使用RADIUS配置ISE的FDM外部身份验证和授权

目录

简介

本文档介绍将Cisco Firepower设备管理器(FDM)与身份服务引擎(ISE)集成，以便管理员用户通过RADIUS协议进行身份验证，从而实现GUI和CLI访问。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower设备管理器(FDM)
- 身份服务引擎 (ISE)
- RADIUS协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower威胁防御(FTD)设备，所有平台Firepower设备管理器(FDM)版本6.3.0+
- ISE版本3.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

互操作性

- 用户配置有用户角色的RADIUS服务器
- 必须在RADIUS服务器上使用cisco-av-pair配置用户角色
- Cisco-av-pair = fdm.userrole.authority.admin
- ISE可用作RADIUS服务器

许可

无特定许可证要求，基本许可证就足够了

背景信息

此功能允许客户使用RADIUS为这些用户配置外部身份验证和多个用户角色。

RADIUS支持Management Access，具有3个系统定义的用户角色：

- 只读
- READ_WRITE（无法执行系统关键操作，如升级、还原等）
- 管理员

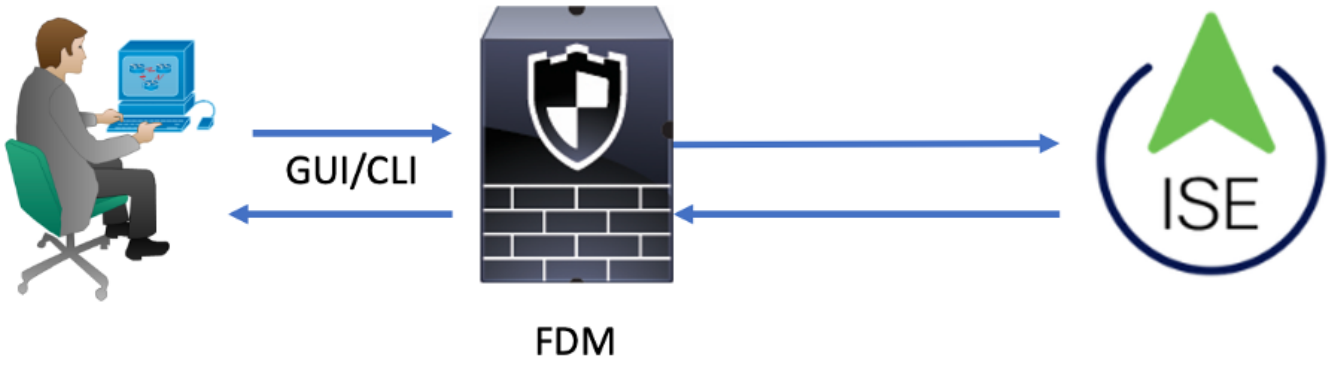
可以测试RADIUS服务器的配置，监控活动用户会话和删除用户会话。

此功能在FDM 6.3.0版中实施。在6.3.0版本之前，FDM仅支持一个用户（管理员）。

默认情况下，Cisco Firepower设备管理器对用户进行本地身份验证和授权，以便采用集中式身份验证和授权方法，您可以通过RADIUS协议使用思科身份服务引擎。

网络图

下一张图片提供了网络拓扑的示例



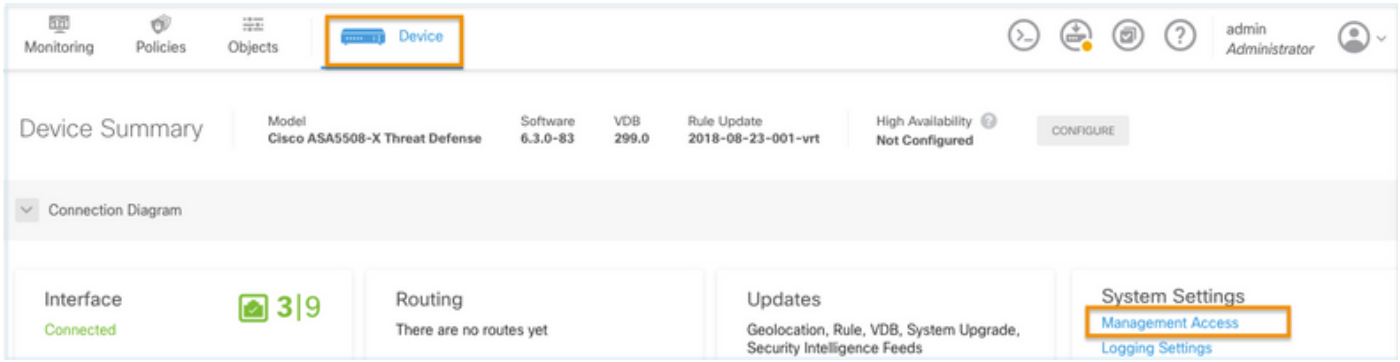
Process:

1. 管理员用户引入其凭证。
2. 身份验证过程已触发，ISE在本地或通过Active Directory验证凭证。
3. 身份验证成功后，ISE会向FDM发送用于身份验证和授权信息的Permit数据包。
4. 帐户在ISE上执行，并且身份验证活动日志成功。

