Configure FDM External Authentication and Authorization with ISE Using RADIUS

Contents

Introduction

Prerequisites

- Requirements
- Interoperability
- Licensing

Background Information

- Network Diagram

Configure

- FDM Configuration
- ISE Configuration

Verify

Troubleshoot

Common Issues

Limitations

Q&A

Introduction

This document describes the procedure to integrate Cisco Firepower Device Manager (FDM) with Identity Services Engine (ISE) for administrator users authentication with RADIUS Protocol for both GUI and CLI access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Device Manager (FDM)
- Identity Services Engine (ISE)
- RADIUS protocol

Components Used

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

- Firepower Threat Defense (FTD) Device, all platforms Firepower Device Manager (FDM) version 6.3.0+
- ISE version 3.0

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.

Interoperability

- RADIUS server with users configured with user roles
- User roles must be configured on RADIUS server with cisco-av-pair
- Cisco-av-pair = fdm.userrole.authority.admin
- ISE can be used as a RADIUS server

Licensing

No specific license requirement, the base license is sufficient

Background Information

This feature allows customers to configure External Authentication with RADIUS and multiple user roles for those users.

RADIUS support for Management Access with 3 system-defined user roles:

- READ_ONLY
- READ_WRITE (cannot perform system critical actions like Upgrade, Restore and so on)
- ADMIN

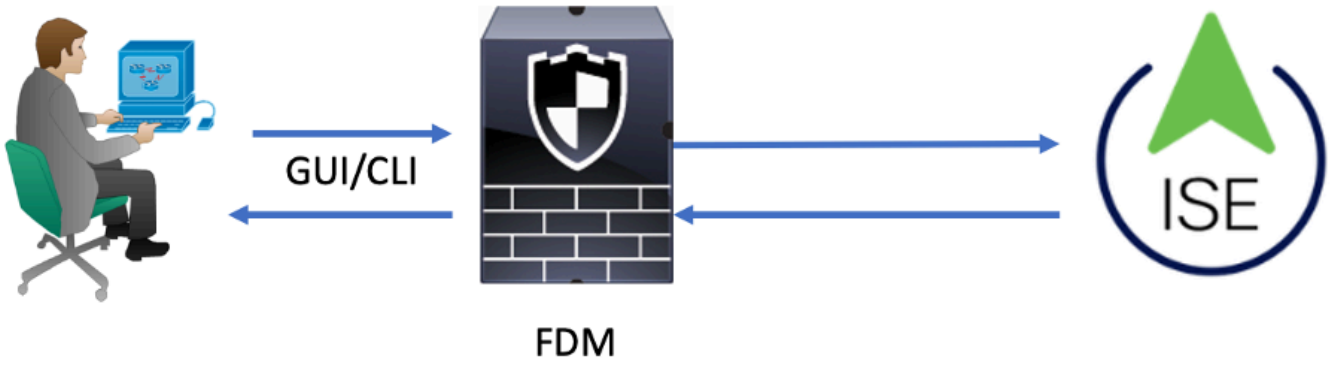
There is the ability to test the RADIUS server's configuration and to monitor active user sessions and delete a user session.

The feature was implemented in FDM version 6.3.0. Prior to the 6.3.0 release, FDM had support for one user(admin) only.

By default, Cisco Firepower Device Manager authenticates and authorizes users locally, in order to have a centralized authentication and authorization method you can use Cisco Identity Service Engine through RADIUS protocol.

Network Diagram

The next image provides an example of a network topology



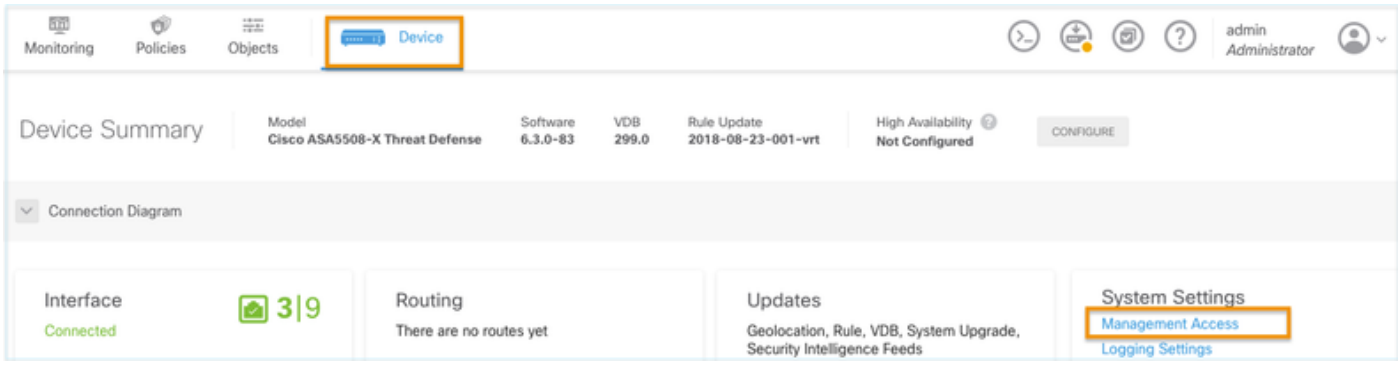
Process:

1. Admin User introduces its credentials.
2. Authentication process triggered and ISE validates the credentials locally or through Active Directory.
3. Once authentication is successful ISE sends a Permit packet for authentication and authorization information to FDM.
4. Account performs on ISE and a successful authentication live log happens.

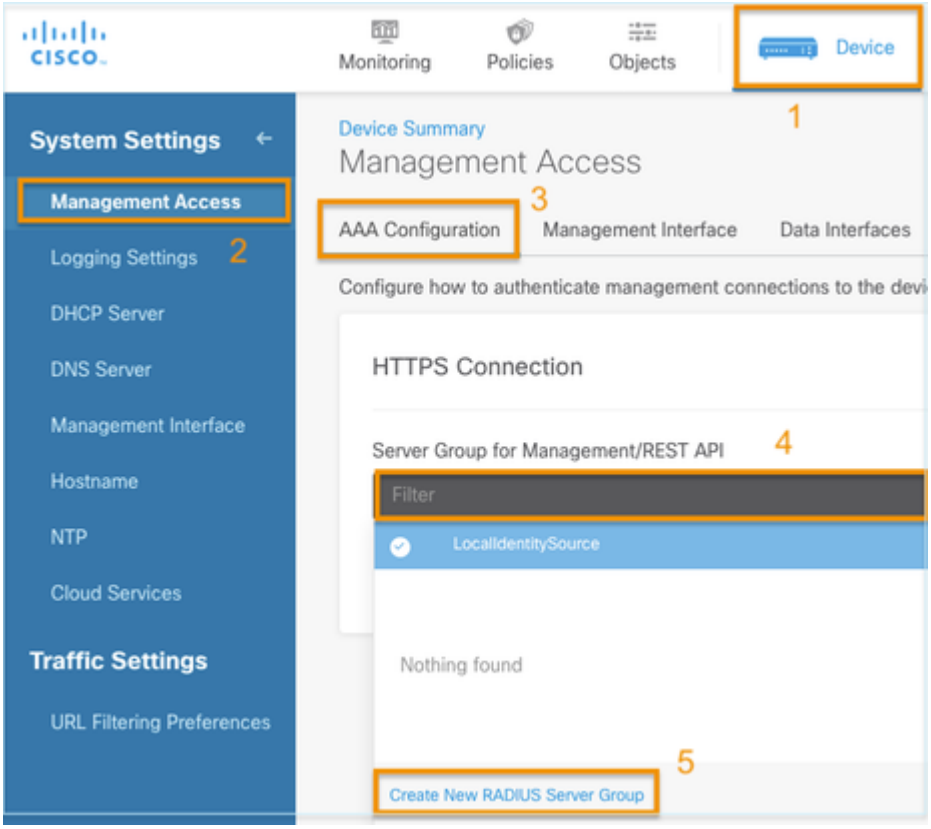
Configure

FDM Configuration

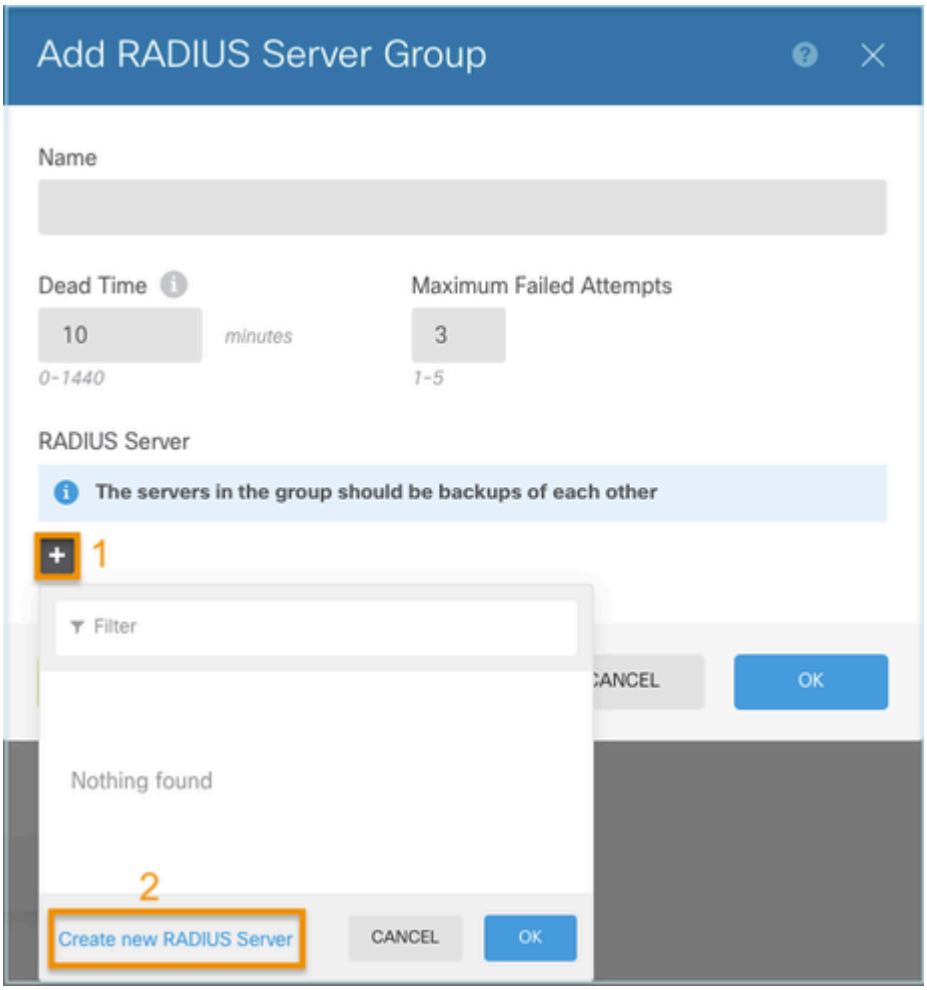
Step 1. Log in into FDM and navigate to Device > System Settings > Management Access tab

