: 192.168.192.90

Port: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address:

Port: 1812

RADIUS Secret Key:

RADIUS-Specific Parameters

Timeout (Seconds): 30

Retries: 3

Access Admin:



Warning: The timeout range is different for the FTD and the FMC, so if you share an object and change the default value of 30 seconds, be sure not to exceed the smaller timeout range (1-300 seconds) for FTD devices. If you set the timeout to a higher value, the threat defense RADIUS configuration does not work.

Enable the RADIUS Server

Step 1. In FMC GUI navigate to **Devices > Platform Settings**. **Edit** your current policy or create a new one if you do not have any assigned to the FTD you need access to. Enable the RADIUS server under **External Authentication** and click **Save**.

Firewall Management Center
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin ▾ **SECURE**

FTD Policy
Enter Description

You have unsaved changes **Save** **Cancel**

2

Policy Assignments (1)

Manage External Authentication Server

Name	Description	Method	Server:Port	Encryption	Enabled
ISE-RADIUS-FMC	RADIUS Auth for FMC	RADIUS	192.168.192.90:1812	no	<input type="checkbox"/>
ISE-RADIUS-FTD	RADIUS Auth for FTD CLI	RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>

1

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP Access
ICMP Access
NetFlow
SSH Access
SMTP Server
SNMP

Step 2. Make sure the FTD you need to gain access to is listed under Policy Assignments as a Selected Device.

Firewall Management Center
Devices / Platform Settings Editor

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin ▾ **SECURE**

FTD Policy
Enter Description

Policy Assignments (1)

Manage External Authentication Server

Name	Description	Method	Server:Port	Encryption	Enabled
ISE-RADIUS-FTD	RADIUS Auth for FTD CLI	RADIUS	192.168.192.90:1812	no	<input checked="" type="checkbox"/>
ISE-RADIUS-FMC	RADIUS Auth for FMC	RADIUS	192.168.192.90:1812	no	<input type="checkbox"/>

Policy Assignments

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Search by name or value

698354673
Group
FTD2140-HA
vFTD_192.168.192.83

Add to Policy

Selected Devices

vFTD_192.168.192.83

Cancel OK

Step 3. Deploy the changes.

cies **Devices** Objects Integration

Deploy 🔍 ⚙️ ? admin ▾ **SECURE**

Advanced Deploy ☐ Ignore warnings **Deploy** **Cancel**

☒ vFTD_192.168.192.83 Ready for Deployment

ments (1)



Note: If you previously configured an existent external username as an internal user using the *configure user add* command, the threat defense first checks the password against the internal user, and if that fails, it checks the RADIUS server. Note that you cannot later add an internal user with the same name as an external user as the deployment will fail; only pre-existing internal users are supported.

Verify

- Test that your new deployment is working properly.
- In the FMC GUI navigate to the RADIUS server settings and scroll down to the **Additional Test Parameters** section.
- Enter a username and password for the ISE user and click **Test**.

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

*Required Field

Cancel Test **Save**

- A successful test shows a green **Success Test Complete** message at the top of the browser window.

Firewall Management Center
Create External Authentication Object

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ? admin ▾

Users User Roles **External Authentication** Single Sign-On (SSO)

Success
Test Complete.

External Authentication Object

Authentication Method

Name *

- You can expand the **Details** under the **Test Output** for more information.

▸ Define Custom RADIUS Attributes

Additional Test Parameters

User Name

Password

Test Output

Show Details ▾

User Test

```
check_auth_radius: szUser: firewall_admin
RADIUS config file: /var/tmp/4VQpxhXof/radiusclient_0.conf
radiusauth - response: [User-Name=firewall_admin]
radiusauth - response: [Class=Administrator]
radiusauth - response: [Class=CACS:c0a8c05a_CNaQKf8ZB2sOTPFOSbmj8V6n727Es2627TeUjzXUdA:ISE-LVILLAFR/479011358/67]
"firewall_admin" RADIUS Authentication OK
check_is_radius_member attrib match found: [Class=Administrator] - [Class=Administrator] *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

Cancel Test **Save**

- Check the authentication request and response in your ISE RADIUS under **Operations > RADIUS > Live Logs**.

- Bookmarks
- Dashboard
- Context Visibility
- Operations**
- Policy
- Administration
- Work Centers
- Interactive Help

Live Logs

Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat

Refresh Never

Show Latest 20 records

Within Last 3

Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...
X				firewall_admin	x Endpoint ID	Endpoint Pr	Authenticat	Authorizatic	Authorizati
Jun 07, 2025 11:45:38.9...			2	firewall_admin	10.24.184.31		FMC and ...	FMC and ...	FMC_GUI...
Jun 07, 2025 11:44:30.1...				firewall_admin	10.24.184.31		FMC and ...	FMC and ...	FMC_GUI...
Jun 07, 2025 11:38:12.4...				firewall_admin	10.24.184.31		FMC and ...	FMC and ...	FMC_GUI...
Jun 07, 2025 11:19:54.2...				firewall_admin	10.24.184.31		FMC and ...	FMC and ...	FMC_GUI...
Jun 06, 2025 08:20:15.8...				firewall_admin	10.24.198.101		FMC and ...	FMC and ...	FMC_GUI...
Jun 06, 2025 08:19:13.4...				firewall_admin	10.24.198.101		FMC and ...	FMC and ...	FMC_GUI...
Jun 06, 2025 08:07:04.5...				firewall_admin	10.24.198.101		FMC and ...	FMC and ...	FMC_GUI...