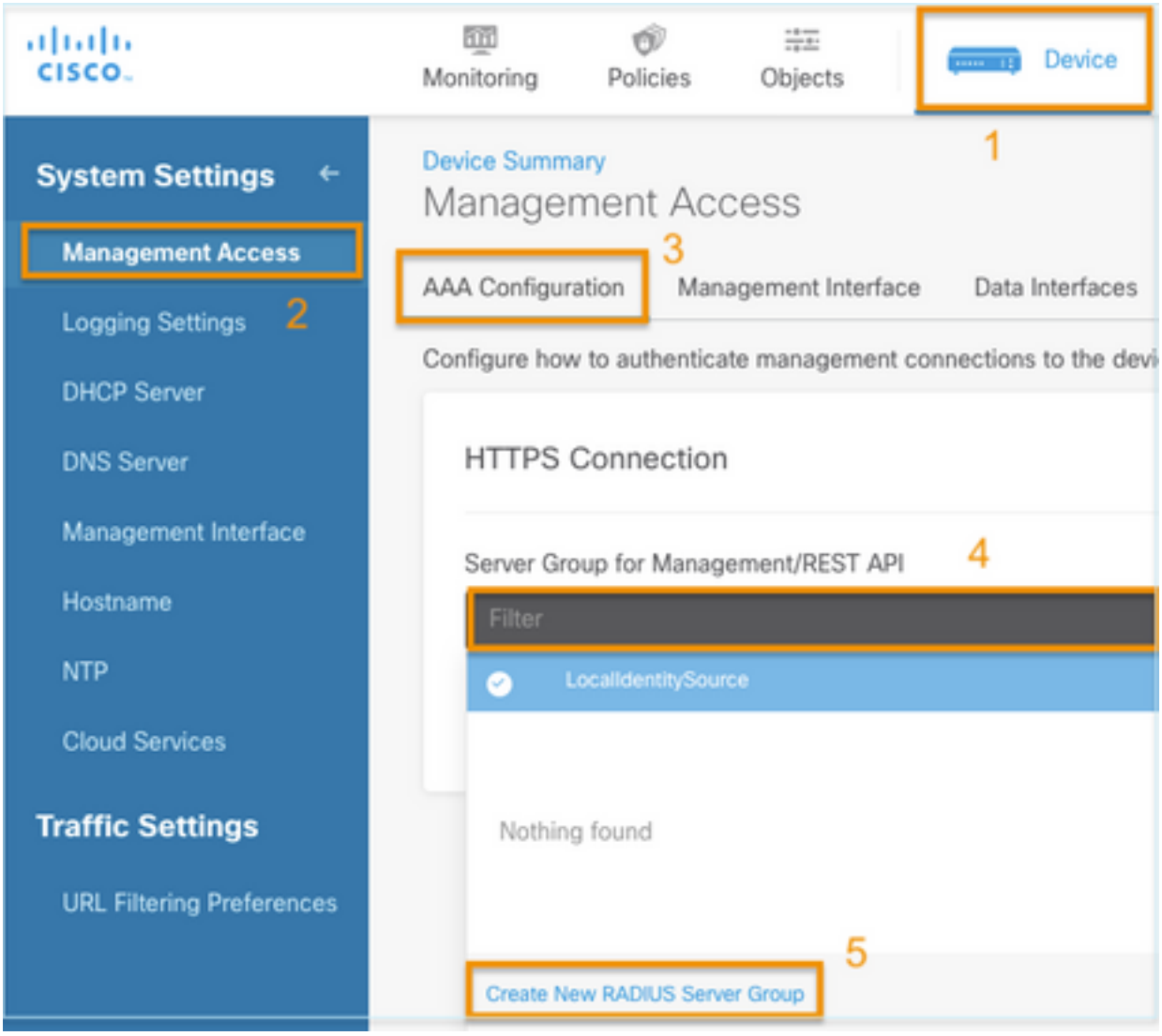
配置

FDM 配置

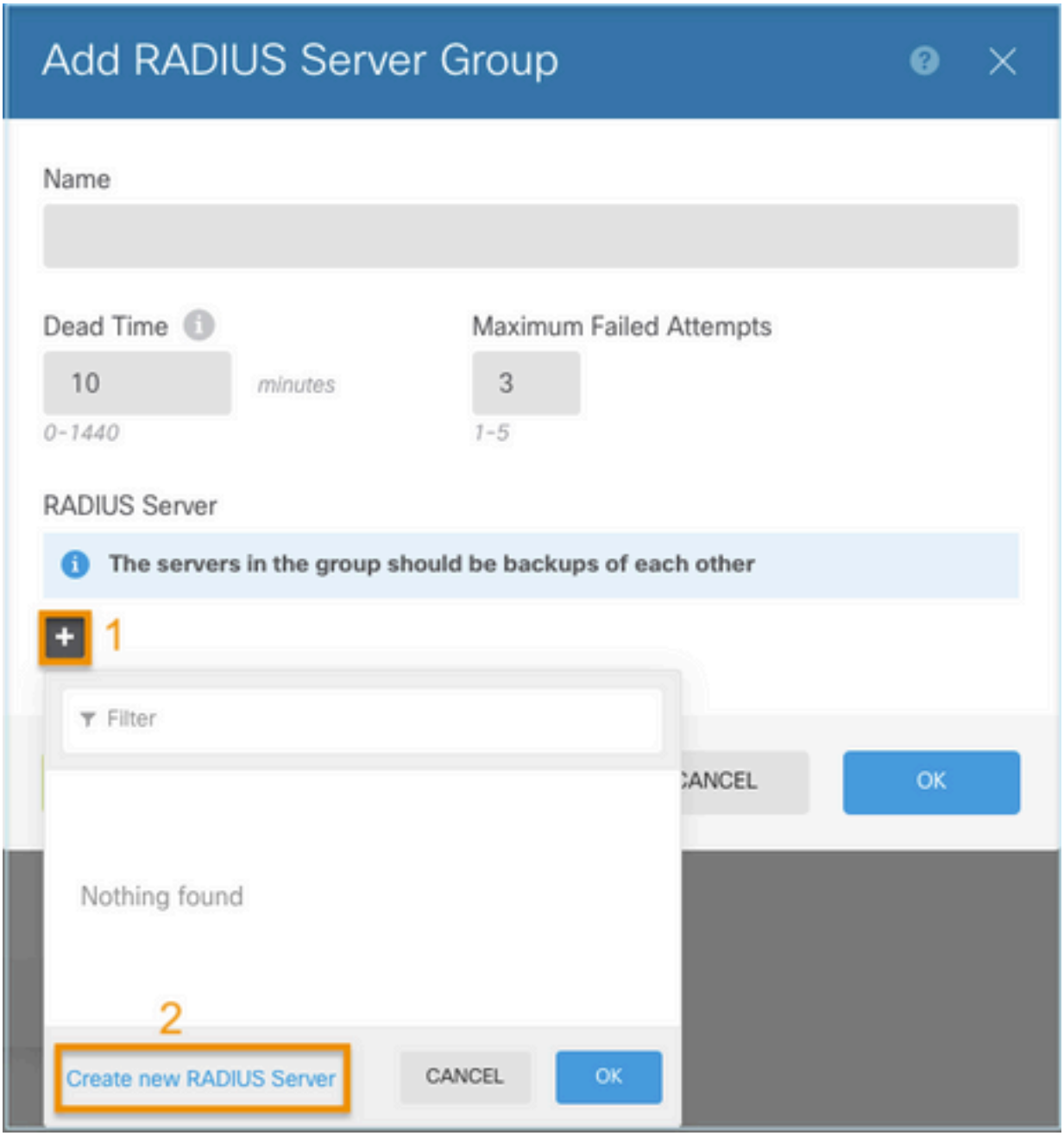
步骤1:登录到FDM，然后导航到“设备”>“系统设置”>“管理访问”选项卡

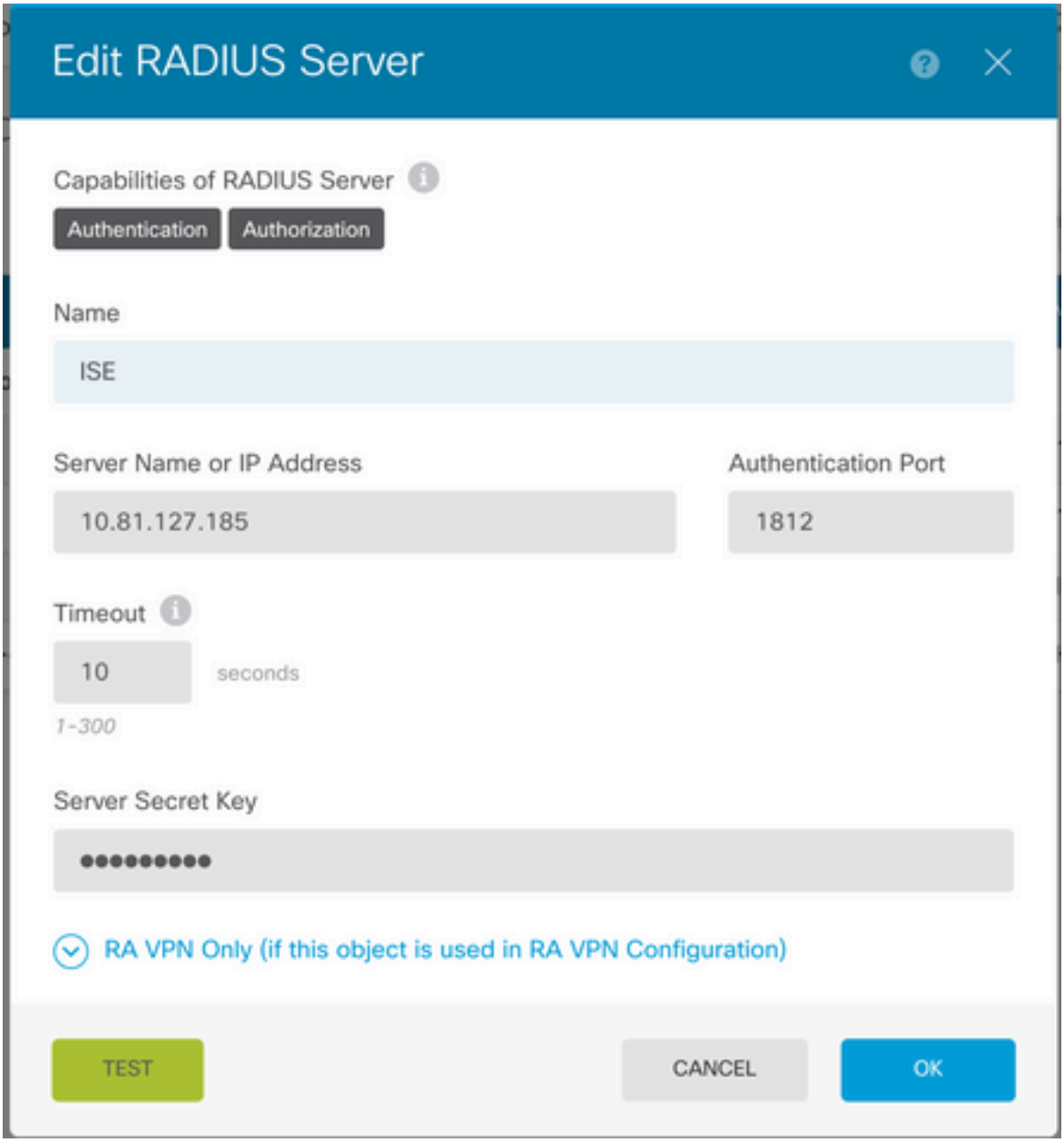


第二步：创建新的RADIUS服务器组

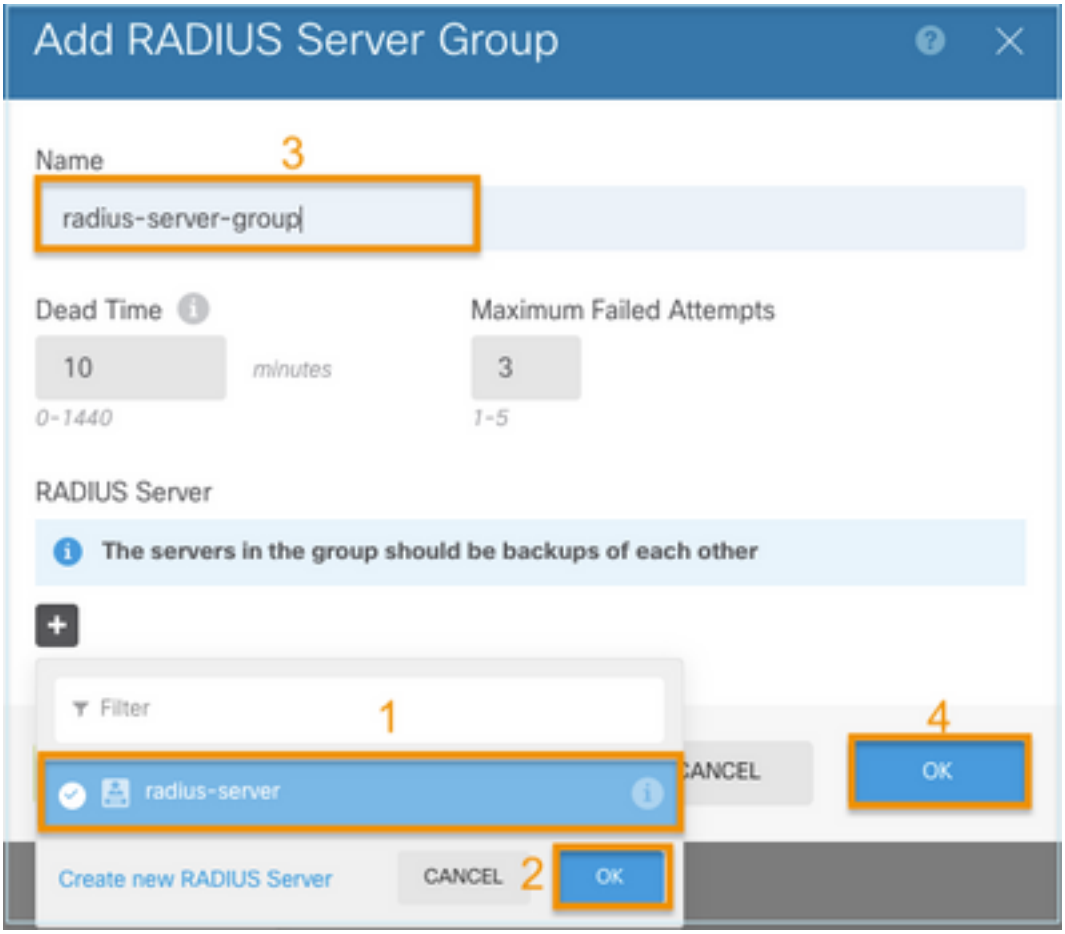


第三步：创建新的RADIUS服务器

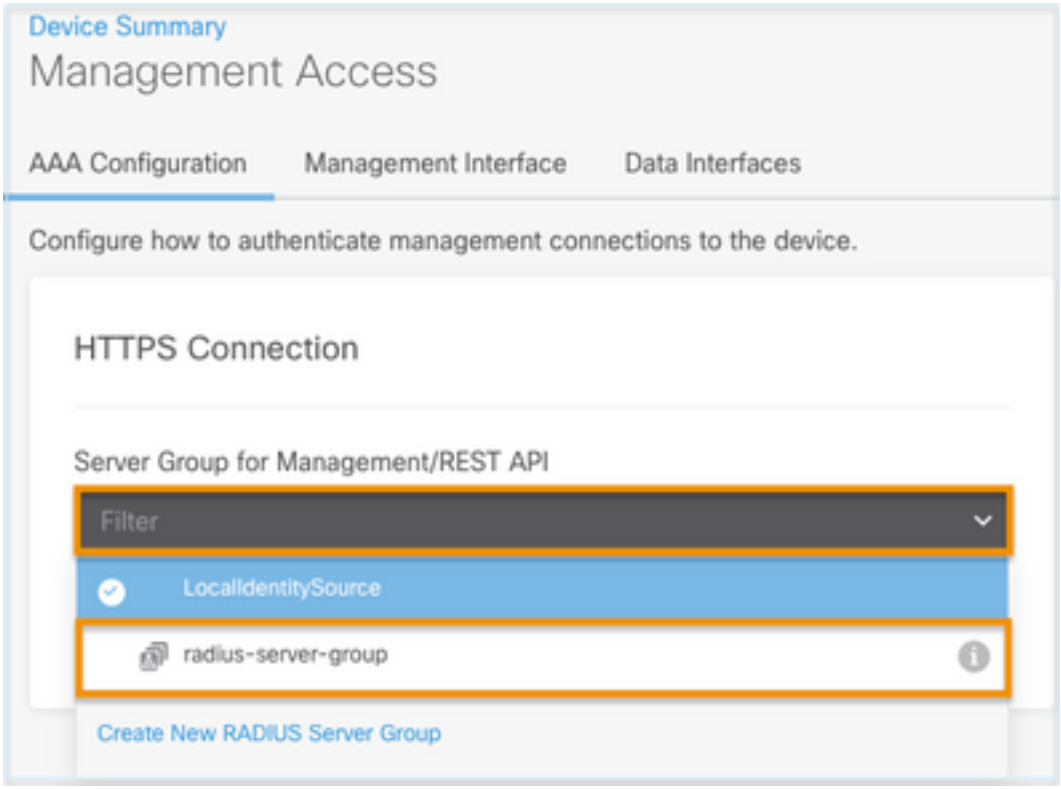

Add RADIUS Server Group
Name
Dead Time
10
minutes
0-1440
Maximum Failed Attempts
3
1-5
RADIUS Server
The servers in the group should be backups of each other
1
Filter
CANCEL
OK
Nothing found
2
Create new RADIUS Server
CANCEL
OK