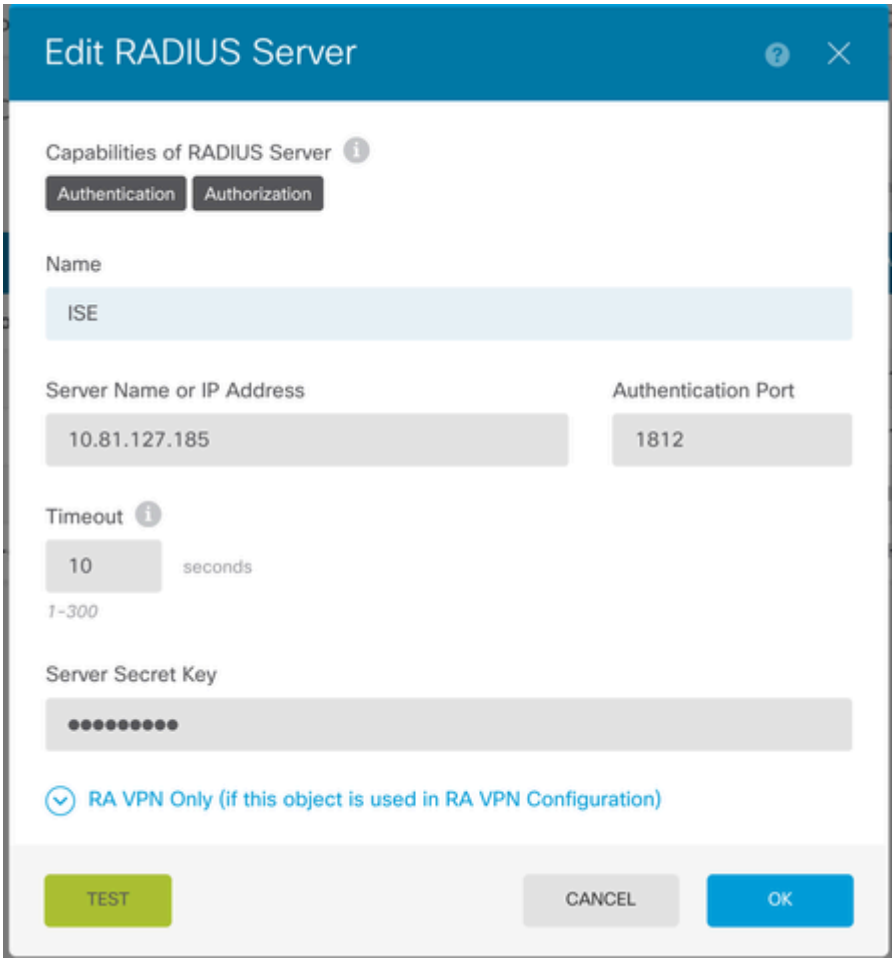


Step 2. Create New RADIUS Server Group

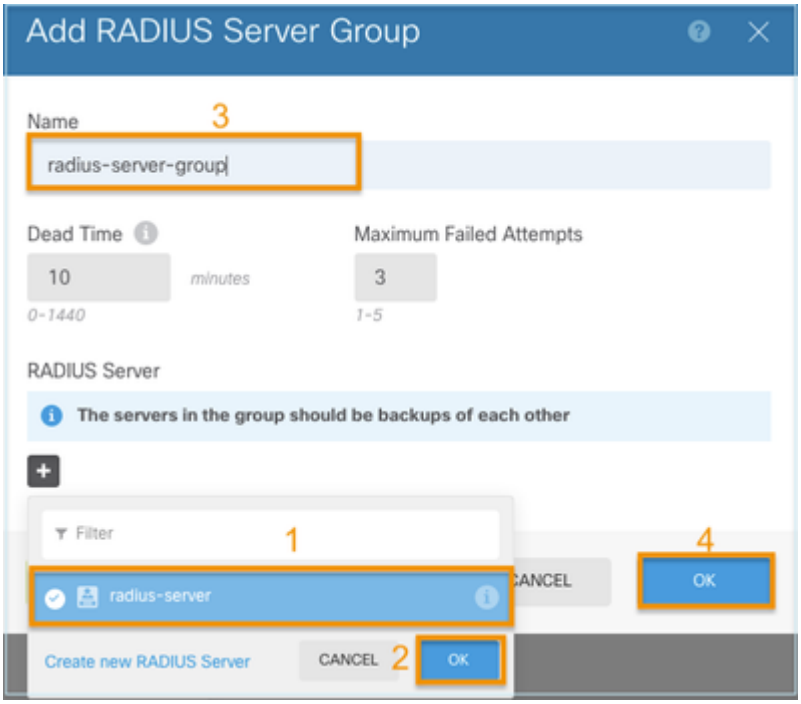


Step 3. Create new RADIUS Server

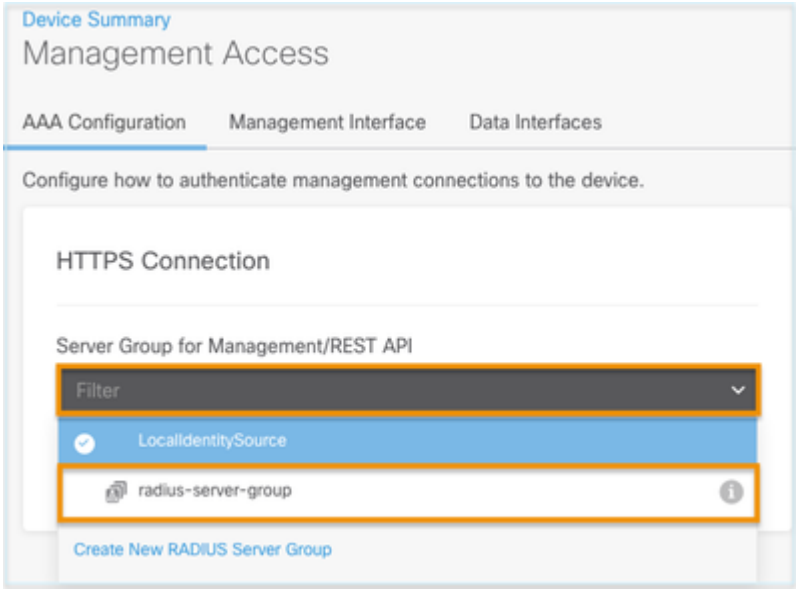

Add RADIUS Server Group
Name
Dead Time
10
minutes
0-1440
Maximum Failed Attempts
3
1-5
RADIUS Server
The servers in the group should be backups of each other
1
Filter
Nothing found
2
Create new RADIUS Server
CANCEL
OK
CANCEL
OK

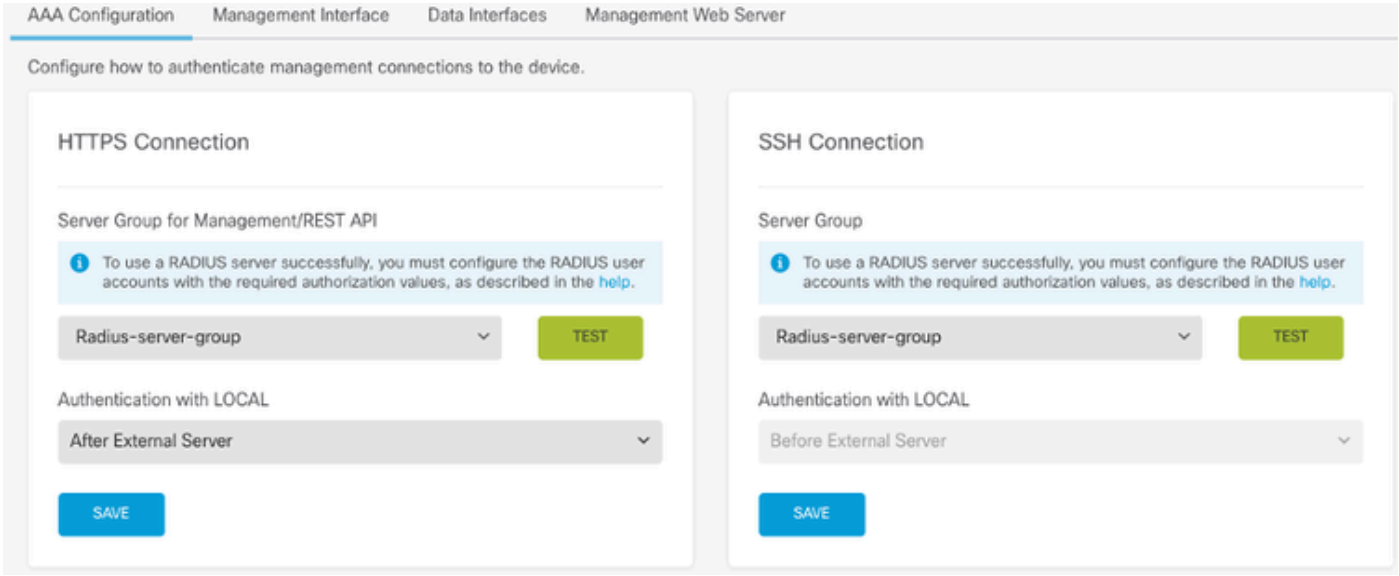

Edit RADIUS Server
Capabilities of RADIUS Server
Authentication
Authorization
Name
ISE
Server Name or IP Address
10.81.127.185
Authentication Port
1812
Timeout
10
seconds
1-300
Server Secret Key
RA VPN Only (if this object is used in RA VPN Configuration)
TEST
CANCEL
OK