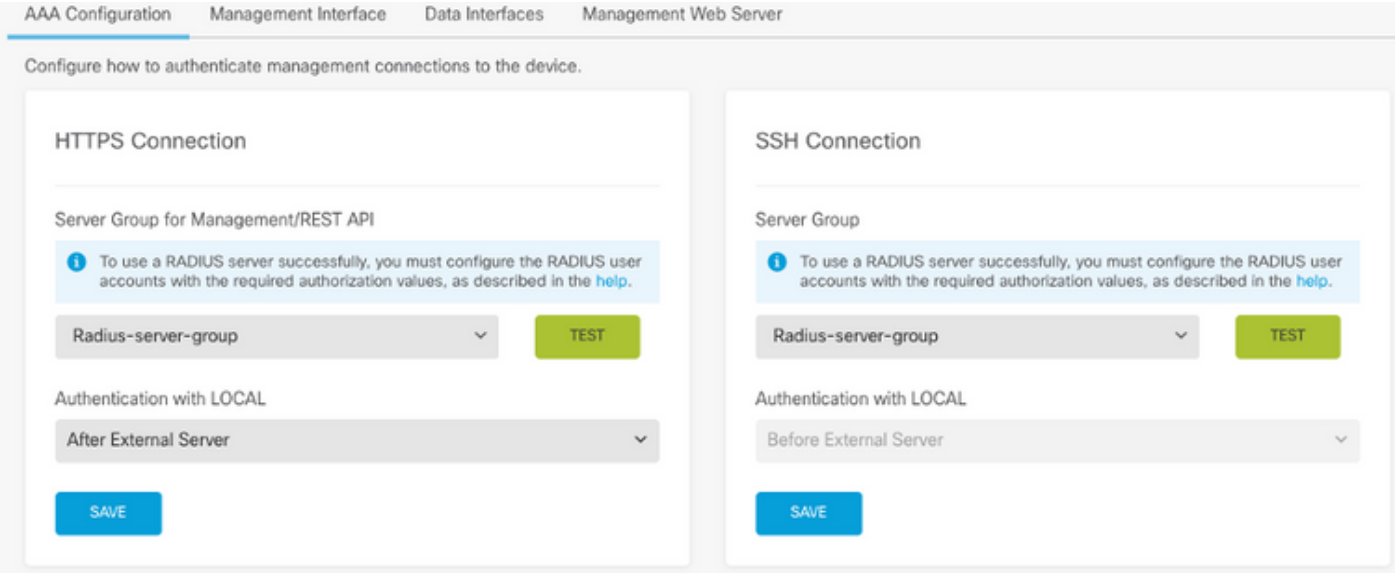


第四步：将RADIUS服务器添加到RADIUS服务器组

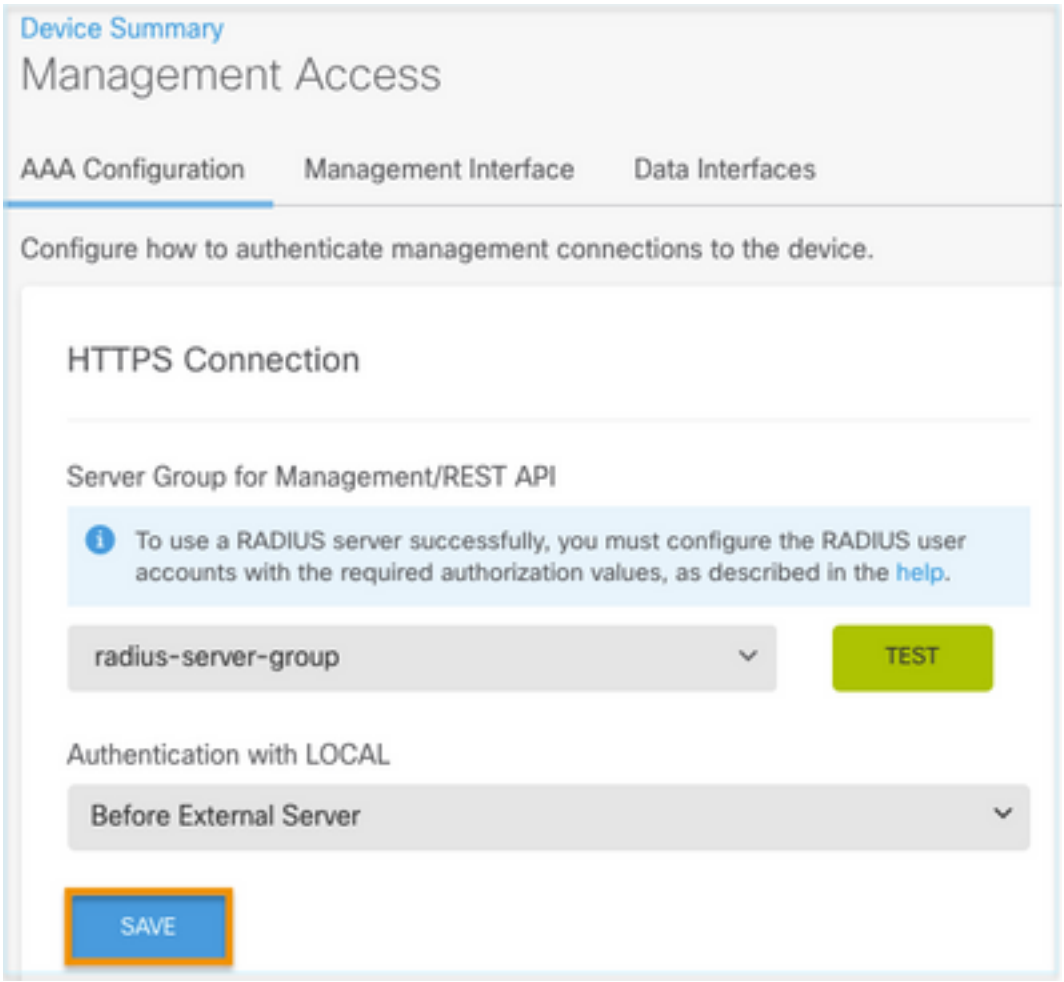


第五步：选择创建的组作为用于管理的服务器组



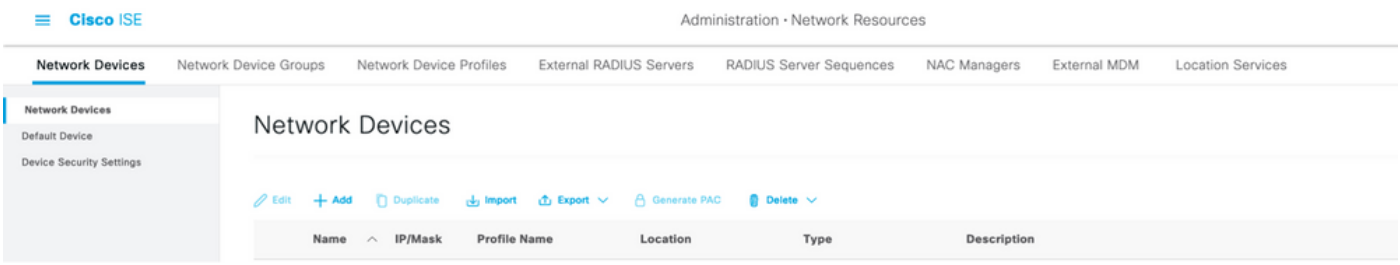


第六步：保存配置

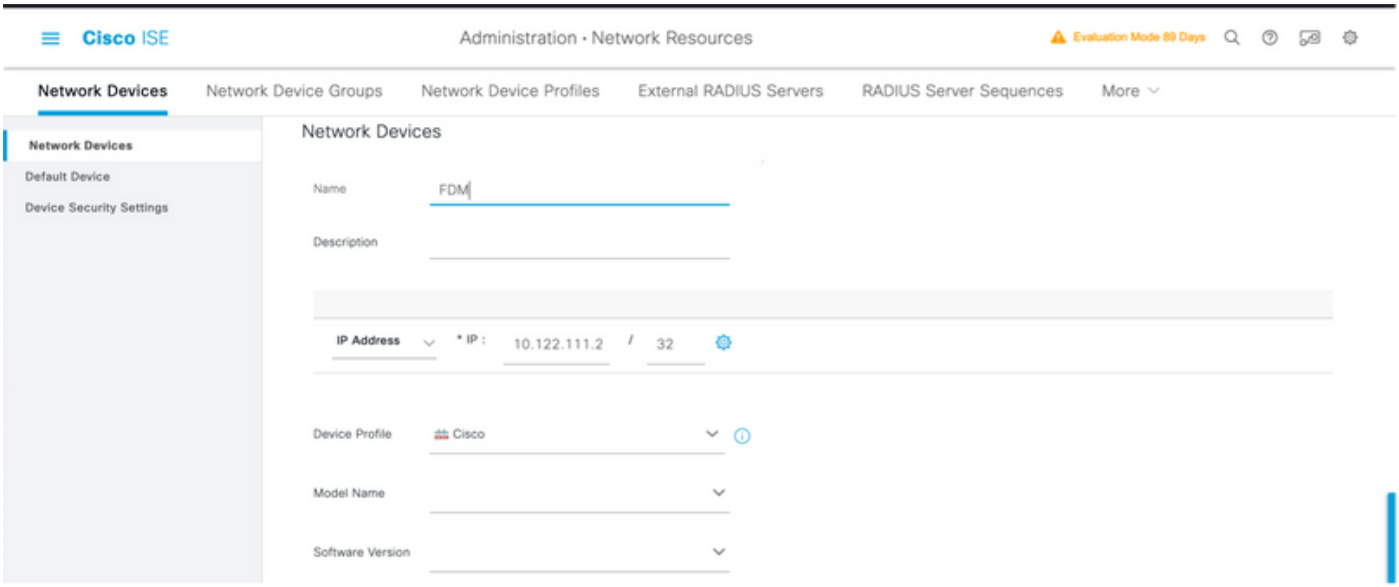


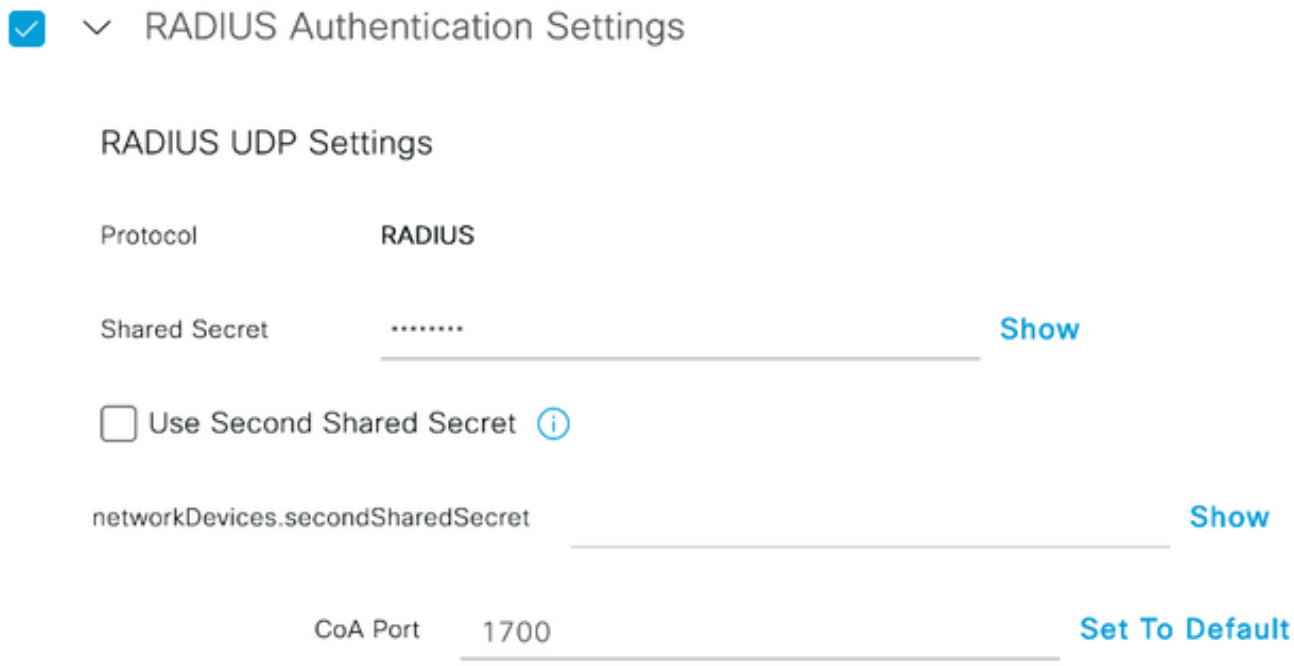
ISE 配置

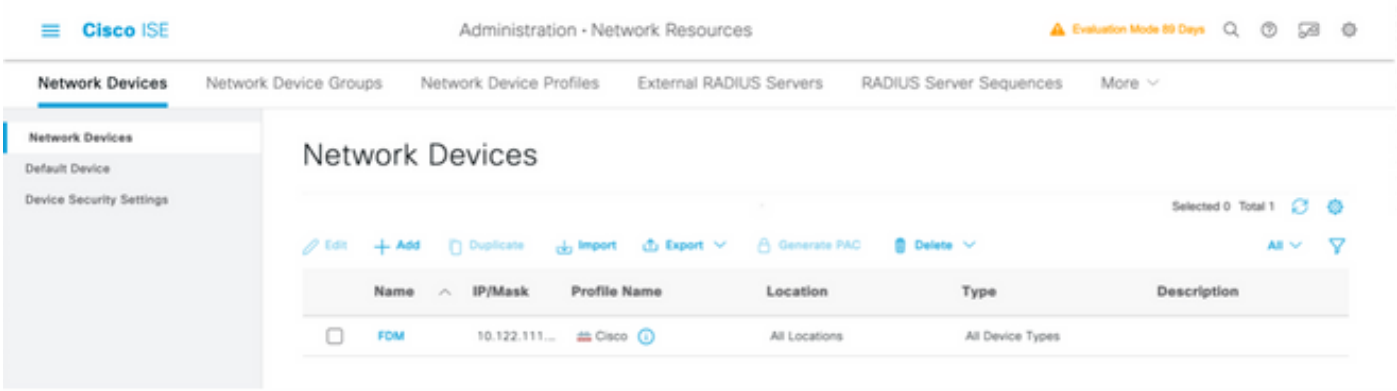
步骤1:导航至三行图标 位于左上角，在**管理>网络资源>网络设备**中选择



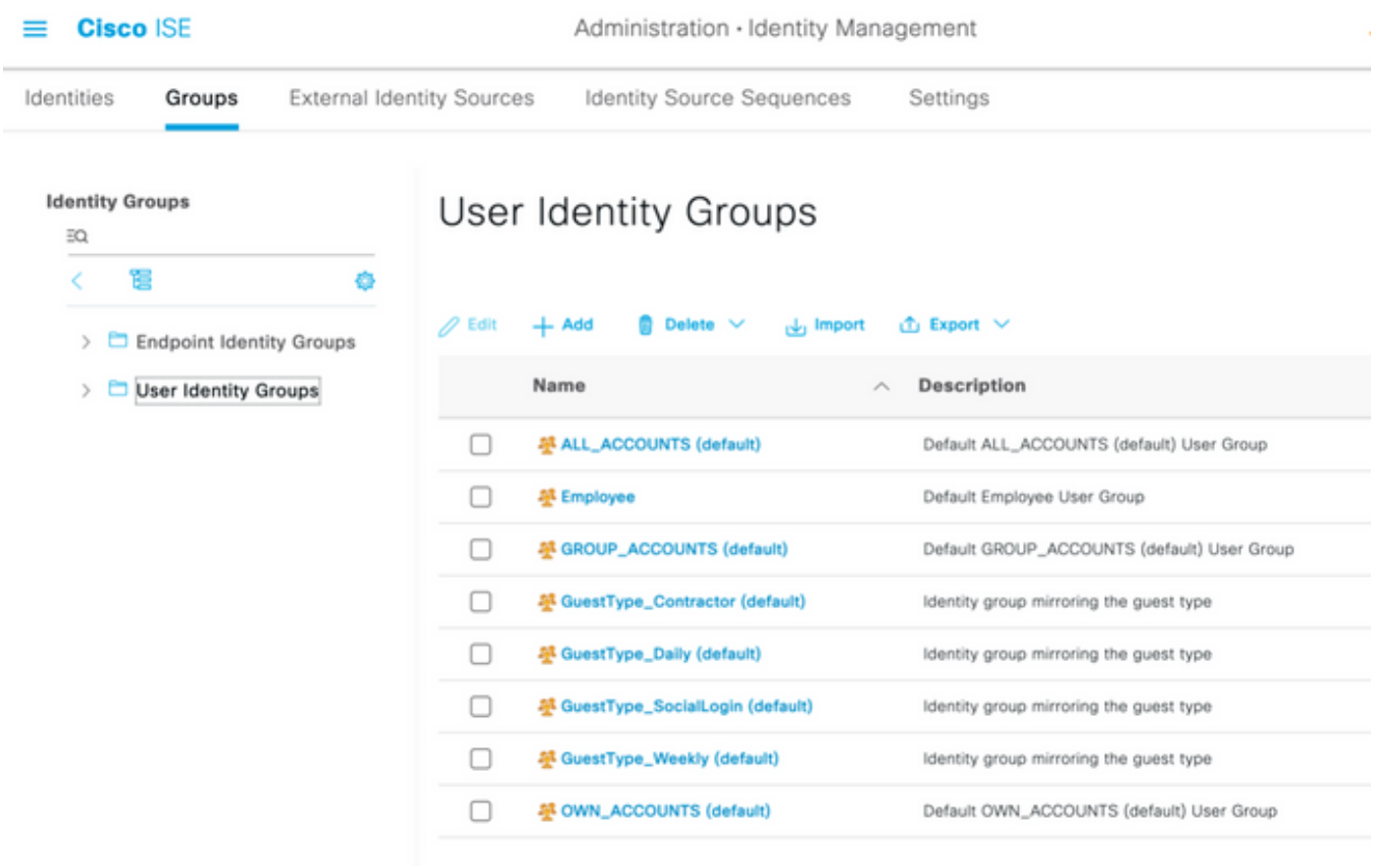
第二步：选择+Add按钮并定义Network Access Device Name和IP地址，然后选中RADIUS复选框并定义共享密钥。提交时选**择**



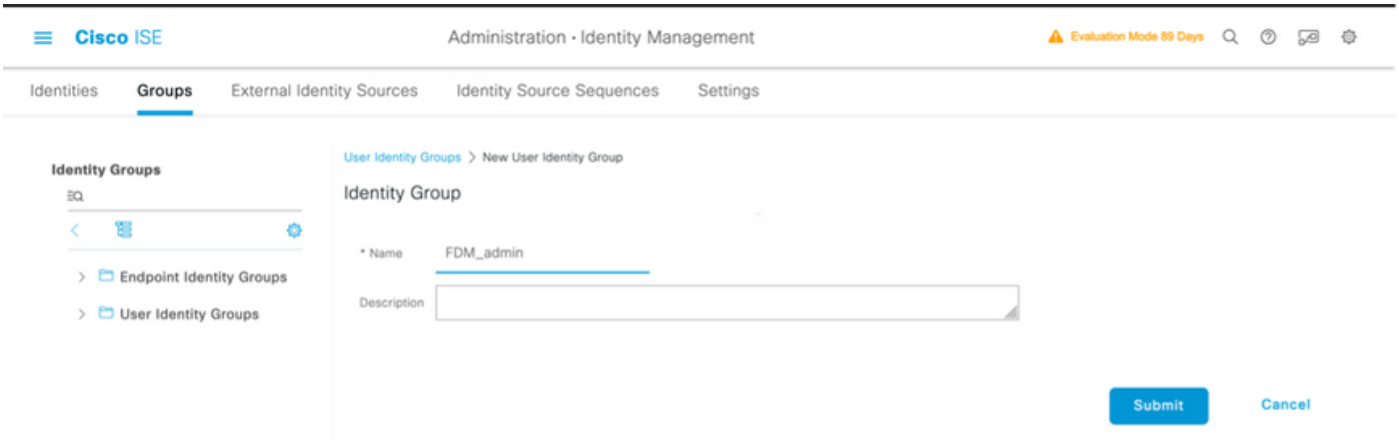


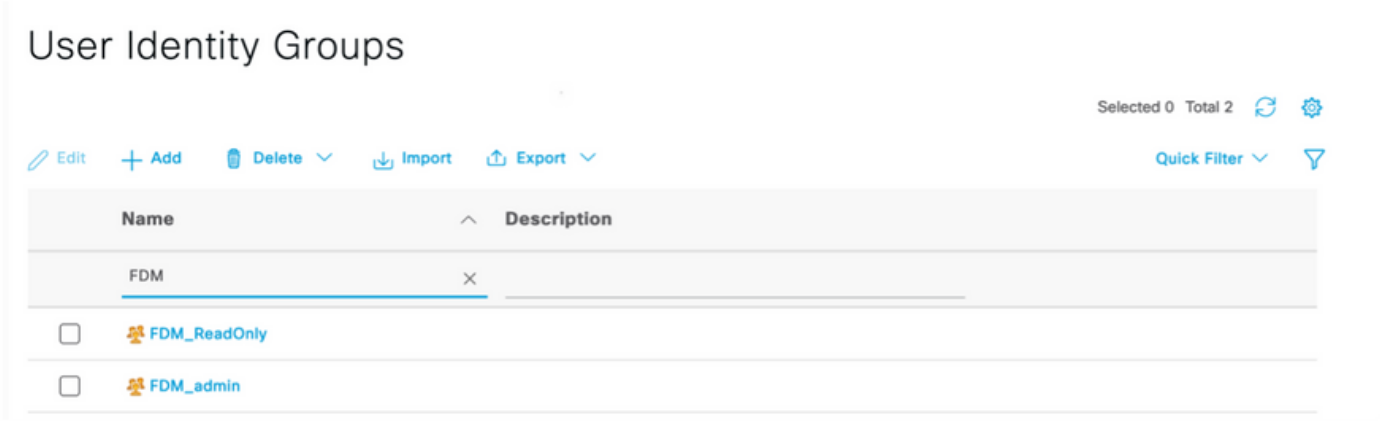


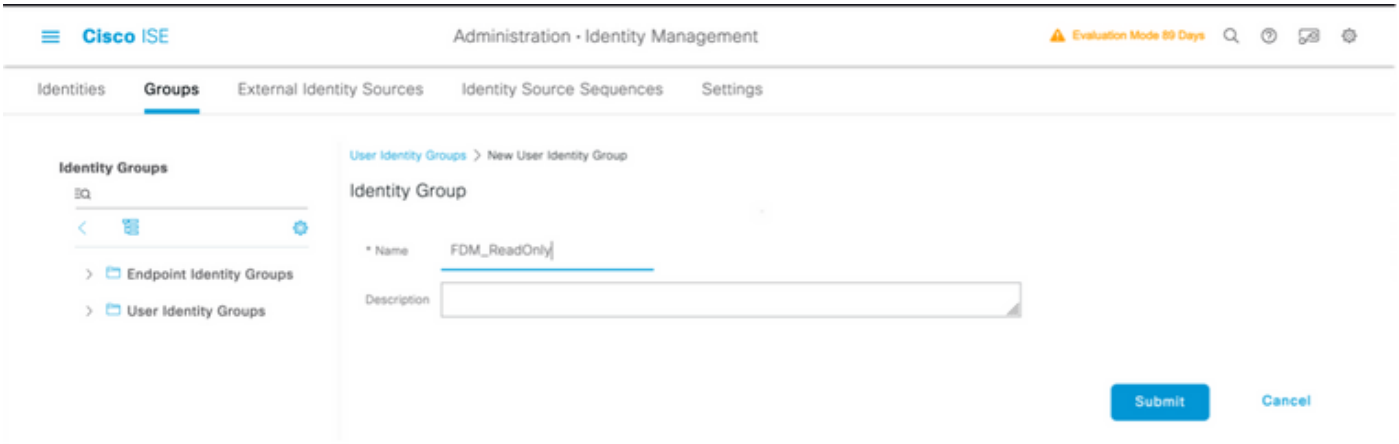
第三步：导航至三行图标 位于左上角，选择管理>身**份管理>组**



第四步：选择用户身份组，然后选择**+添加**按钮。定义名称并在提交时选**择**

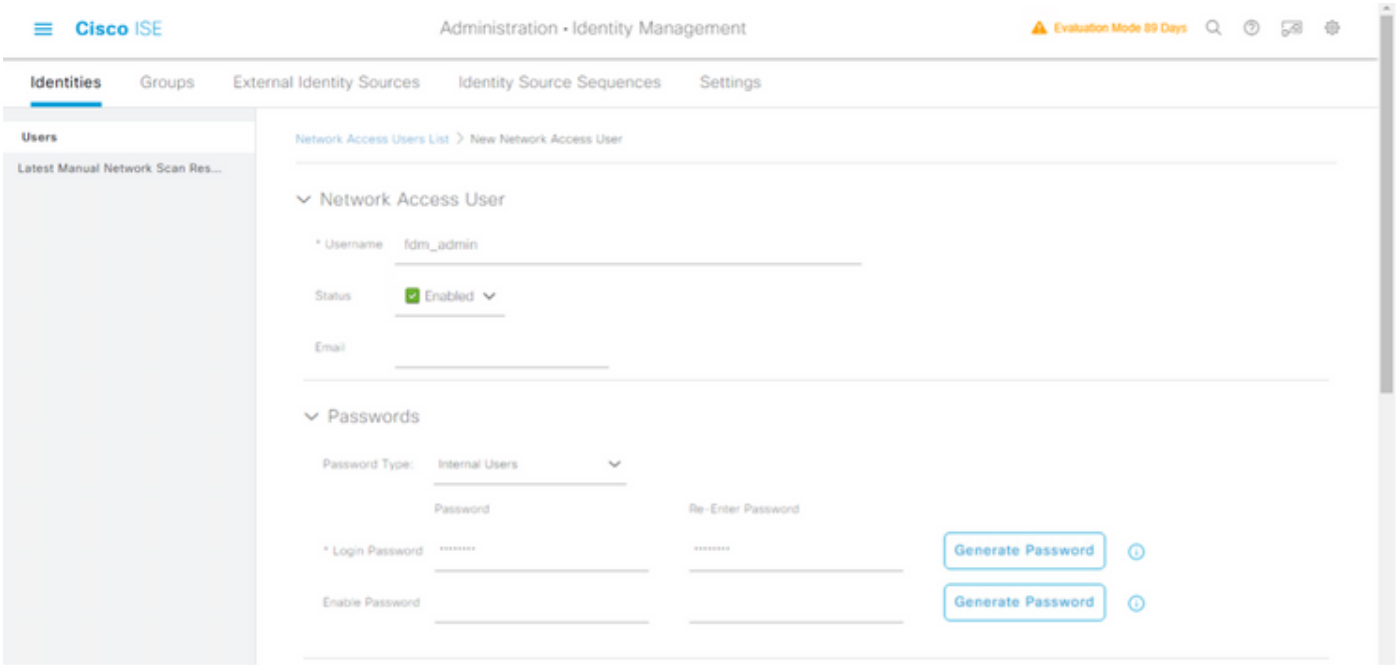


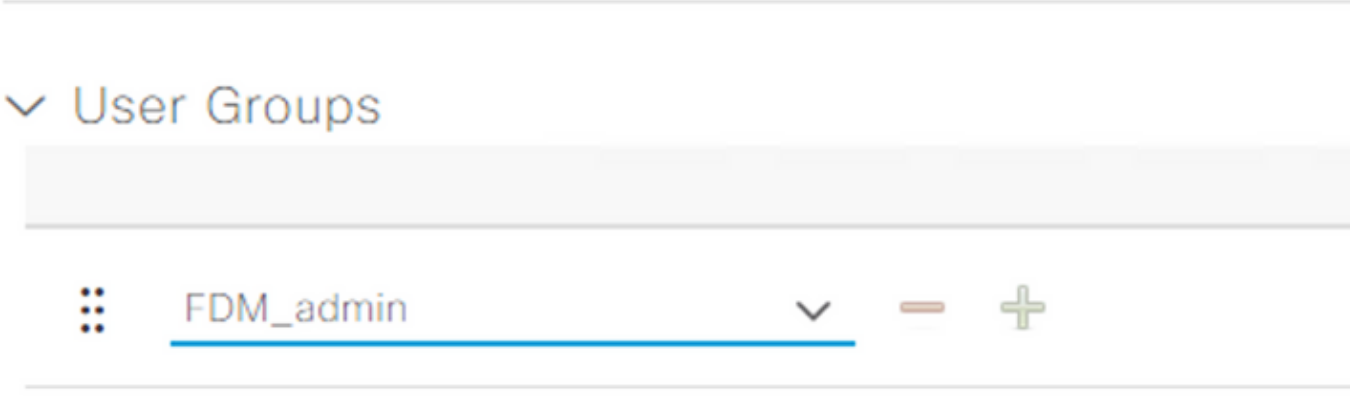


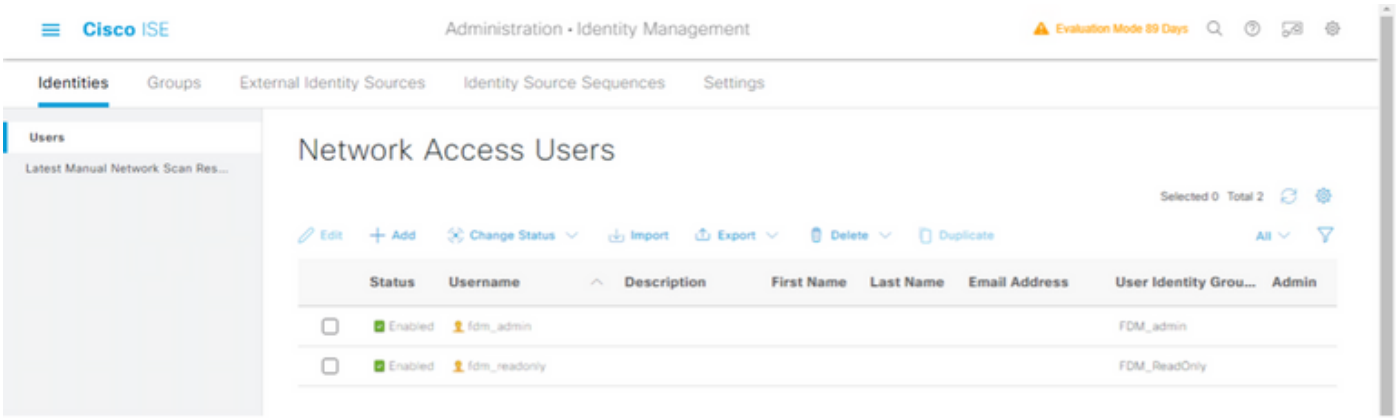


注：在本示例中，FDM_Admin和FDM_ReadOnly身份组已创建，您可以对FDM上使用的每种类型的管理员用户重复步骤4。

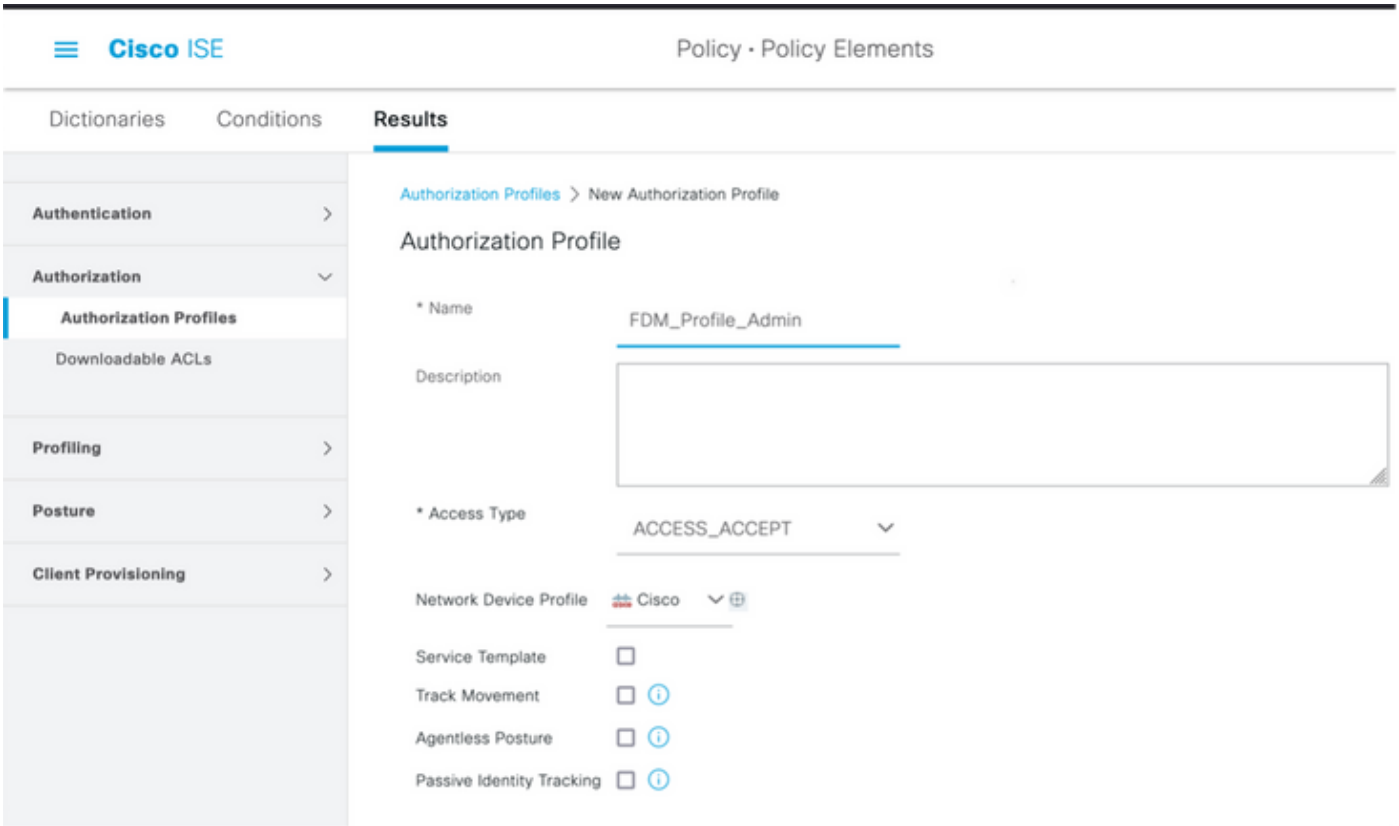
第五步：导航到左上角的三行图标，然后选择Administration > Identity Management > Identities。选择**on+Add**并定义用户名和密码，然后选择用户所属的组。在本示例中，创建了fdm_admin和fdm_readonly用户，并分别将其分配给FDM_Admin和FDM_ReadOnly组。