Step 4. Add RADIUS Server into the RADIUS Server Group

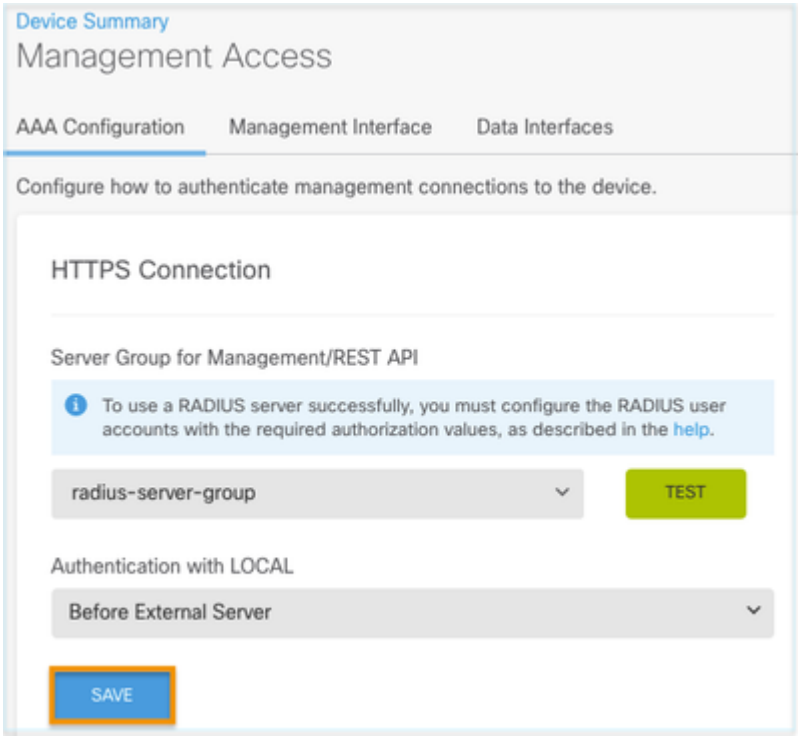


Step 5. Select created group as Server Group for Management



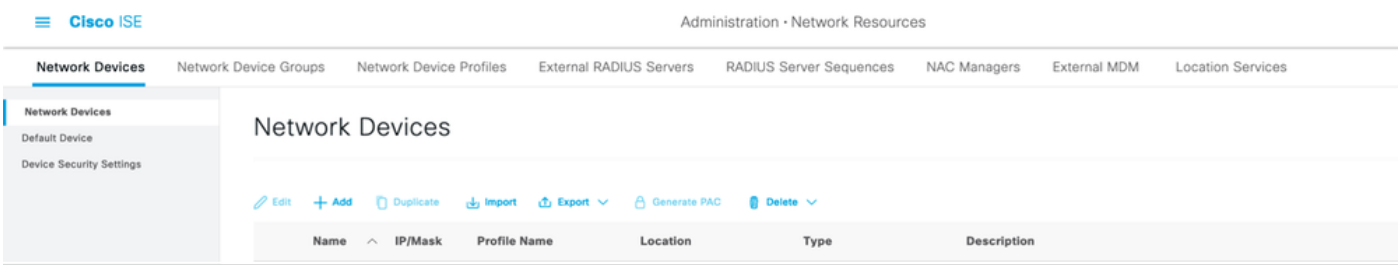


Step 6. Save the configuration

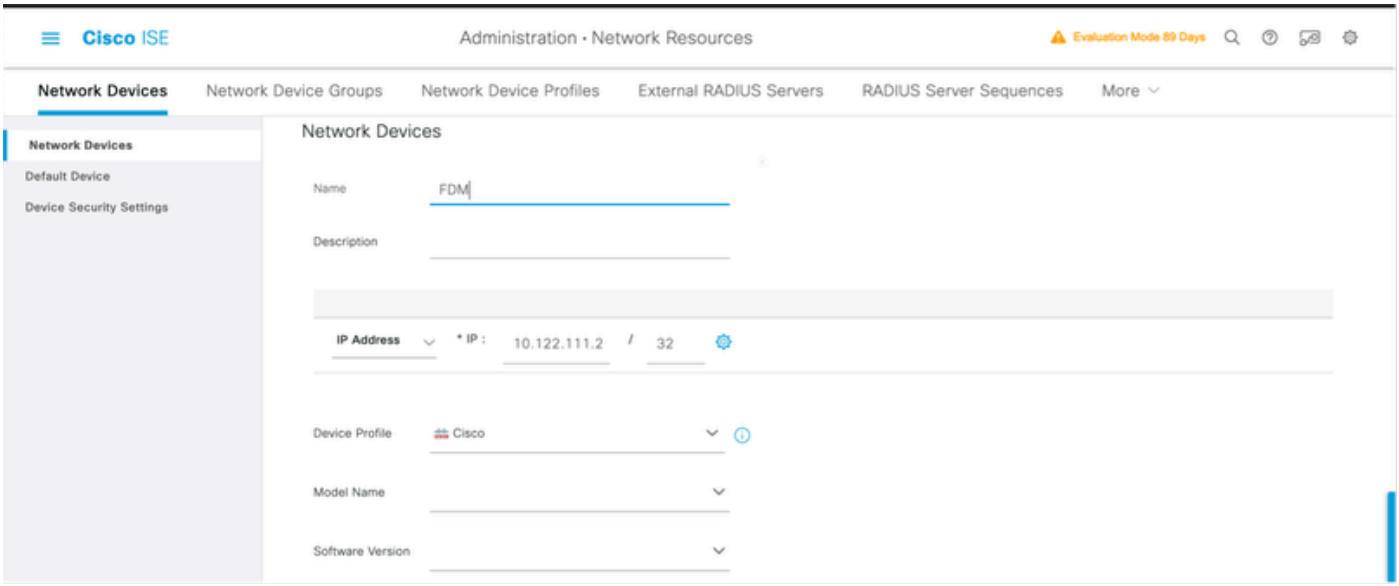


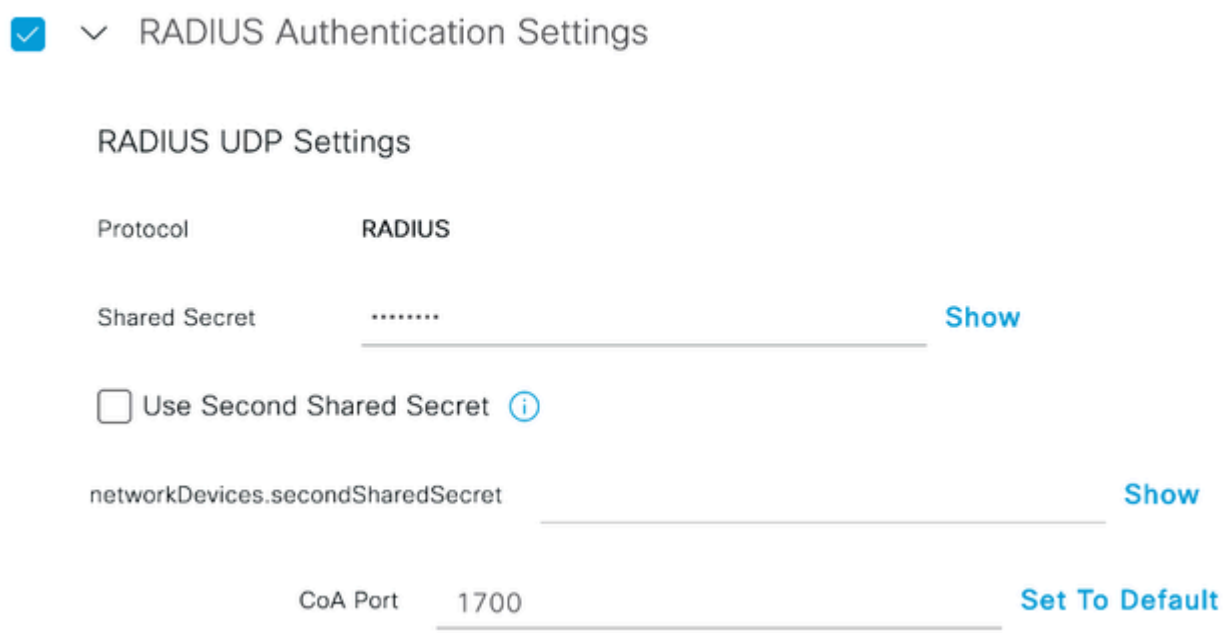
ISE Configuration

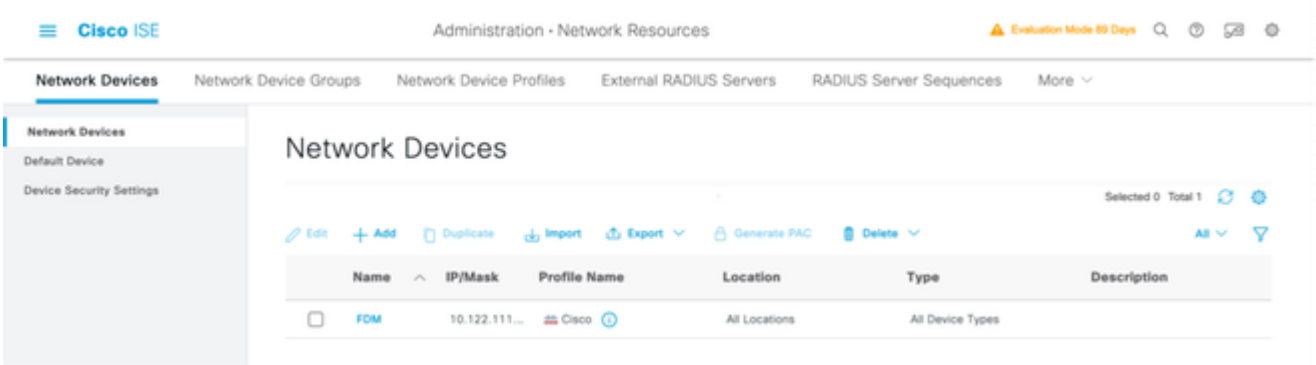
Step 1. Navigate to three lines icon located in the upper left corner and select on **Administration > Network Resources > Network Devices**



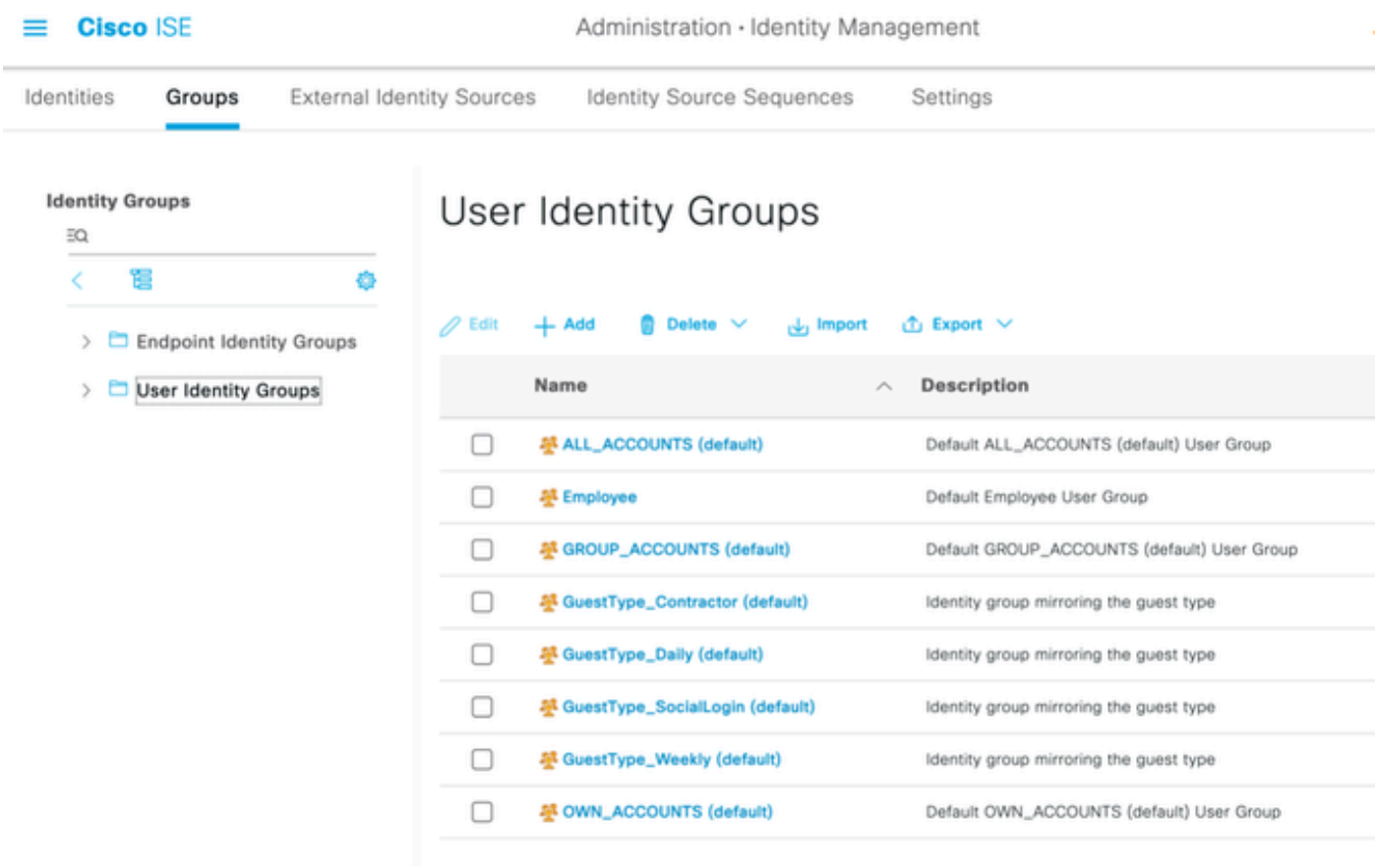
Step 2. Select the **+Add** button and define Network Access Device Name and IPAddress, then check the RADIUS checkbox and define a shared secret. Select on **Submit**



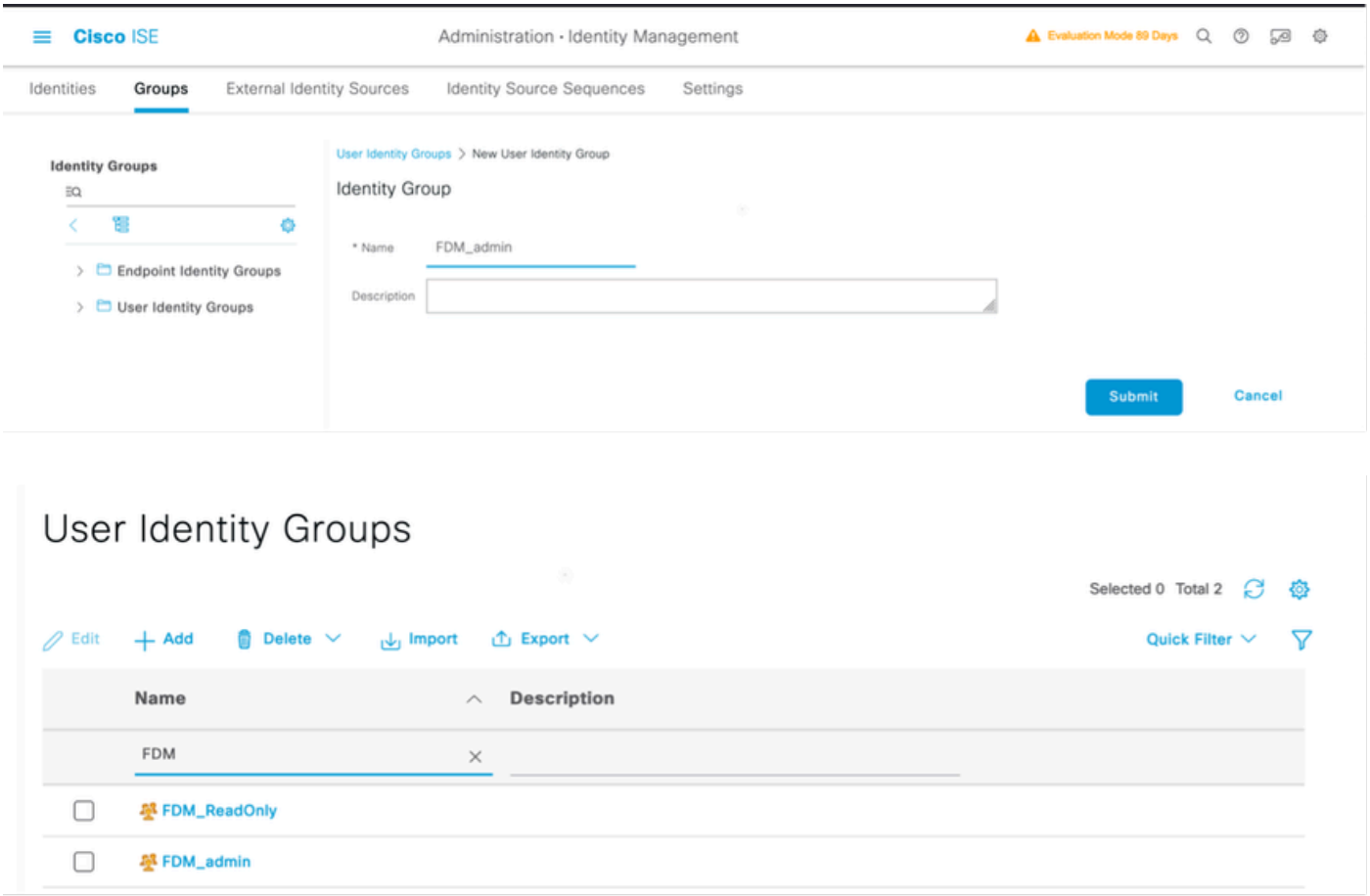


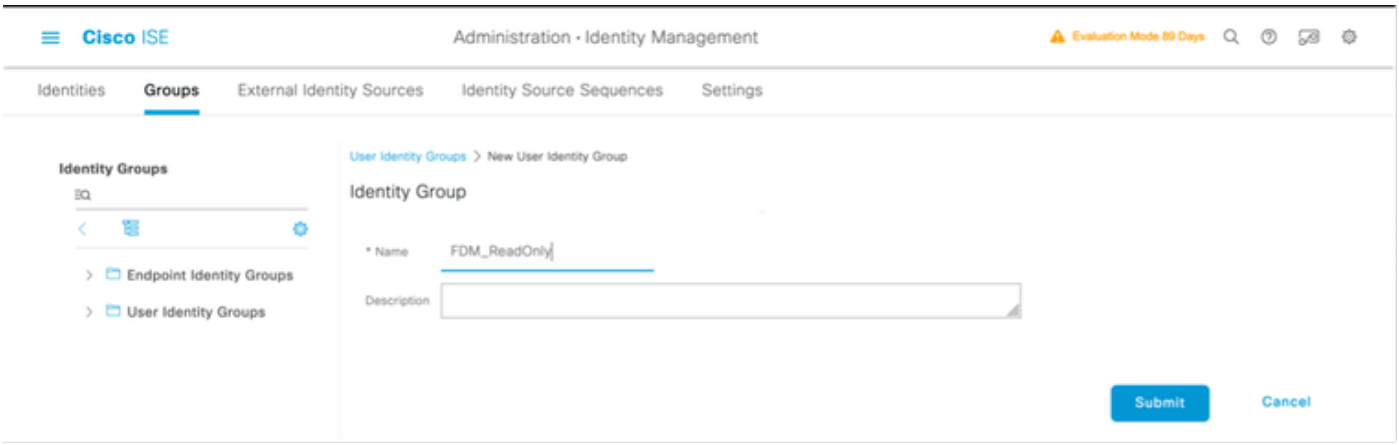


Step 3. Navigate to three lines icon located in the upper left corner and Select on **Administration > Identity Management > Groups**



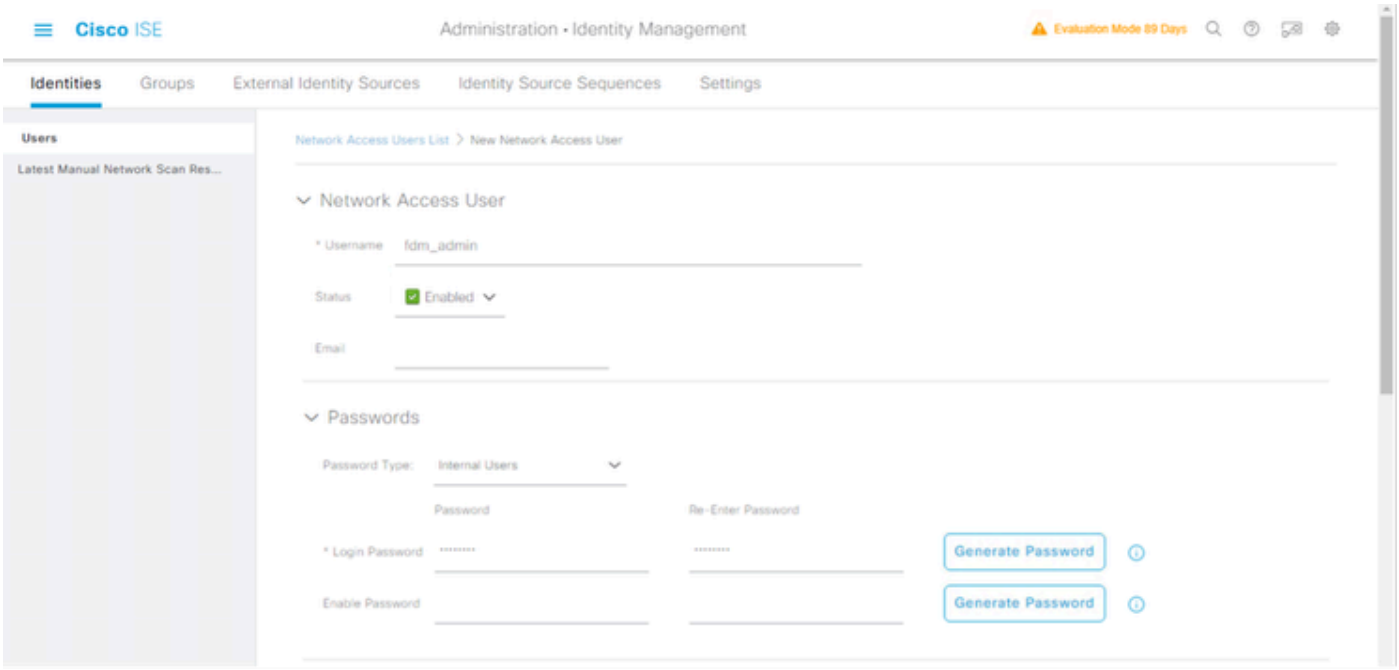
Step 4. Select on User Identity Groups and select on **+Add** button. Define a name and select on **Submit**

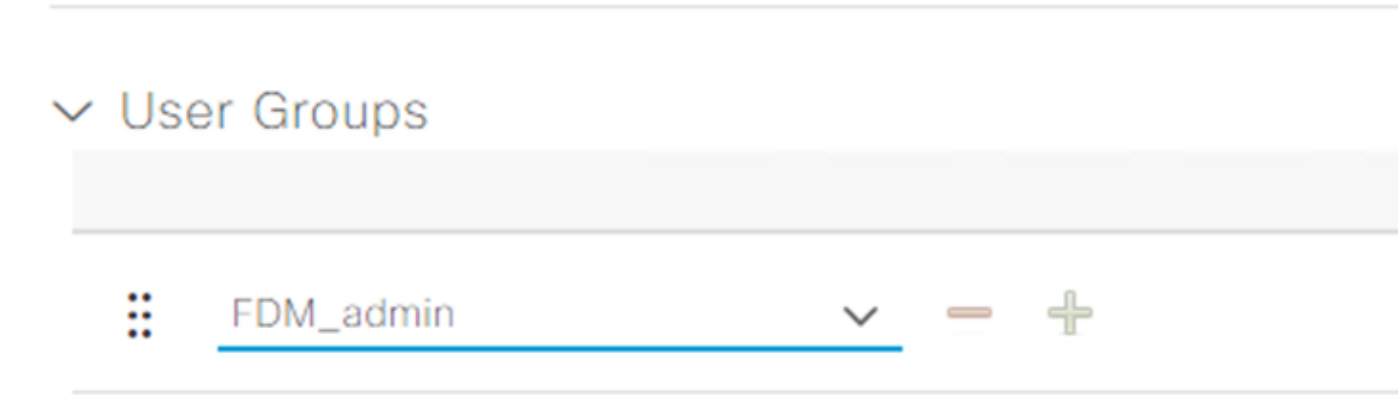


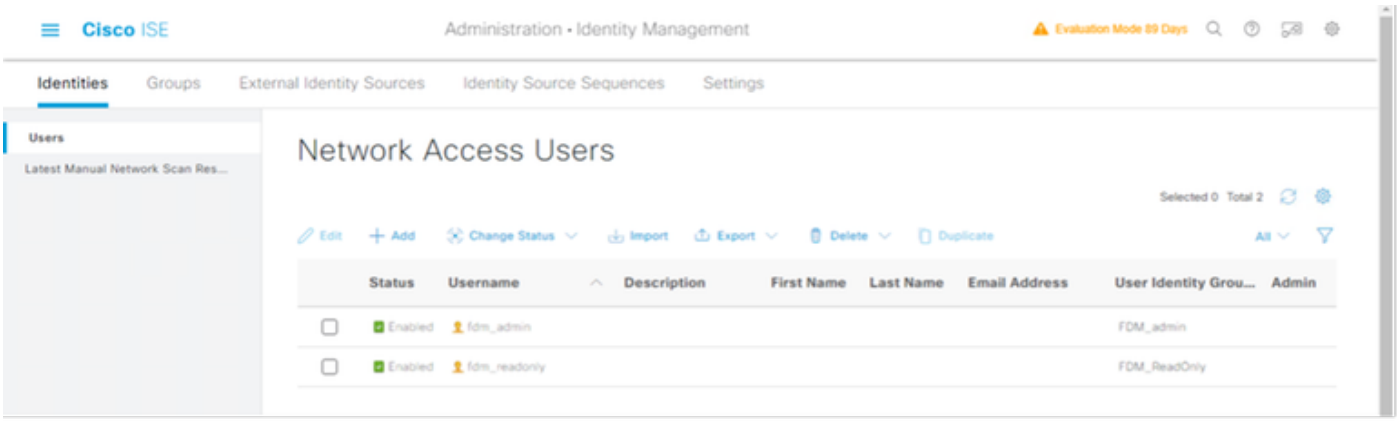


Note: In this example, FDM_Admin and FDM_ReadOnly Identity groups created, you can repeat Step 4 for each type of Admin Users used on FDM.

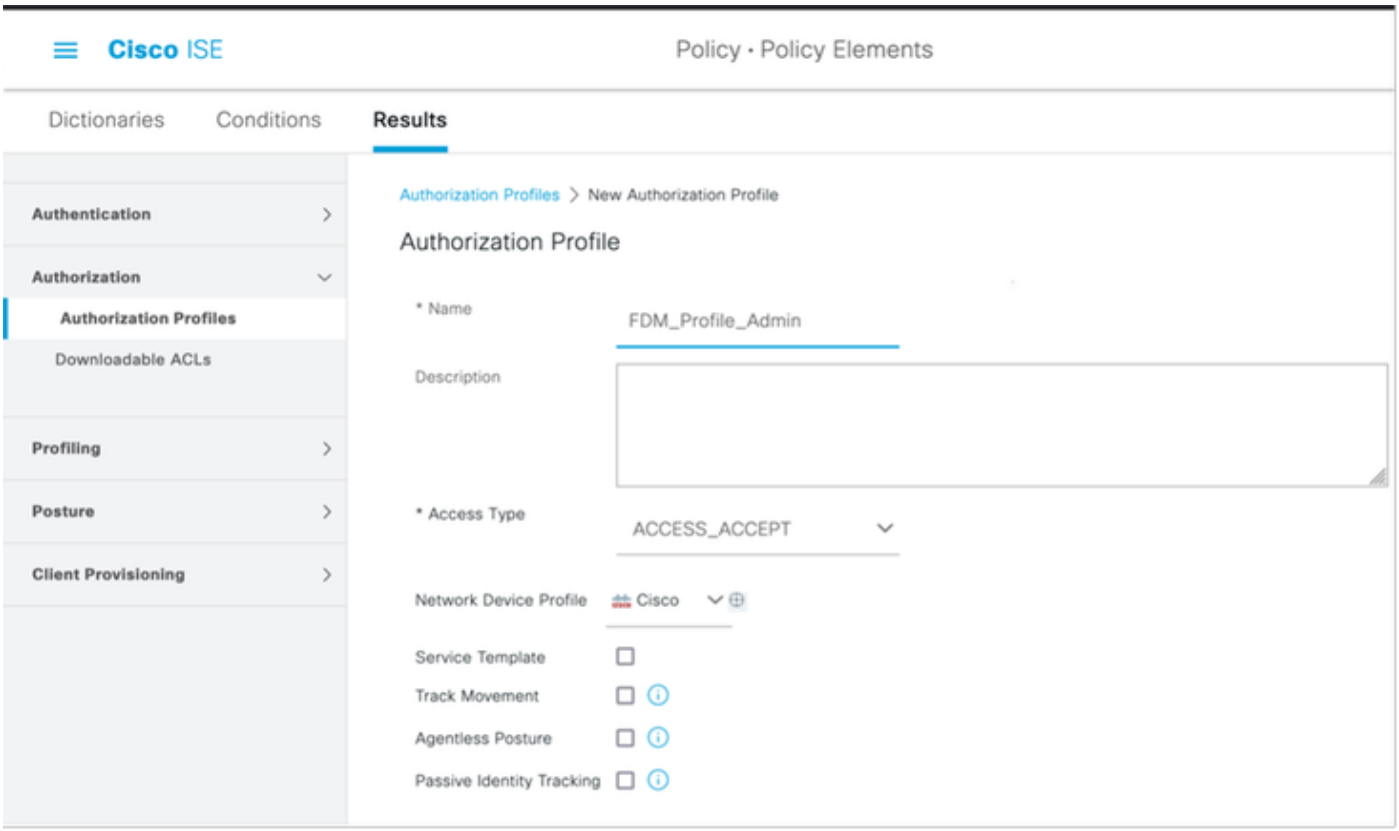
Step 5. Navigate to three lines icon located in the upper left corner and select **Administration > Identity Management > Identities**. Select on **+Add** and define the username and password, then select the group where the user belongs to. In this example, fdm_admin and fdm_readonly users were created and assigned to FDM_Admin and FDM_ReadOnly group respectively.