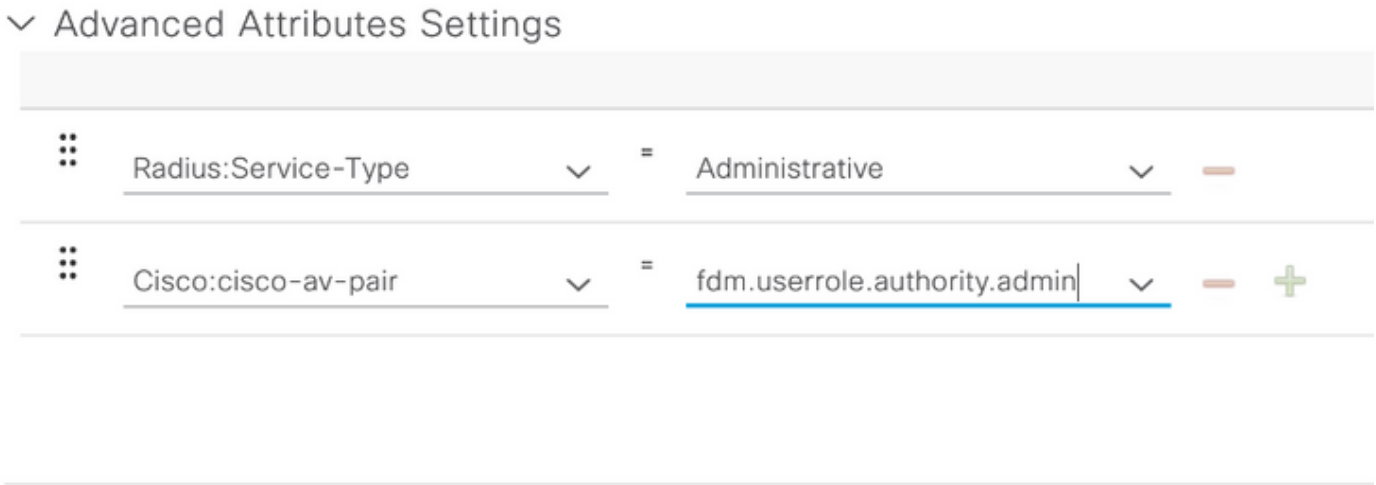


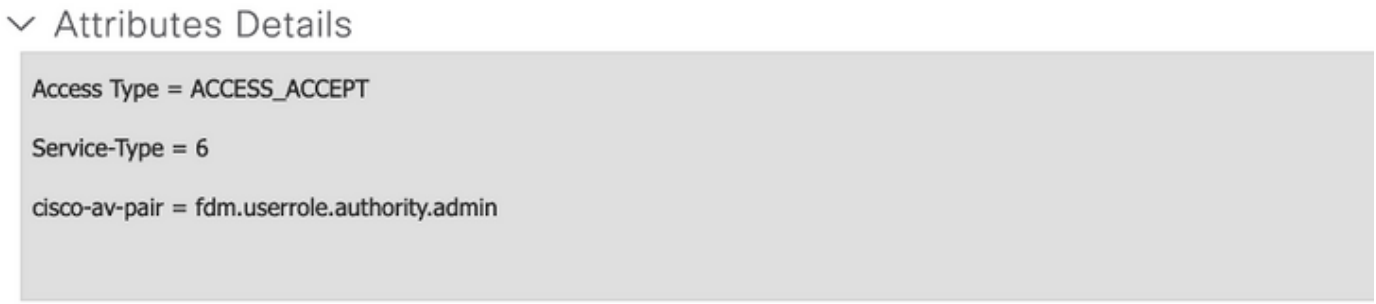


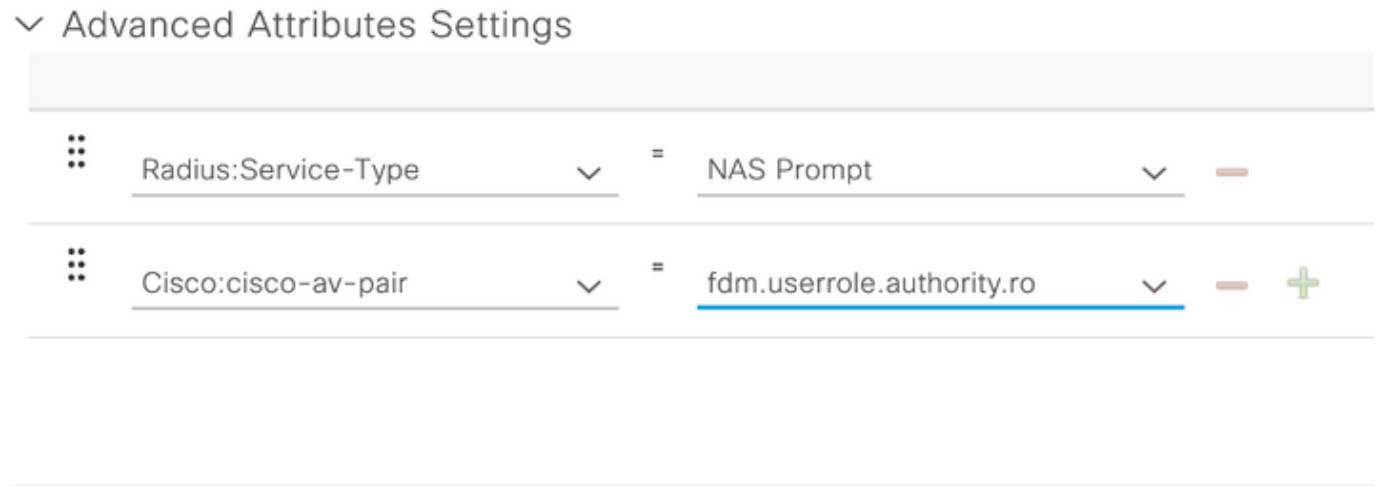


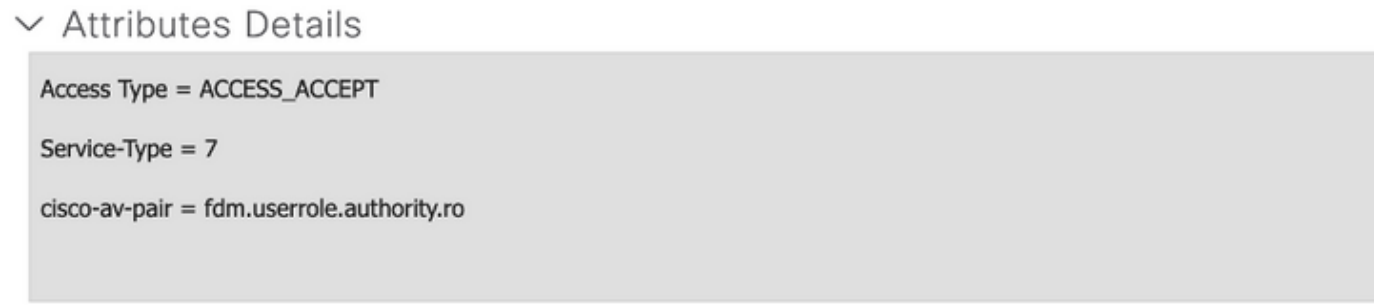
第六步：选择位于左上角的三行图标，然后导航到**Policy > Policy Elements > Results > Authorization > Authorization Profiles，选择**on **+Add**，为**Authorization Profile**定义名称。选择**Radius Service-type**并选择**Administrative**，然后选择**Cisco-av-pair**并粘贴管理员用户获得的角色，在这种情况下，用户将获得完全管理员权限(fdm.userrole.authority.admin)。选择**Submit**。对每个角色（配置为本文档中的另一个示例的只读用户）重复此步骤。







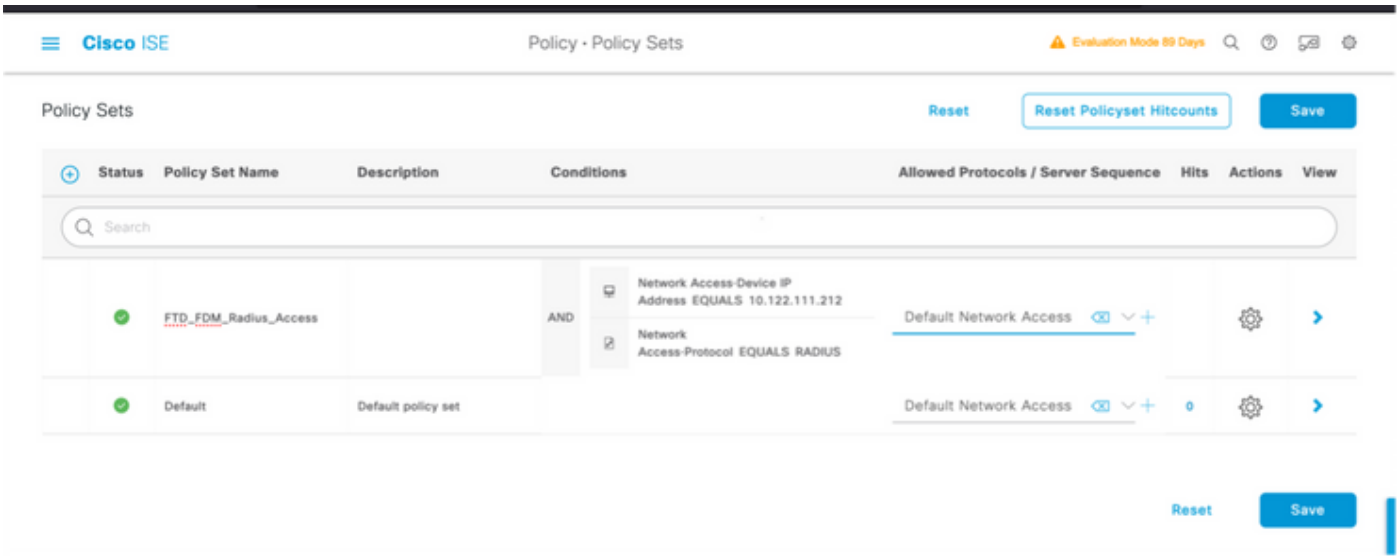




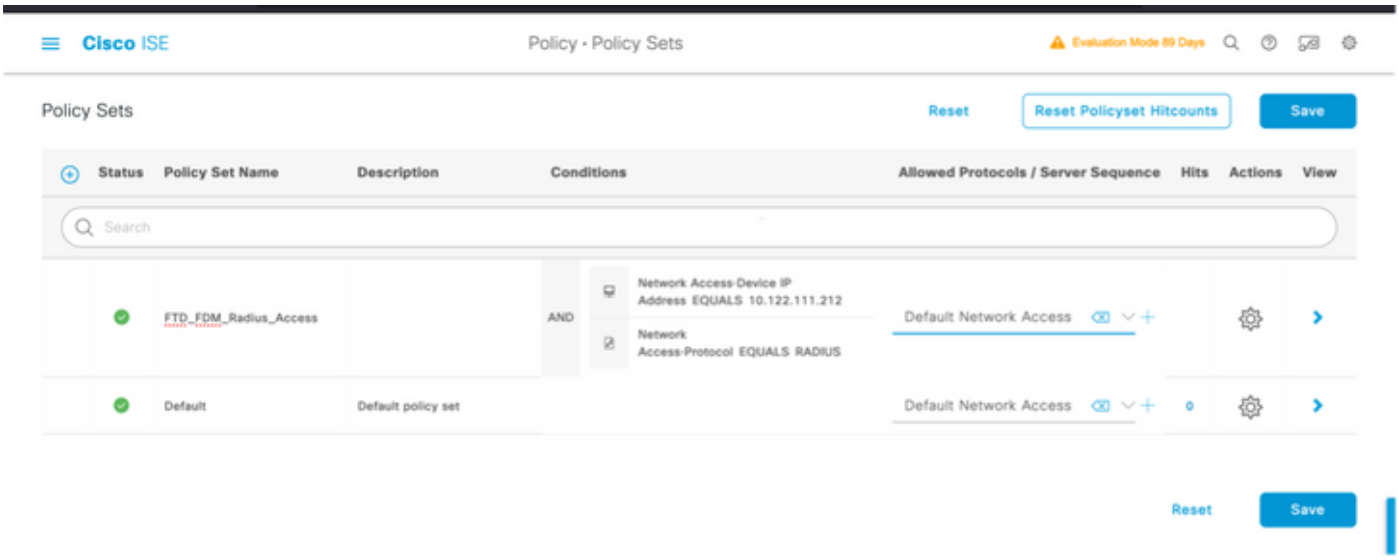
注意：请确保“高级属性”部分的顺序与图像示例中的顺序相同，以避免在使用GUI和CLI登录时产生意外结果。

步骤 8选择三行图标并导航到Policy > Policy Sets。选择日期  **按钮位于Policy Sets标题下，定义名称并在中间的+按钮上选择以添加新条件。**

步骤 9在Condition窗口下，选择添加属性，然后选择Network Device图标，后跟Network access device IP address。 选择**属性值**并添加FDM IP地址。添加新条件并选择**Network Access**，然后选择Protocol选项，选择**RADIUS**，然后选择Use once done。



步骤 10在allow protocols部分下，选择**Device Default Admin**。保存时选**择**



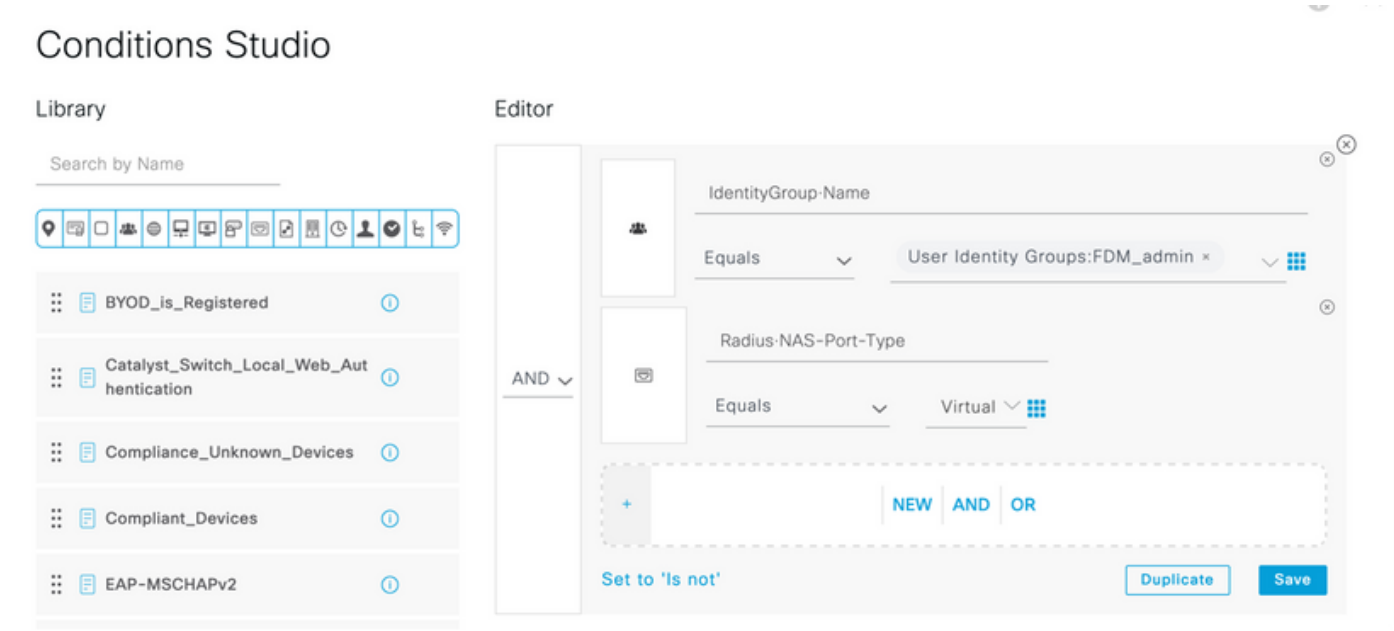
步骤 11选择右箭头  **用于定义身份验证和授权策略的策略集的图标**

步骤 12选择日期  **位于Authentication Policy标题下方，定义名称并在中间的+上选择以添加新条件。在Condition窗口下，选择添加属性，然后选择Network Device Icon，后跟Network access device IP address。 选择Attribute Value并添加FDM IP地址。完成后在Use上选择**

步骤 13选择Internal Users作为Identity Store，然后选择 保存

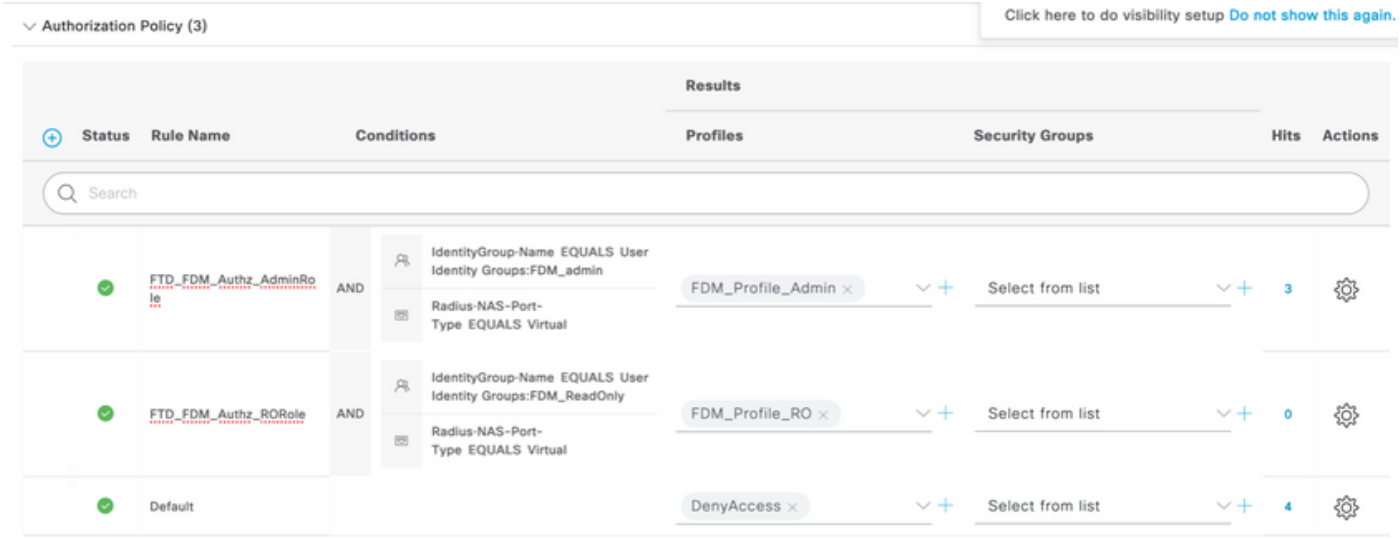
注意：如果ISE加入到Active Directory，身份库可以更改为AD库。

步骤 14选择日期  **位于授权策略标题下方，定义名称并在中间的+上选择以添加新条件。在Condition窗口下，选择添加属性，然后选择Identity Group图标，后跟Internal User:Identity Group。选择FDM_Admin组，选择AND和NEW选项以添加新条件，选择端口图标，然后选择RADIUS NAS-Port-Type:Virtual，然后选择使用。**



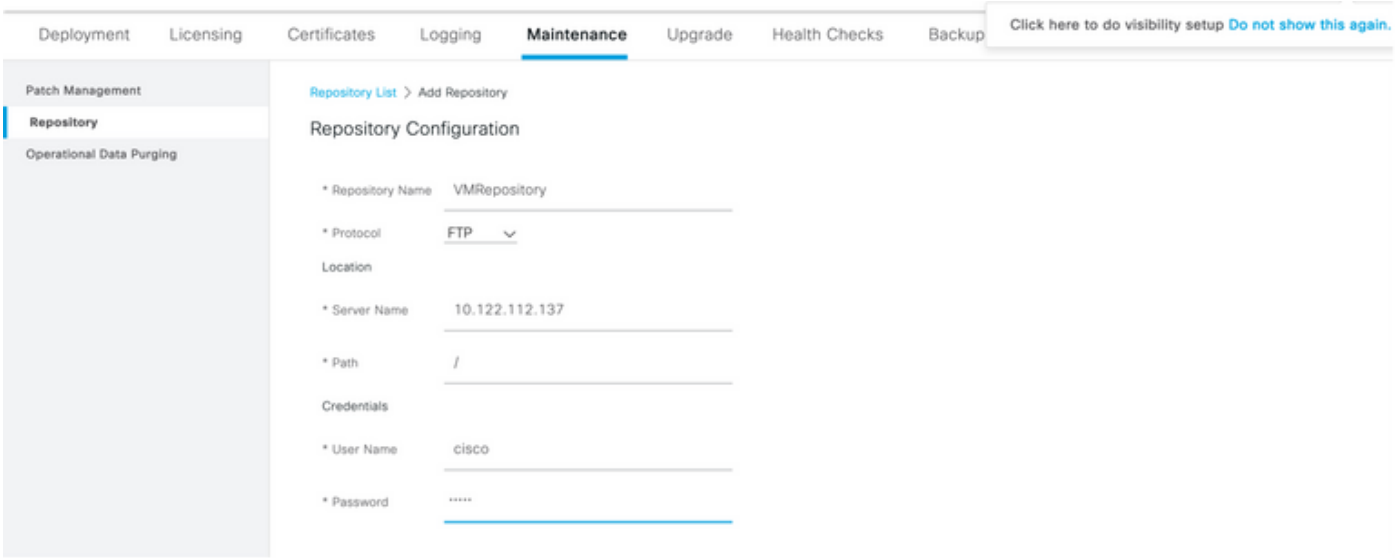
步骤 15在Profiles下，选择第6步中创建的配置文件，然后选择Save

对FDM_ReadOnly组重复步骤14和步骤15



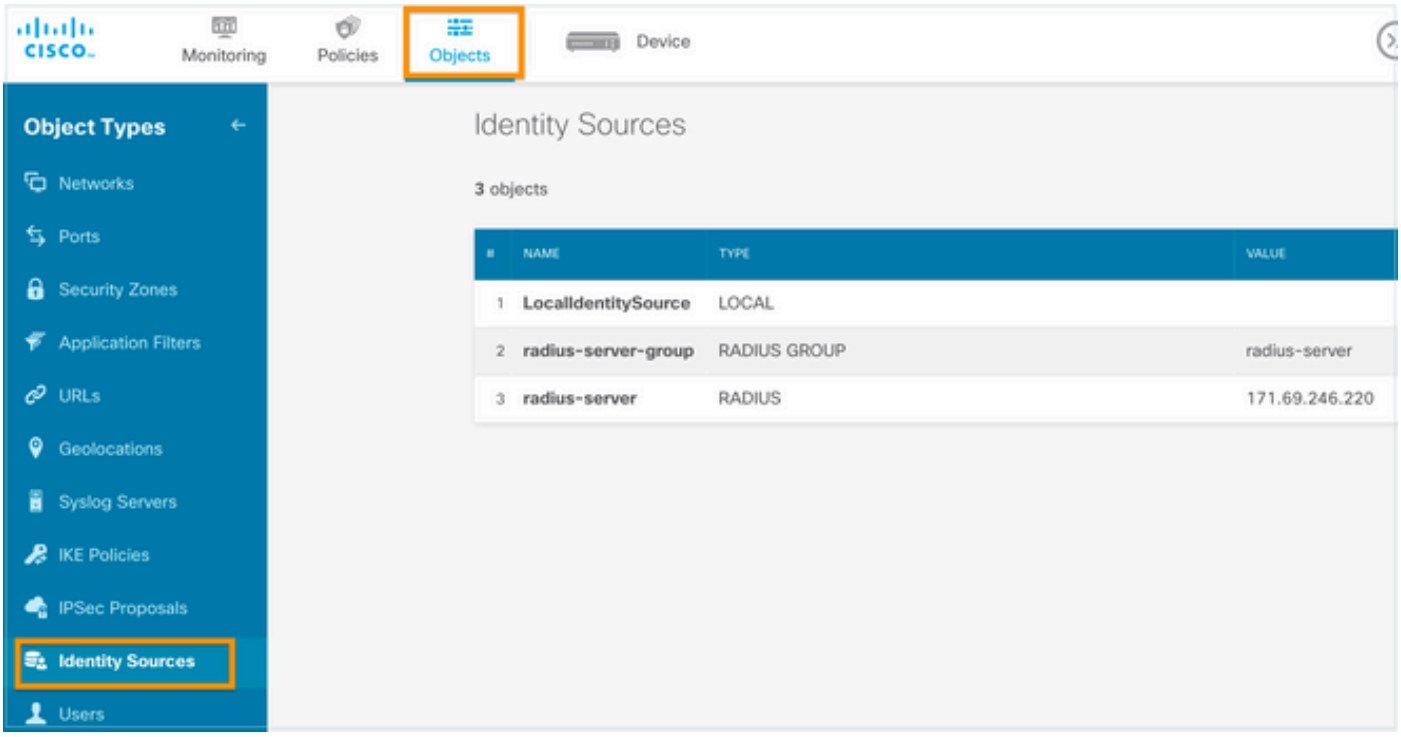
第 16 步（可选）： 导航到左上角的三行图标，在Administration > System > Maintenance > Repository中选择，然后选择+ Add以添加用于存储TCP转储文件以进行故障排除的存储库。