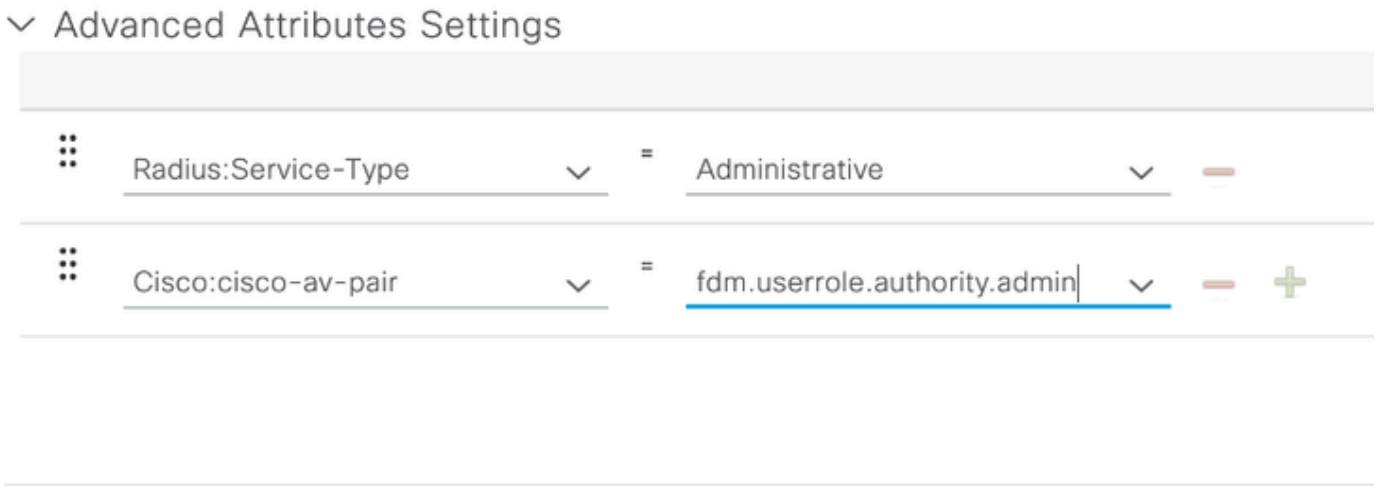


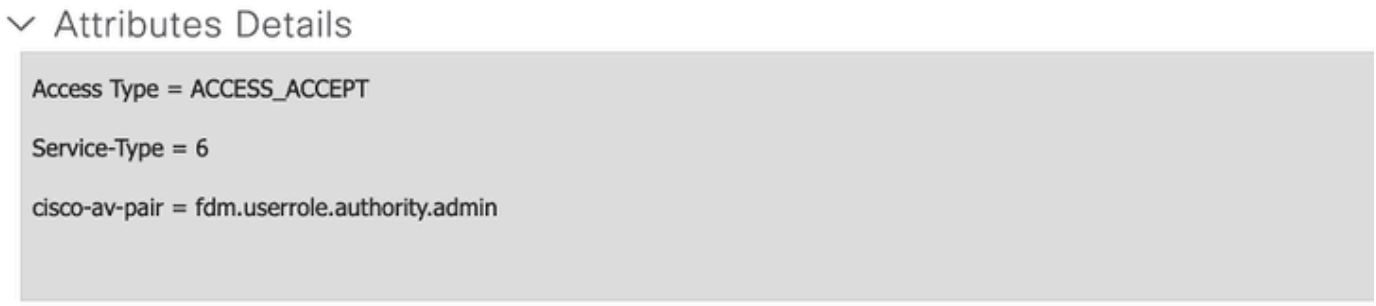


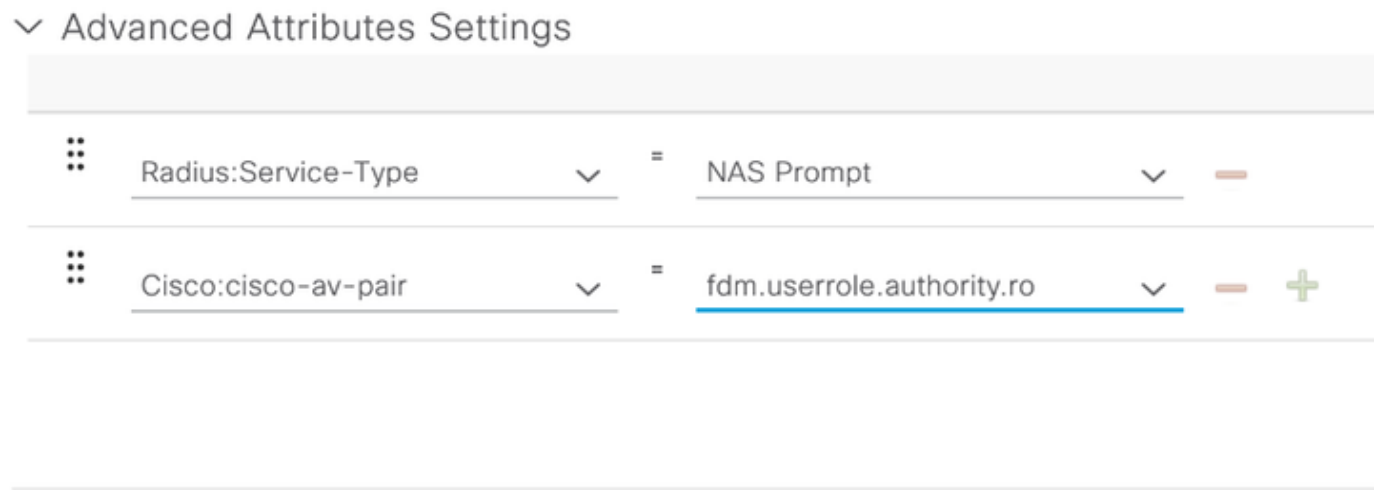


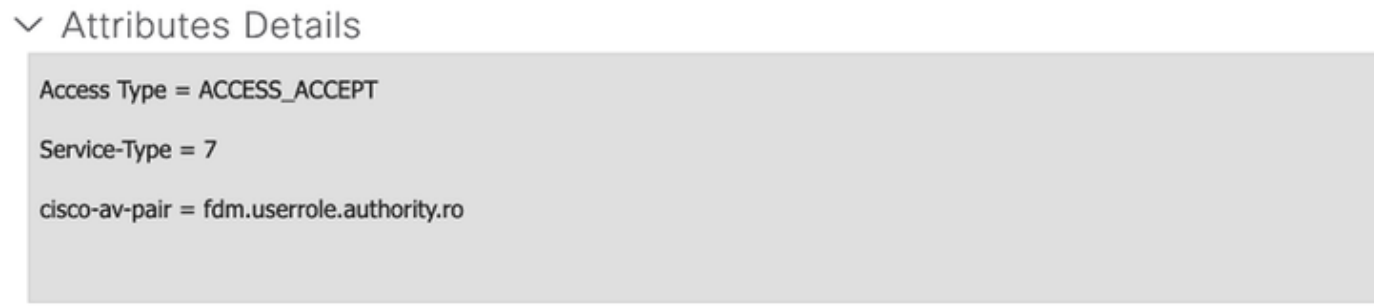
Step 6. Select the three lines icon located in the upper left corner and navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles,** select on **+Add**, define a name for the **Authorization Profile**. Select **Radius Service-type** and select **Administrative**, then select **Cisco-av-pair** and paste the role the admin user gets, in this case, the user receives a full admin privilege (fdm.userrole.authority.admin). Select on **Submit**. Repeat this step for each role, read-only user configured as another example in this document.







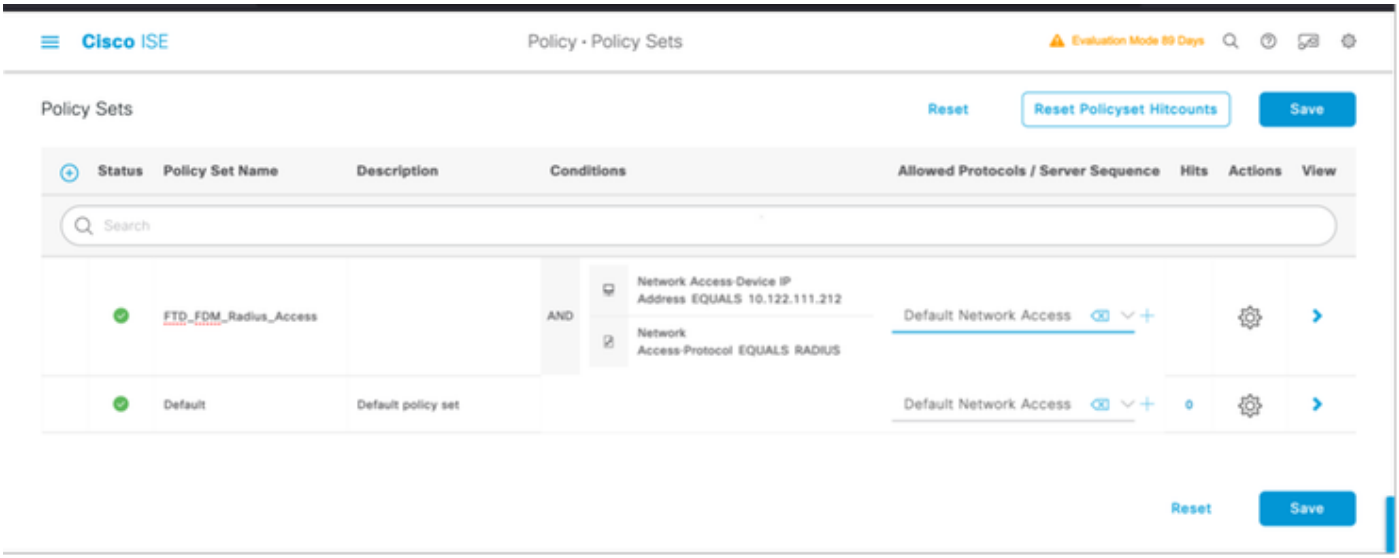




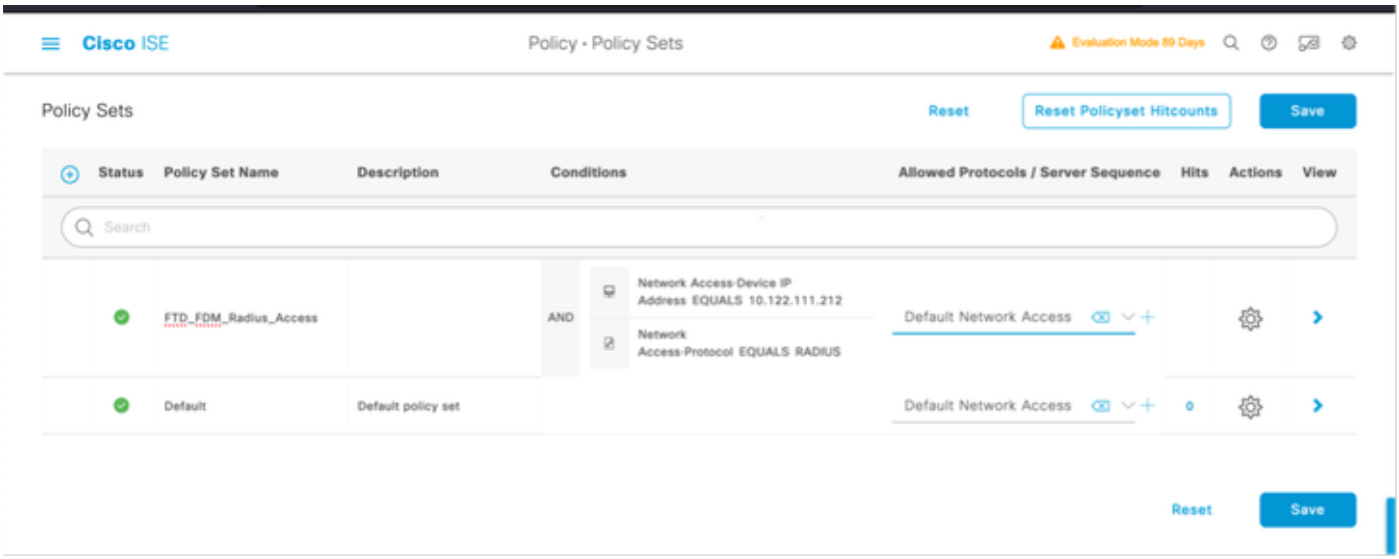
Note: Ensure the order of the Advance attributes section is as with the images example in order to avoid unexpected result when log in with GUI and CLI.

Step 8. Select the three lines icon and navigate to **Policy > Policy Sets.** Select the ⊕ button located near Policy Sets title, define a name and select on the + button in the middle to add a new condition.

Step 9. Under Condition window, select to add an attribute and then select on **Network Device** Icon followed by Network access device IP address. Select **Attribute Value** and add the FDM IP address. Add a new condition and select on **Network Access** followed by Protocol option, select on **RADIUS** and select on Use once done.



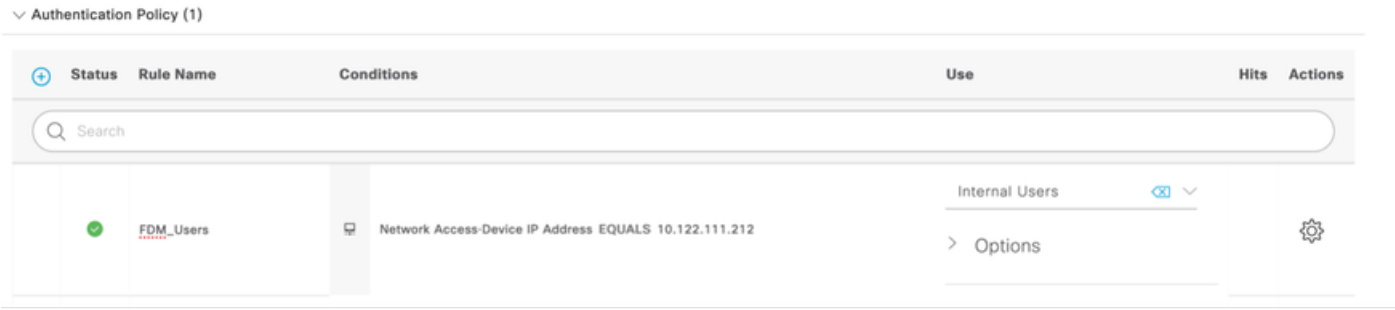
Step 10. Under allow protocols section, select **Device Default Admin**. Select on **Save**



Step 11. Select on the right arrow › icon of the Policy Set to Define authentication and authorization policies

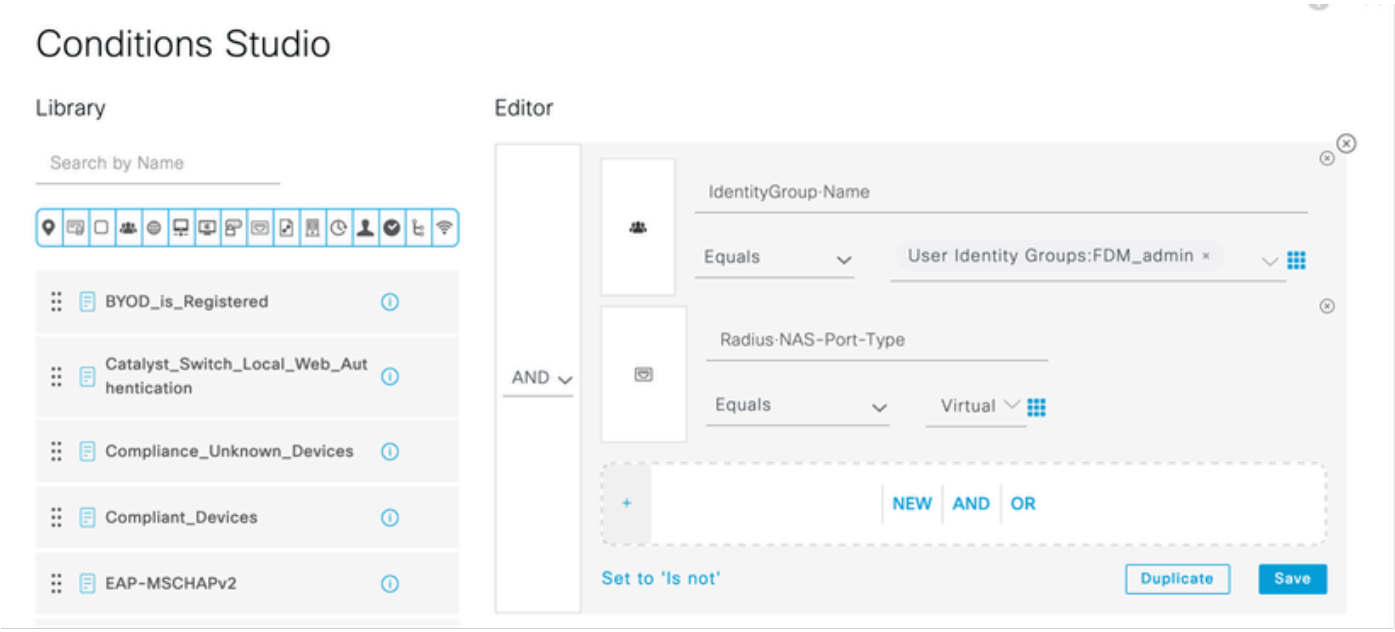
Step 12. Select the ⊕ located near Authentication Policy title, define a name and select on the + in the middle to add a new condition. Under Condition window, select to add an attribute and then select on **Network Device** Icon followed by Network access device IP address. Select on **Attribute Value** and add the FDM IP address. Select on **Use** once done

Step 13. Select **Internal Users** as the Identity Store and select on **Save**



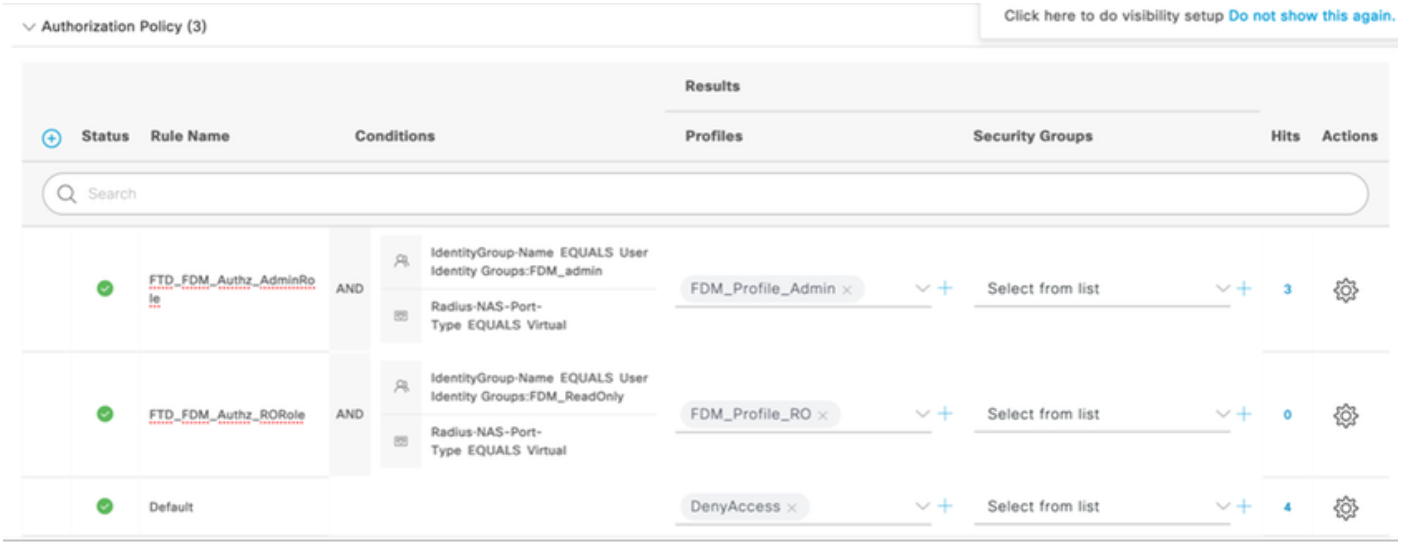
Note: Identity Store can be changed to AD store if ISE is joined to an Active Directory.