第 17 步（可选）：定义存储库名称、协议、服务器名称、路径和凭证。完成后选择Submit。

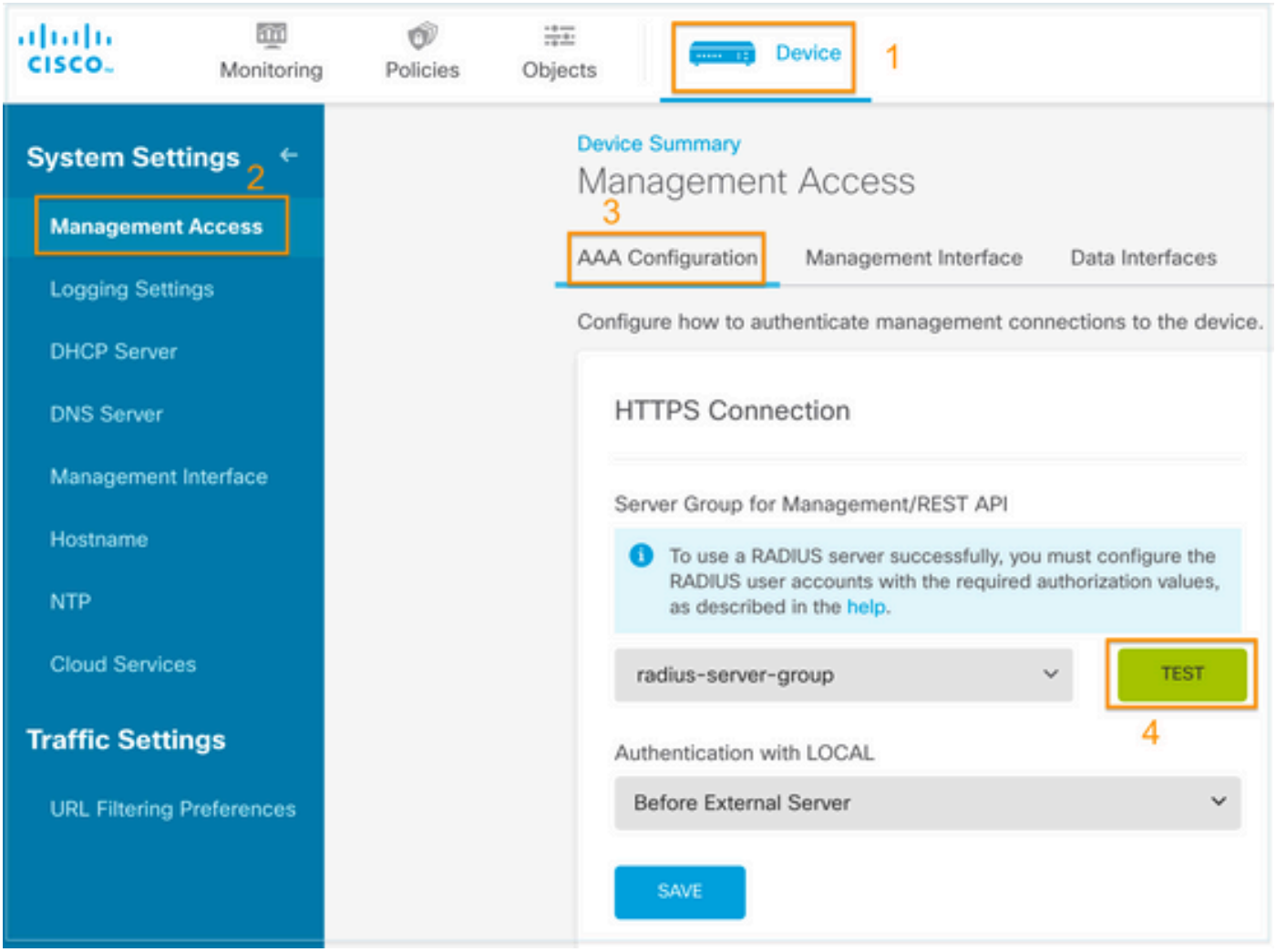


验证

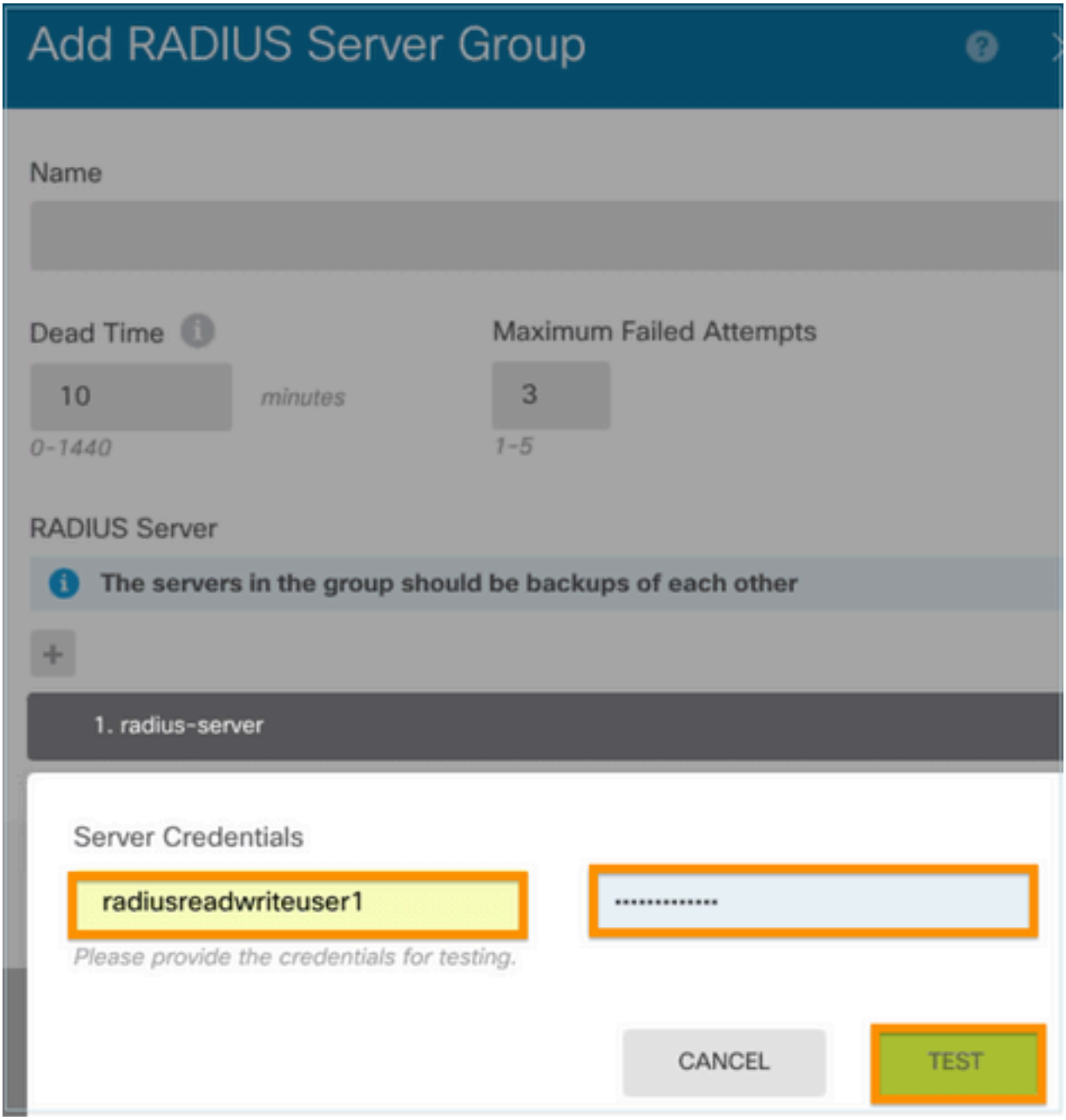
步骤1.导航到Objects > Identity Sources选项卡并验证RADIUS服务器和组服务器配置



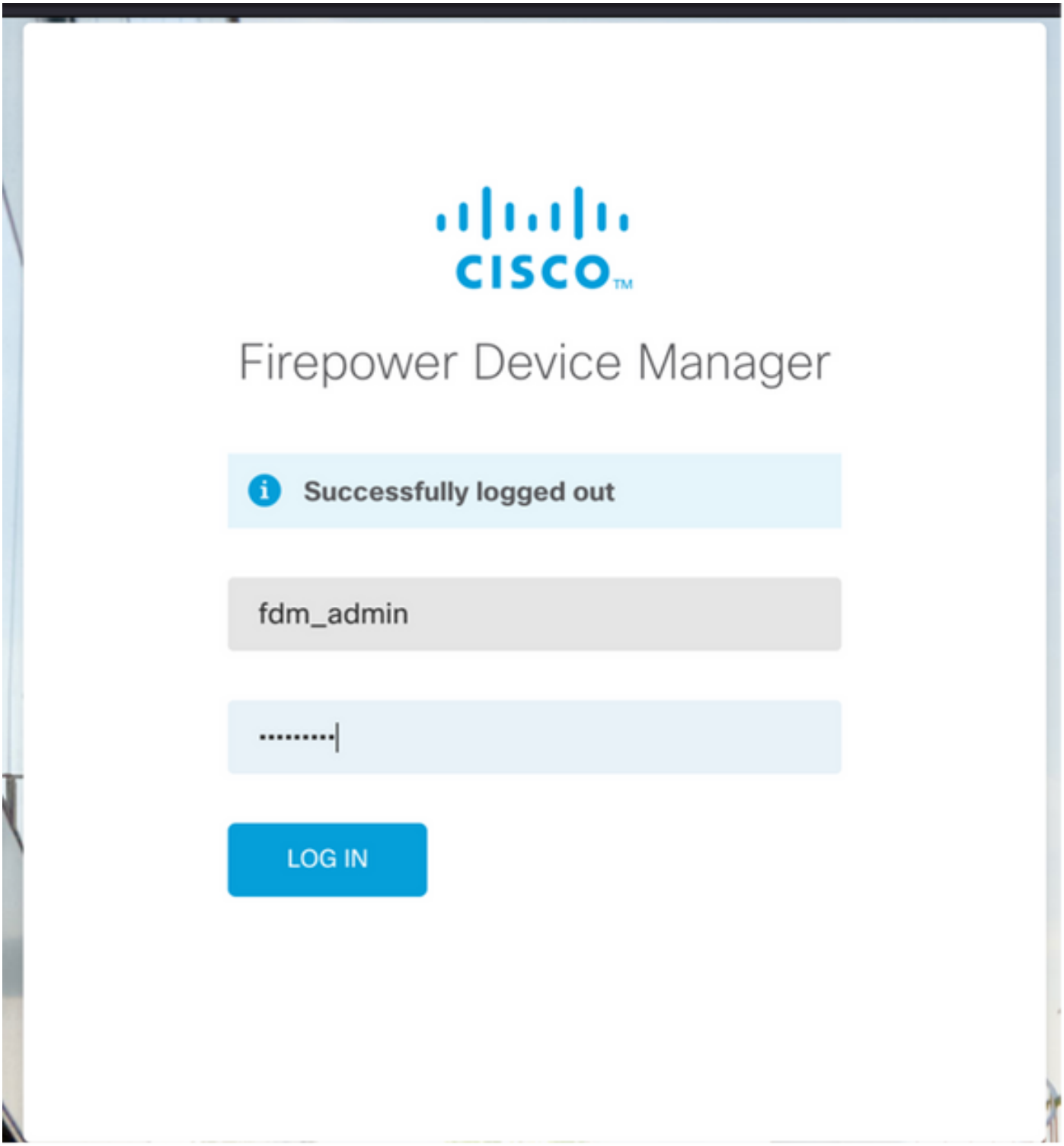
第二步：导航到Device > System Settings > Management Access选项卡，然后选择TEST按钮



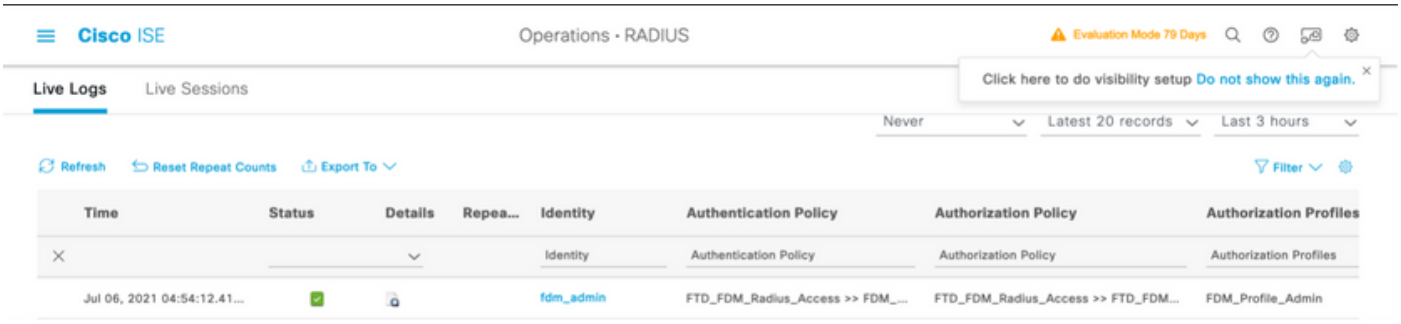
第3步：插入用户凭证并选择TEST按钮



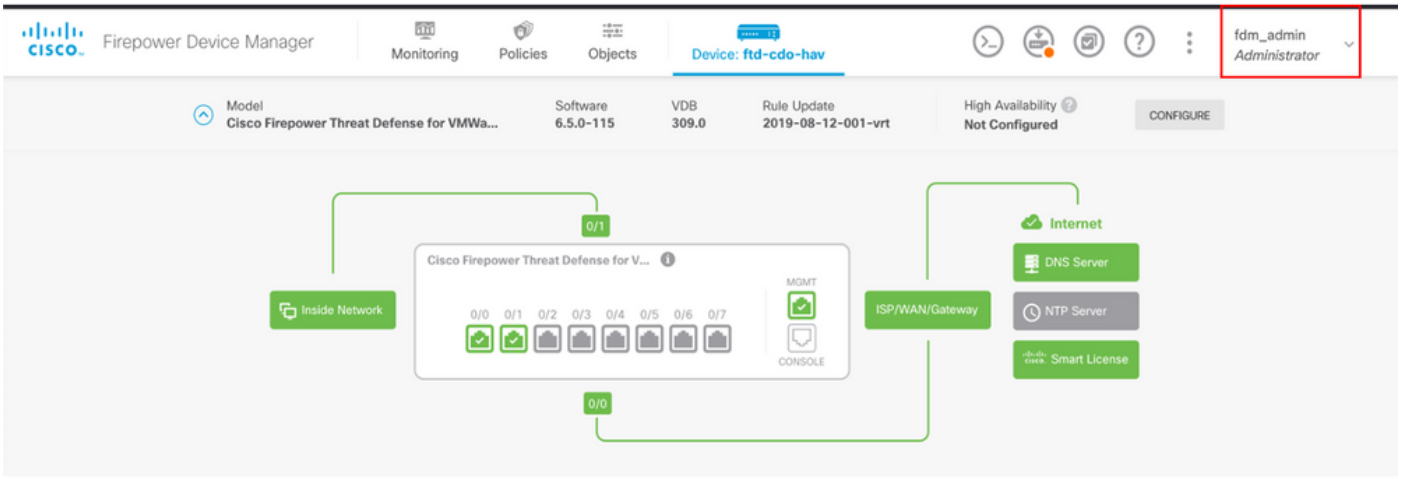
第四步：打开新窗口浏览器并键入https://FDM_ip_Address，在ISE配置部分下使用在第5步中创建的fdm_admin用户名和密码。



可以在ISE RADIUS实时日志上验证登录尝试是否成功



管理员用户也可以在FDM的右上角查看



Cisco Firepower设备管理器CLI（管理员用户）

```
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)

>
```