Step 14. Select the located near Authorization Policy title, define a name and select on the + in the middle to add a new condition. Under Condition window, select to add an attribute and then select on **Identity Group** icon followed by **Internal User:Identity Group.** Select the FDM_Admin Group, Select the **AND** along with **NEW** option to add a new condition, select on port icon followed by **RADIUS NAS-Port-Type:Virtual** and select on Use.



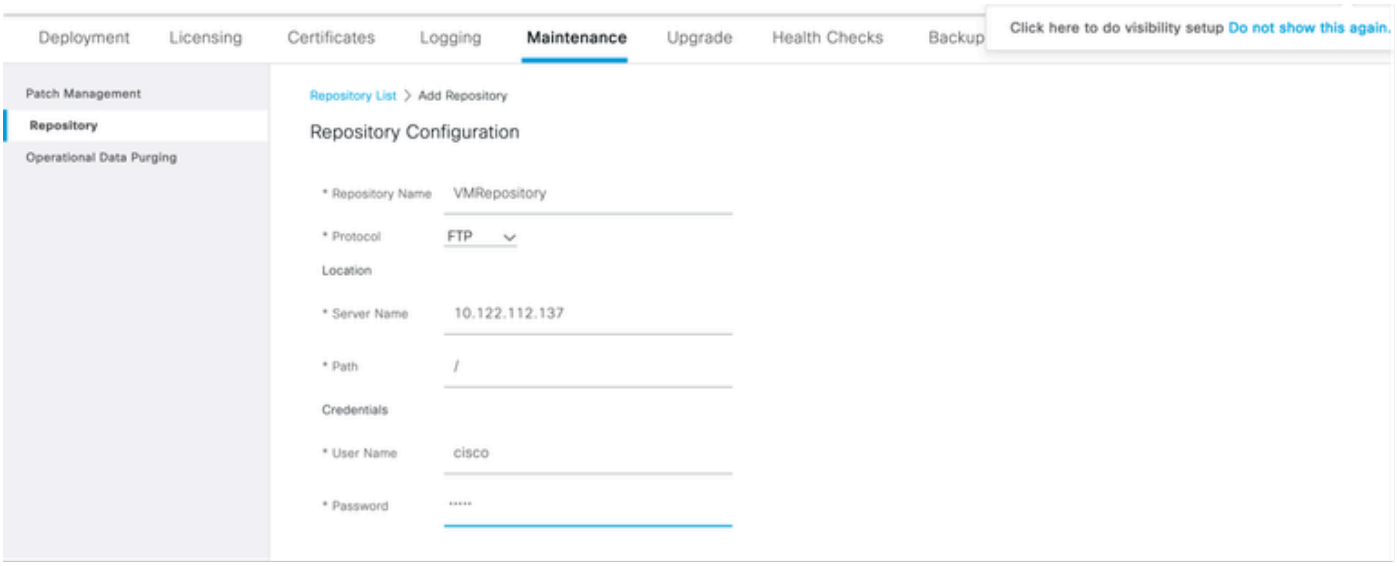
Step 15. Under Profiles, select the profile created in Step 6 and then select on **Save**

Repeat Step 14 and 15 for FDM_ReadOnly group



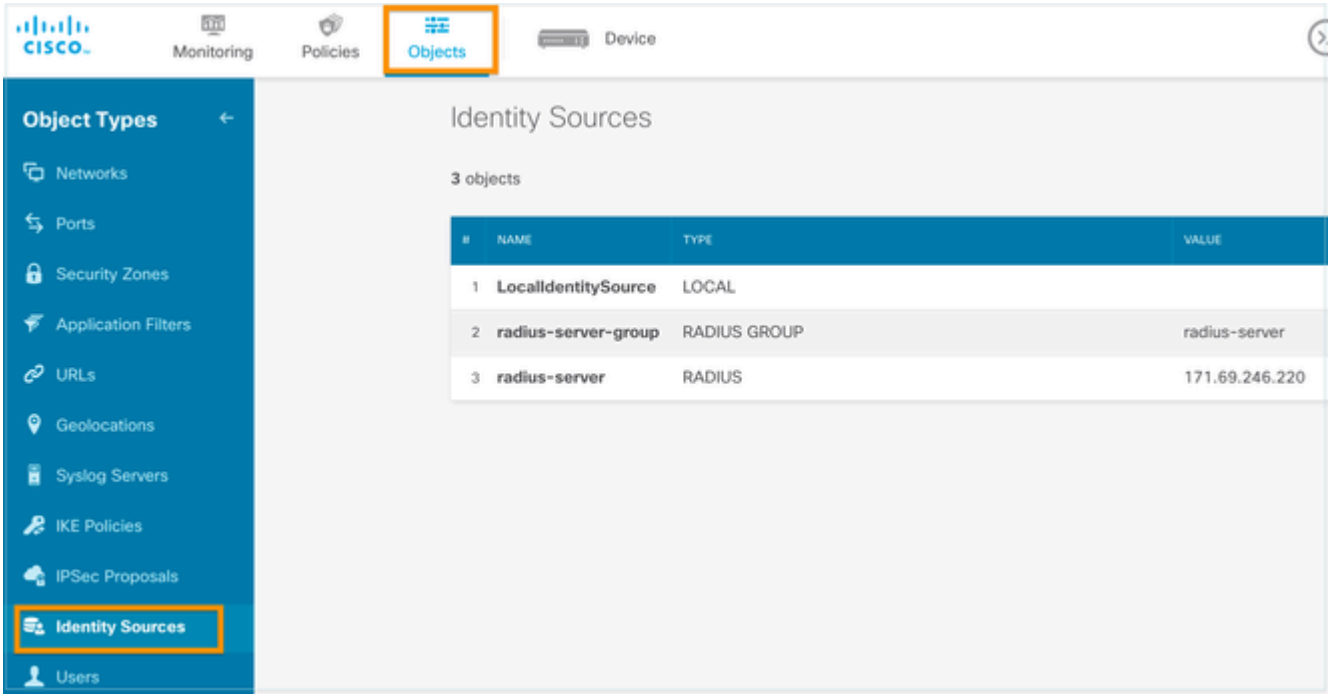
Step 16 (Optional). Navigate to three lines icon located in the upper left corner and select on **Administration > System > Maintenance > Repository** and select on **+Add** to add a repository used to store TCP Dump file for troubleshoot purposes.

Step 17 (Optional). Define a repository Name, protocol, Server Name, path and Credentials. Select on **Submit** once done.

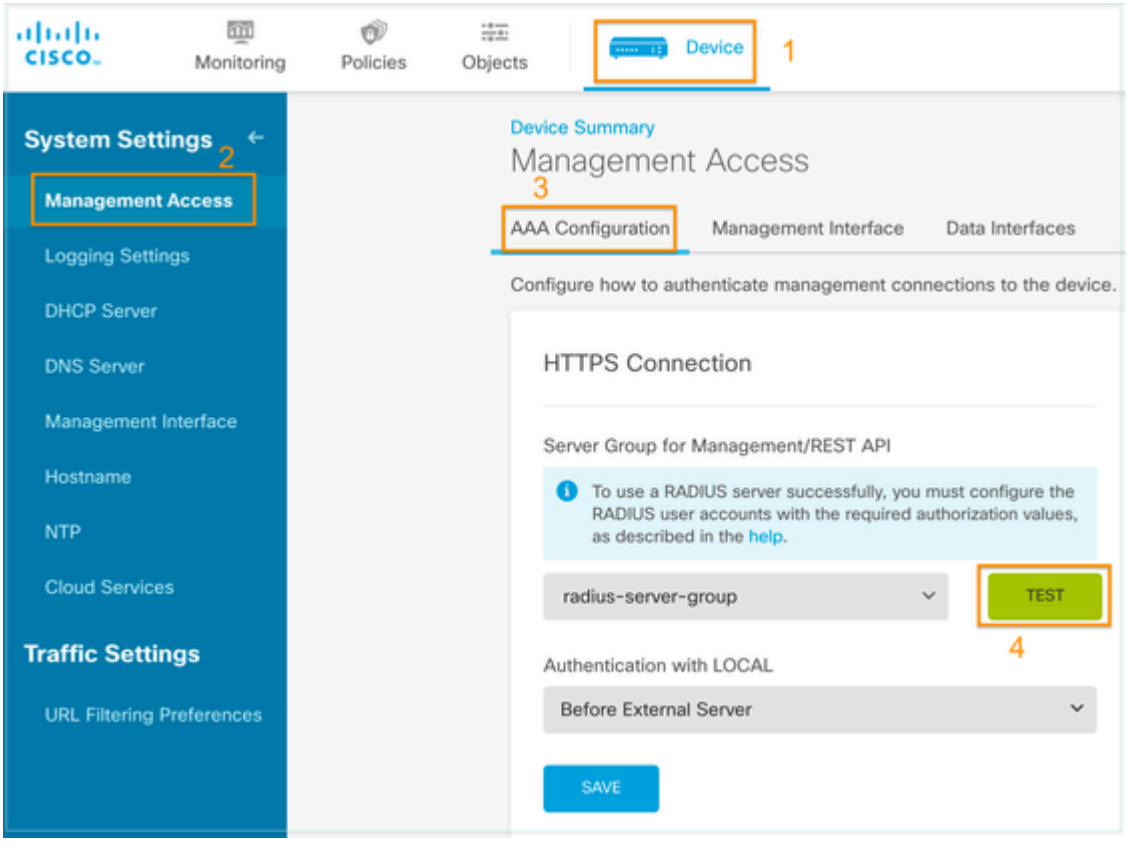


Verify

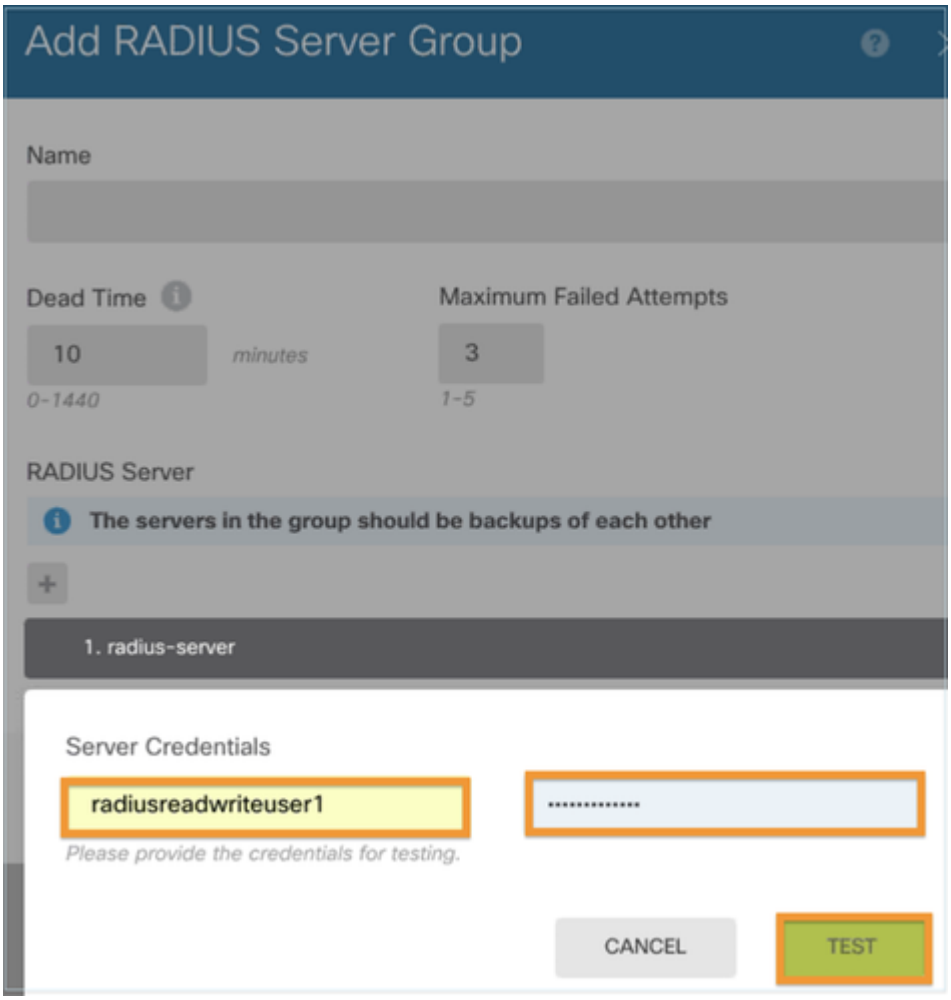
Step 1. Navigate to **Objects > Identity Sources** tab and verify RADIUS Server and Group Server configuration



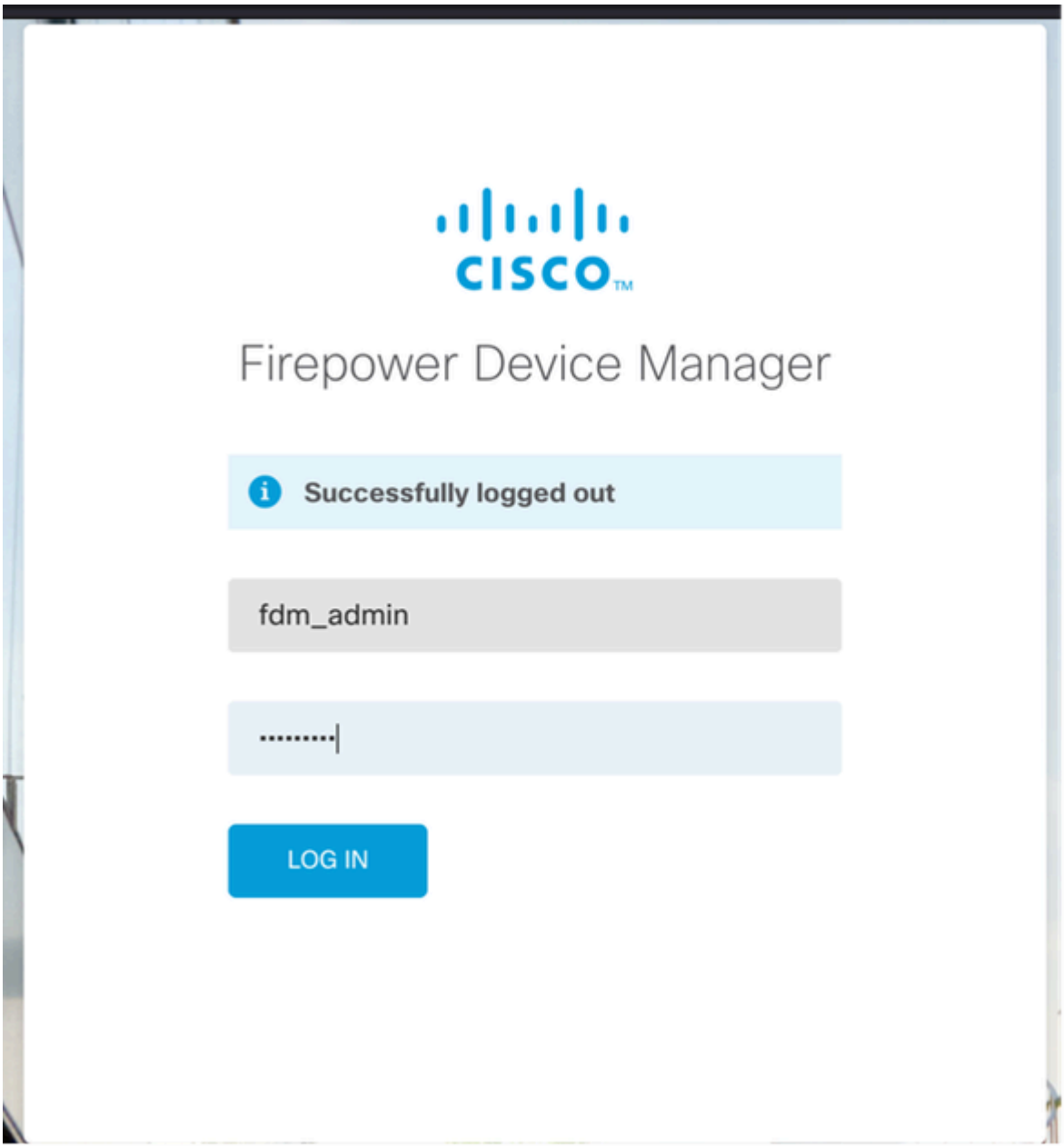
Step 2. Navigate to **Device > System Settings > Management Access** tab and select the **TEST** button



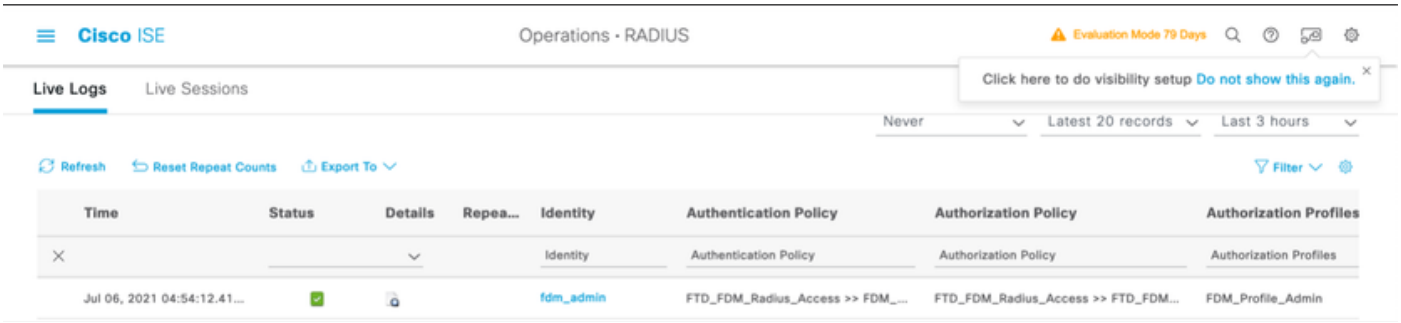
Step 3. Insert user credentials and select the **TEST** button



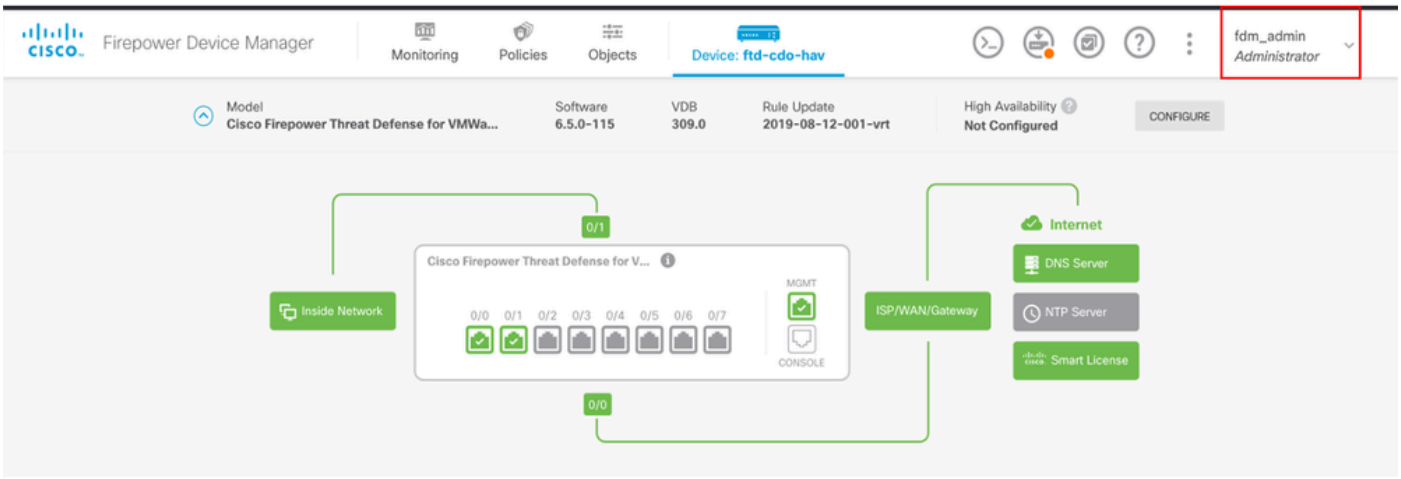
Step 4. Open a new window browser and type https://FDM_ip_Address, use fdm_admin username and password created on step 5 under ISE configuration section.



Successful log in attempt can be verified on ISE RADIUS live logs



Admin User can also be reviewed on FDM on the upper right corner



Cisco Firepower Device Manager CLI (Admin User)

```
[ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212                      ]
 The authenticity of host '10.122.111.212 (10.122.111.212)' can't be established.
 ECDSA key fingerprint is SHA256:sqpyFmCcGBslEjjDMdHnrkqdw40qvc7ne1I+Pjw6fJs.
 Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
 Warning: Permanently added '10.122.111.212' (ECDSA) to the list of known hosts.
[Password:                                                                     ]
 !!! New external username identified. Please log in again to start a session. !!
 !

 Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
 Cisco is a registered trademark of Cisco Systems, Inc.
 All other trademarks are property of their respective owners.

 Cisco Fire Linux OS v6.5.0 (build 4)
 Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

 Connection to 10.122.111.212 closed.

[ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212
[Password:
 Last login: Tue Jul  6 17:01:20 UTC 2021 from 10.24.242.133 on pts/0

 Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
 Cisco is a registered trademark of Cisco Systems, Inc.
 All other trademarks are property of their respective owners.

 Cisco Fire Linux OS v6.5.0 (build 4)
 Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

[>
```

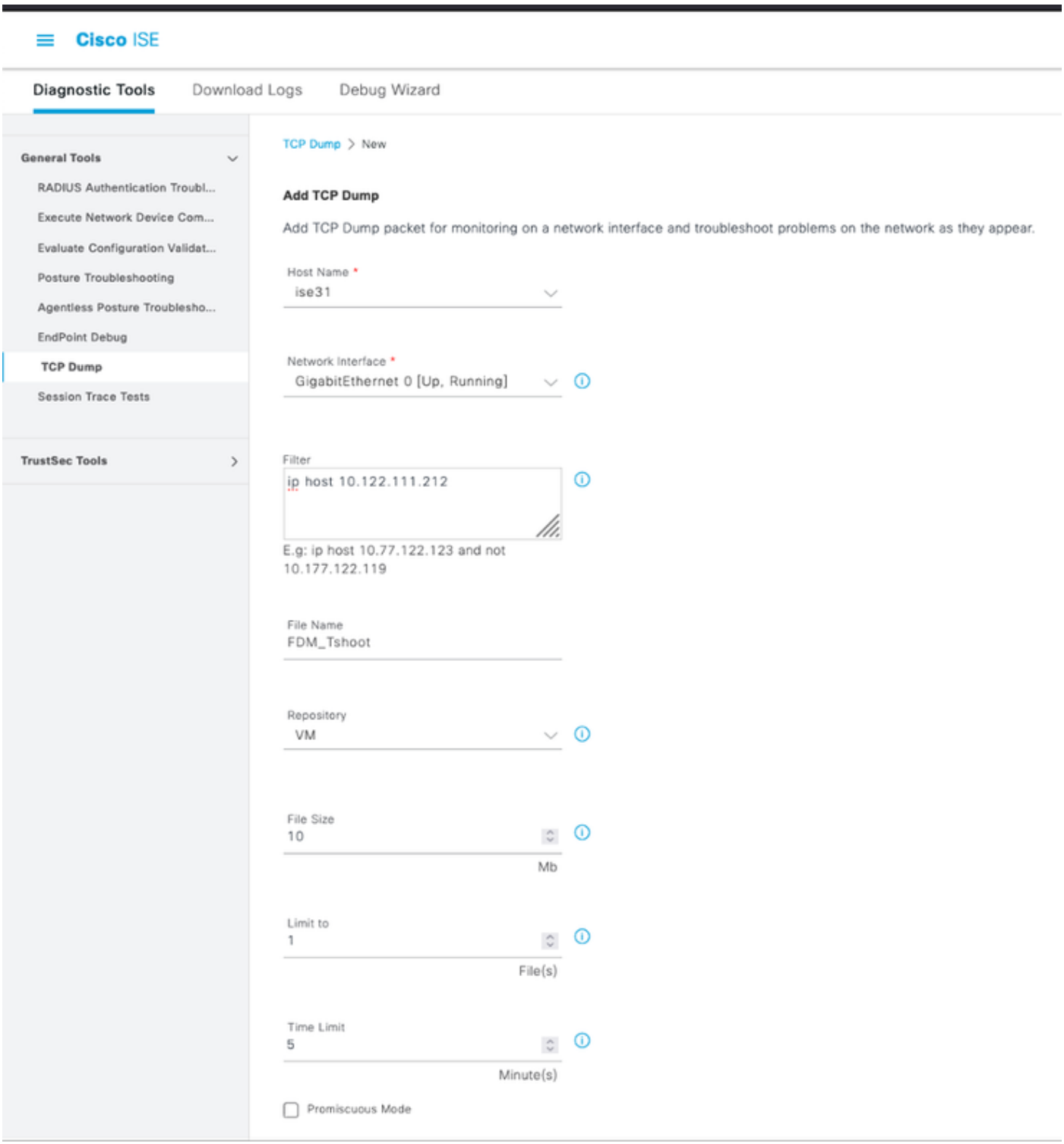
Troubleshoot

This section provides the information you can use to troubleshoot your configuration.

Communication validation with TCP Dump tool on ISE

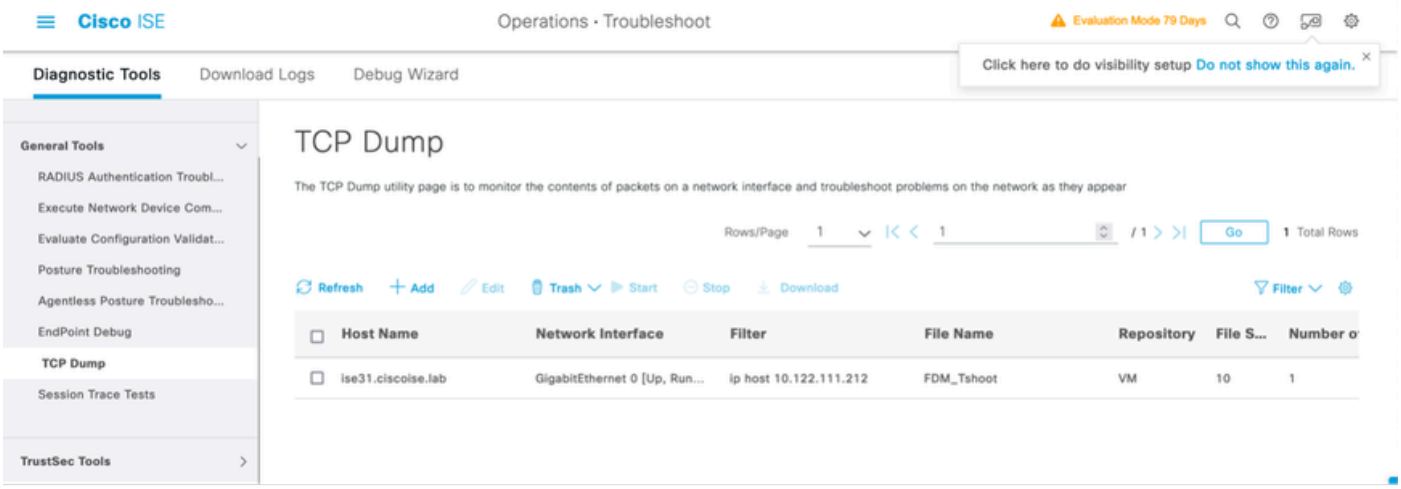
Step 1. Log in on ISE and select the three lines icon located in the upper left corner and navigate to **Operations > Troubleshoot > Diagnostic Tools.**

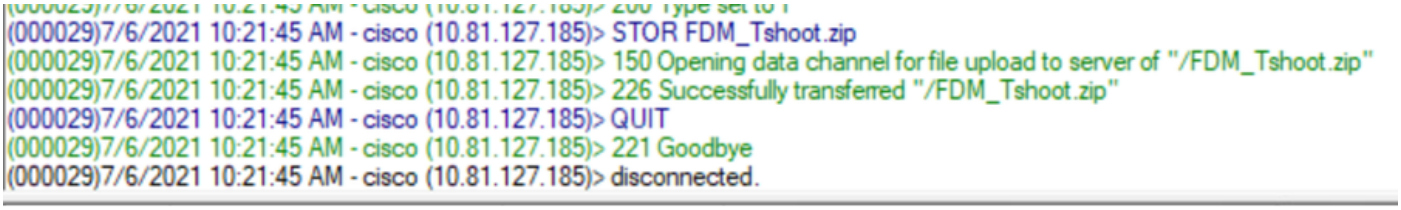
Step 2. Under General tools select on TCP Dumps and then select on **Add+**. Select Hostname, Network Interface File Name, Repository, and optionally a filter to gather only FDM IP address communication flow. Select on **Save and Run**

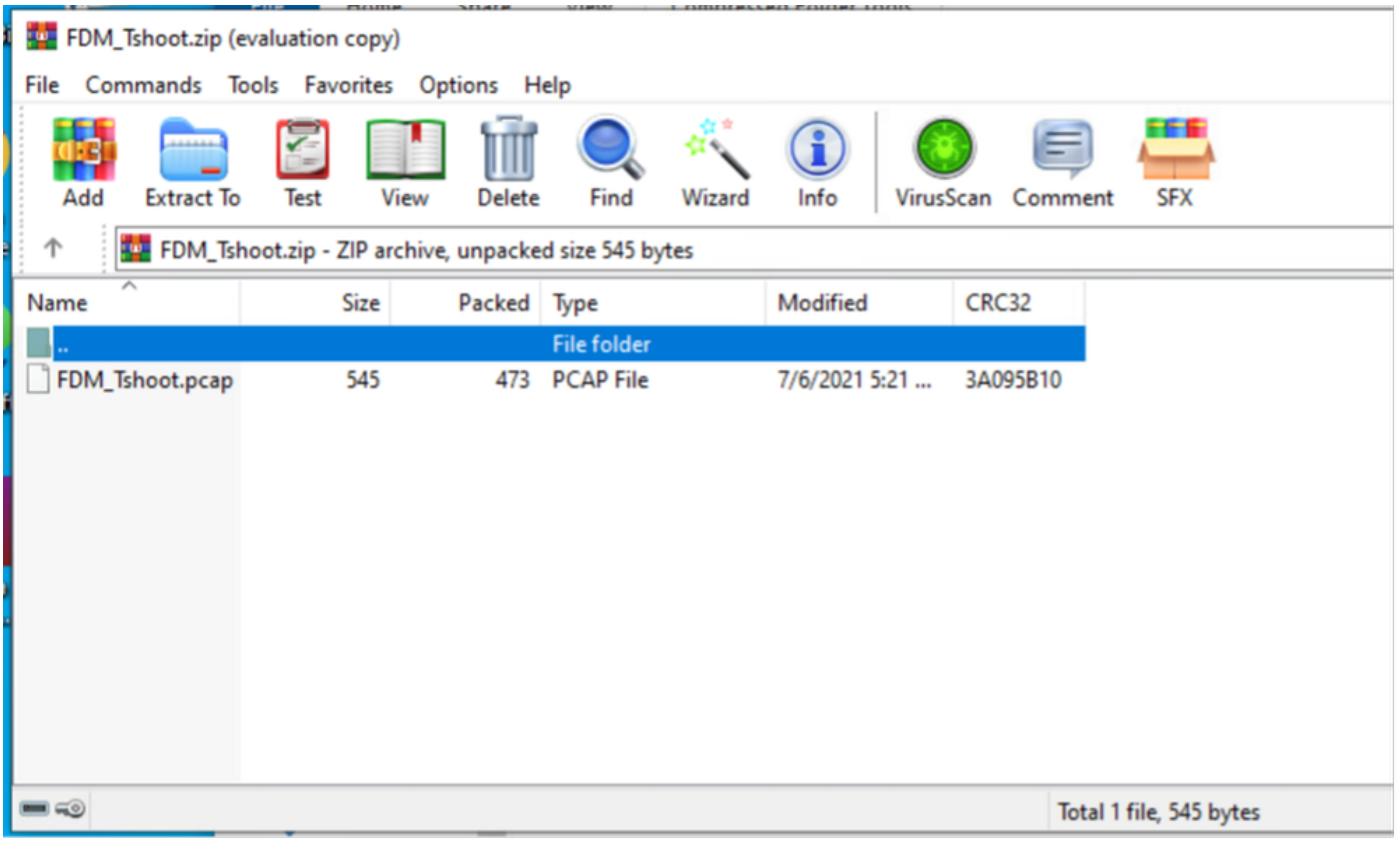


Step 3. Log in on FDM UI and type the admin credentials.

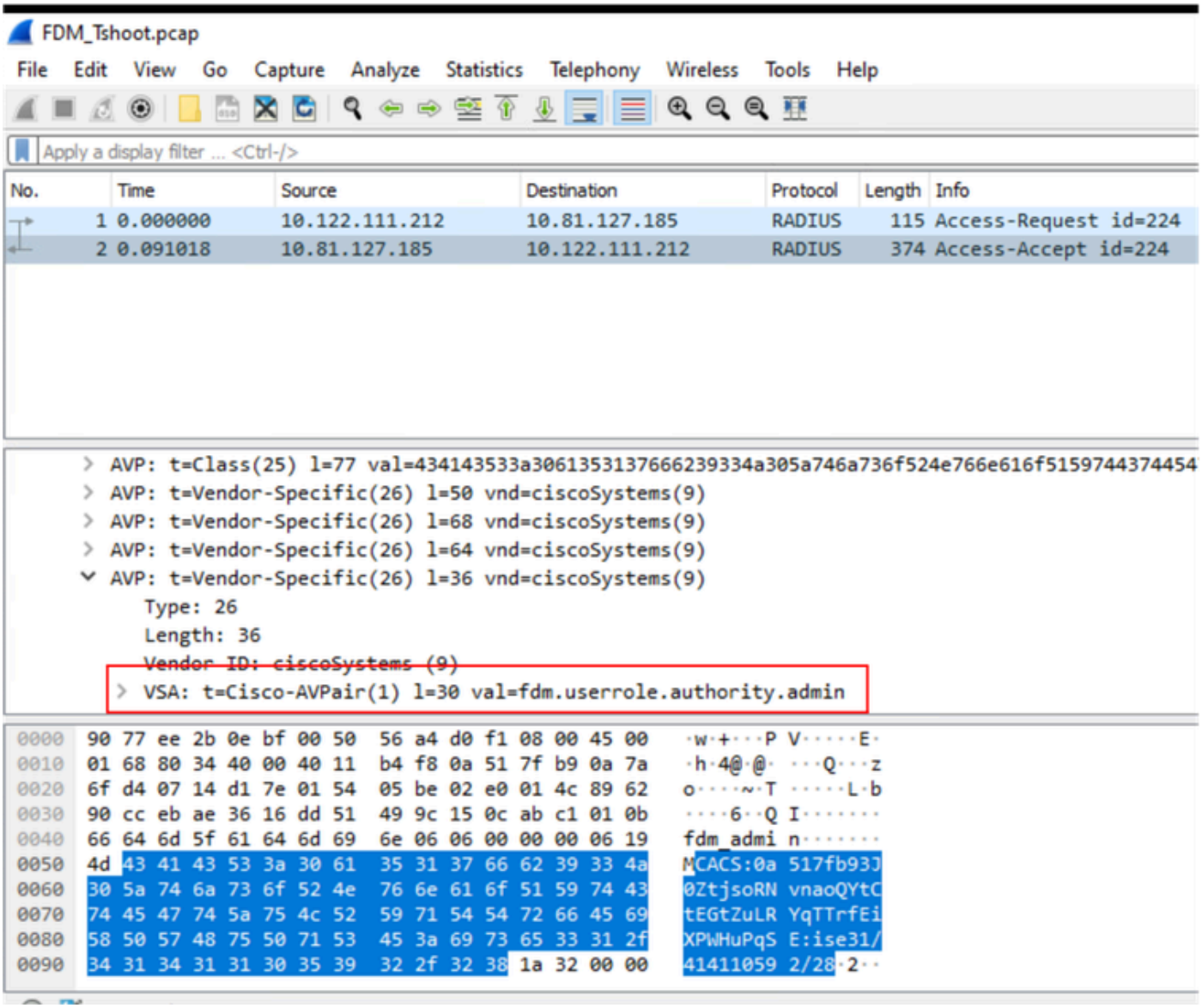
Step 4. On ISE, select on **Stop** button and verify the pcap file has been sent to the defined repository.







Step 5. Open the pcap file to validate the successful communication between FDM and ISE.



If no entries are shown on pcap file validate the next options:

1. Right ISE IP address has been added on FDM configuration
2. In case of a firewall is in the middle verify port 1812-1813 is permitted.
3. Check communication between ISE and FDM

Communication validation with FDM generated file.

In troubleshoot file generated from FDM Device page look for keywords:

- FdmPasswordLoginHelper
- NGFWDefaultUserMgmt
- AAAIdentitySourceStatusManager
- RadiusIdentitySourceManager

All the logs related to this feature can be found in /var/log/cisco/ngfw-onbox.log

References:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-mgmt.html#id_73793

Common Issues

Case 1 - External Auth not working

- Check secretKey, port, or hostname
- Misconfiguration of AVPs on RADIUS
- Server can be in ‘Dead Time’

Case 2 -Test IdentitySource fails

- Make sure the changes to object are saved
- Make sure the credentials are correct

Limitations

- FDM allows max of 5 active FDM sessions.
- Creation of 6th session results in the 1st session revoked
- Name of RadiusIdentitySourceGroup cannot be “LocalIdentitySource”
- Max of 16 RadiusIdentitySources to a RadiusIdentitySourceGroup
- Misconfiguration of AVPs on RADIUS result in Denying access to FDM

Q&A

Q: Does this feature work in Evaluation mode?

A: Yes

Q: If two read-only users log in, where have access to read-only user 1, and they log in from two diff browsers. How does it show? What happens?

A: Both user's sessions are shown in the active user sessions page with the same name. Each entry shows an individual value for the time stamp.

Q: What is the behavior is the external radius server provides an access reject vs. "no response" if you have local auth configured 2nd?

A: You can try LOCAL auth even if you get Access reject or no response if you have local auth configured 2nd.

Q: How ISE differentiates a RADIUS request for admin log in vs. RADIUS request to authenticate an RA VPN user

A: ISE doesn’t differentiate a RADIUS request for Admin Vs RAVPN users. FDM looks at cisco-avpair attribute to figure out Authorization for Admin access. ISE sends all the attributes configured for the user in both the cases.

Q: That means ISE logs is not be able to differentiate between an FDM admin log in and that same user accessing remote access VPN on same device. Is there any RADIUS attribute passed to ISE in the access request that ISE can key on?

A: These are the upstream RADIUS attributes that are sent from the FTD to ISE during RADIUS authentication for RAVPN. These are not sent as part of External Auth Management Access Request and can be used to differentiate a FDM administration log in Vs RAVPN user log in.

146 - Tunnel Group Name or Connection Profile Name.

150 – Client Type (Applicable values: 2 = AnyConnect Client SSL VPN, 6 = AnyConnect Client IPsec VPN (IKEv2).

151 – Session Type (Applicable values: 1 = AnyConnect Client SSL VPN, 2 = AnyConnect Client IPSec VPN (IKEv2).