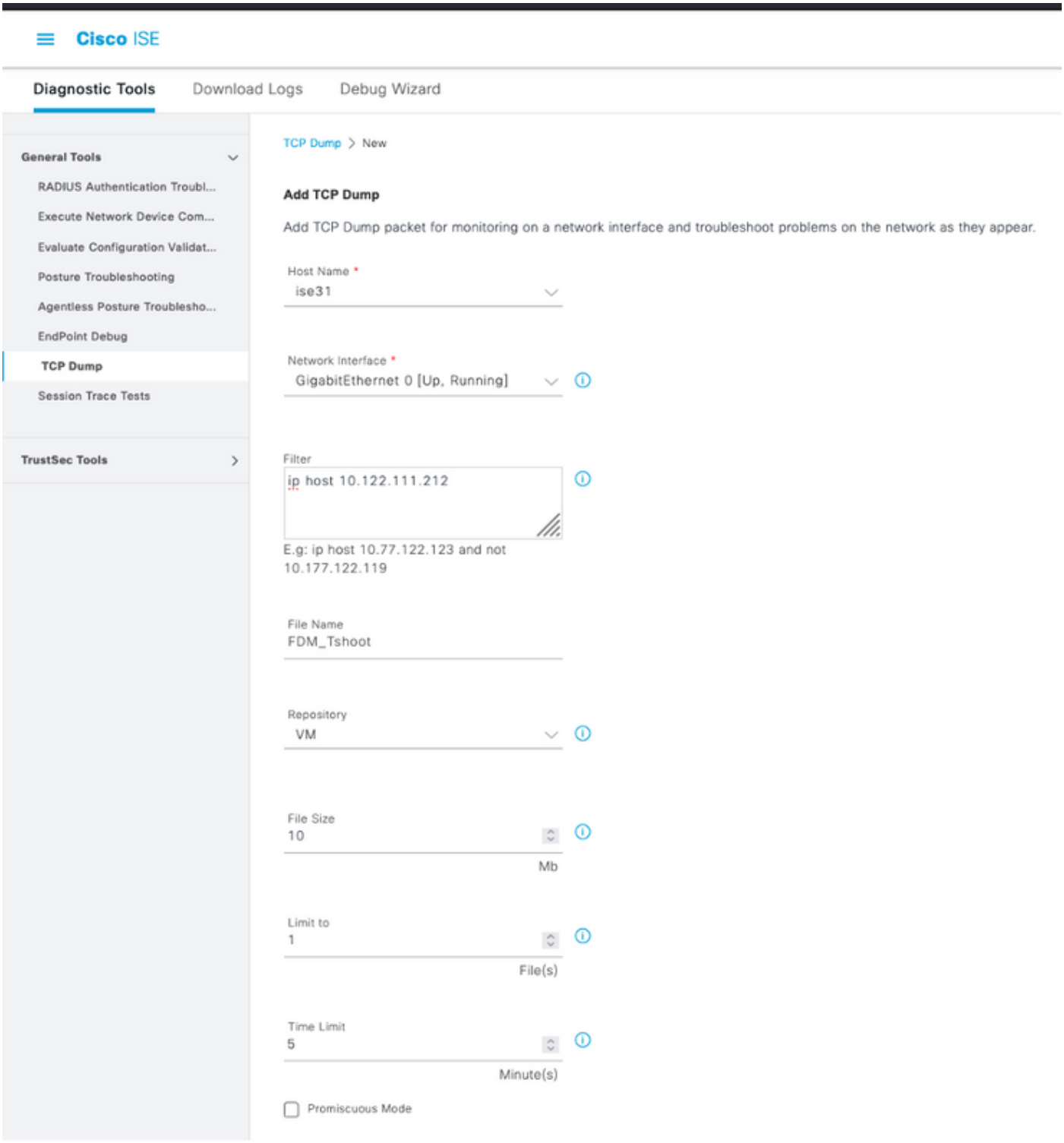
故障排除

本节提供可用于对配置进行故障排除的信息。

使用ISE上的TCP转储工具进行通信验证

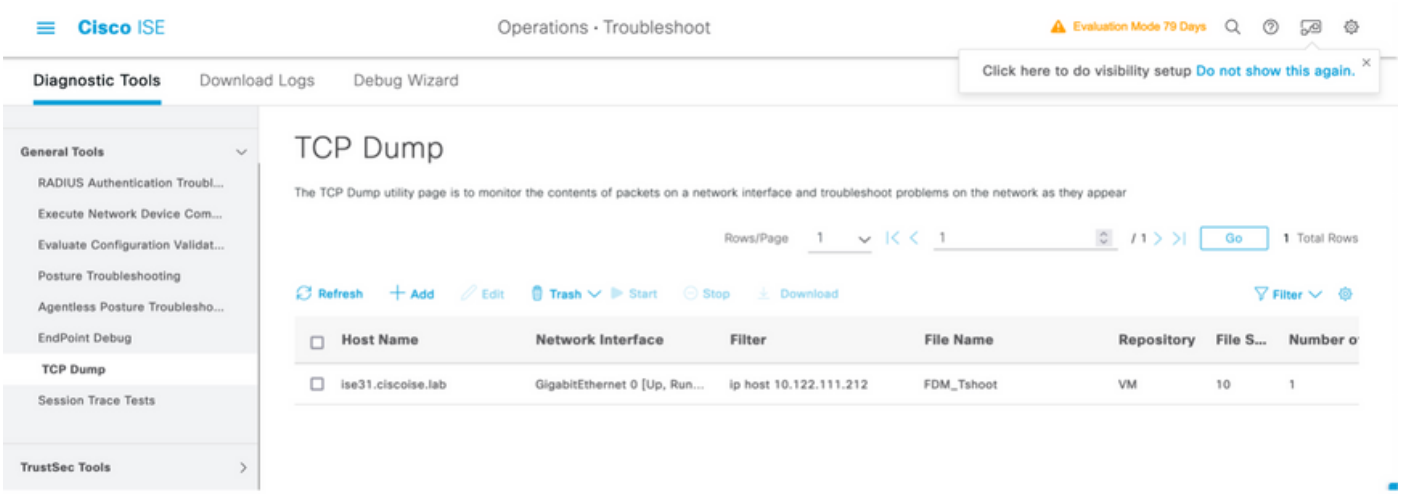
步骤1:登录ISE并选择位于左上角的三行图标，然后导航到**操作>故障排除>诊断工具。**

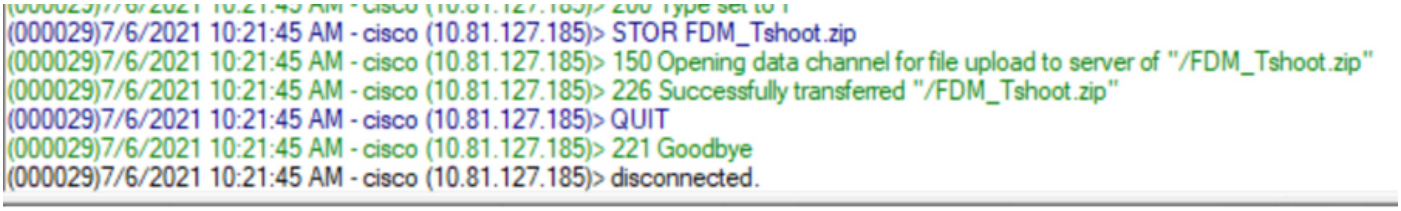
第二步：在General tools（常规工具）下，选择on TCP Dumps（在TCP转储上），然后选择**Add+**。选择主机名、网络接口文件名、存储库，或者选择过滤器以仅收集FDM IP地址通信流。选择**Save and Run**

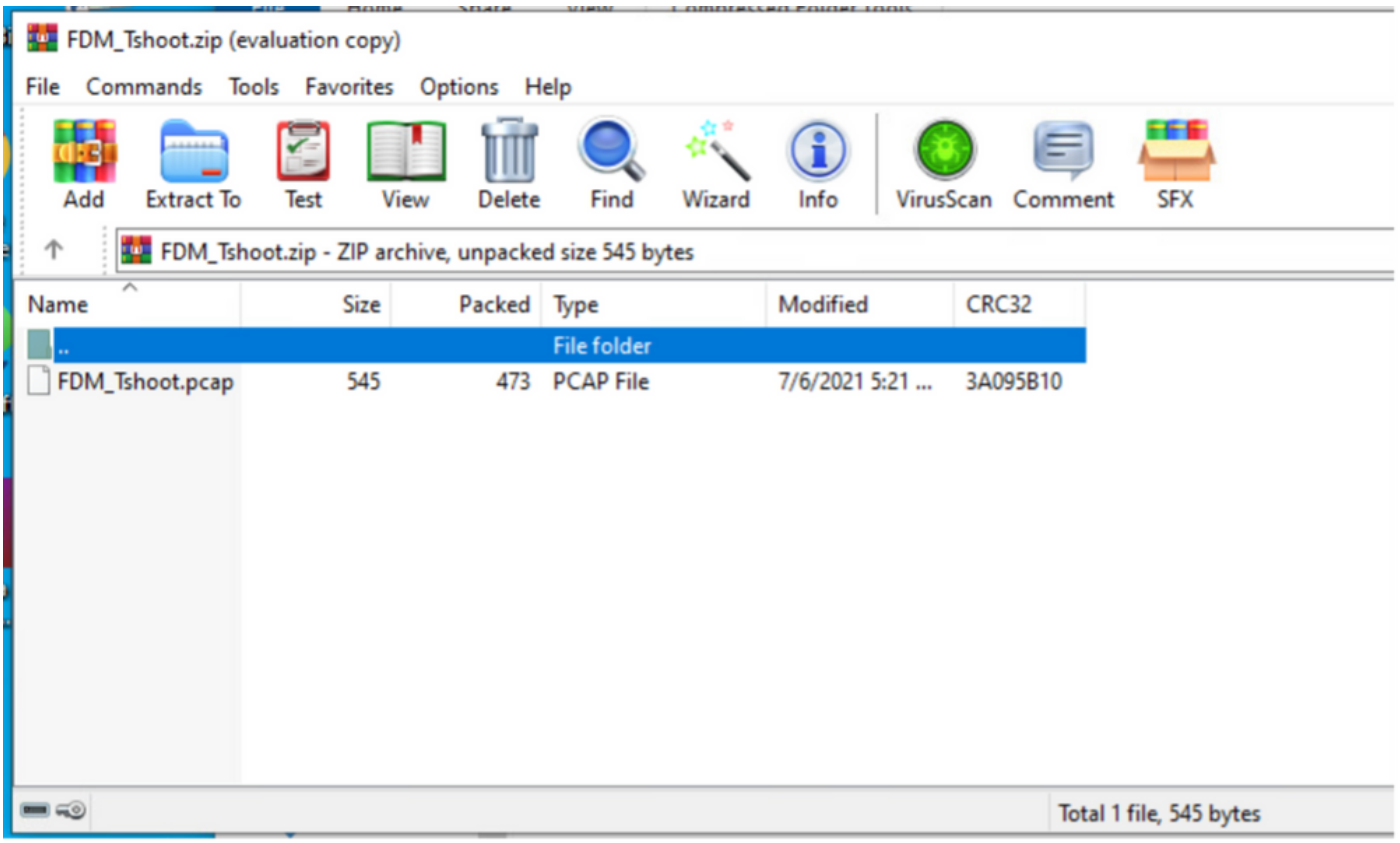


第三步：登录FDM UI并键入管理员凭据。

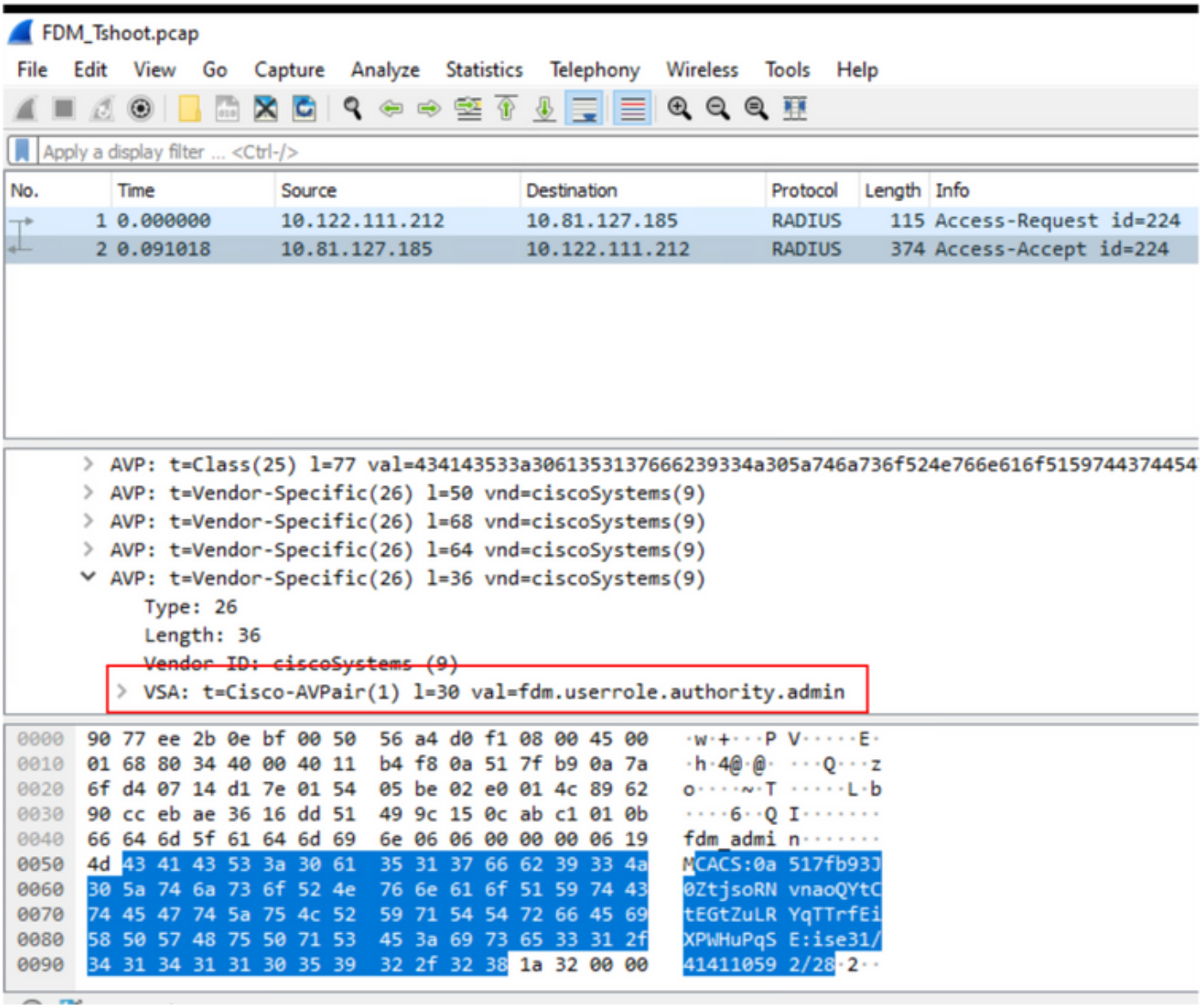
第四步：在ISE上，选择**Stop**按钮并验证pcap文件是否已发送到定义的存储库。







第五步：打开pcap文件以验证FDM和ISE之间的成功通信。



如果pcap文件上未显示任何条目，则验证以下选项：

1. 已向FDM配置中添加了正确的ISE IP地址
2. 如果防火墙位于中间，则验证是否允许端口1812-1813。
3. 检查ISE和FDM之间的通信

使用FDM生成的文件进行通信验证。

在排除从FDM设备页面生成的文件故障时，查找关键字：

- FdmPasswordLoginHelper
- NGFWDefaultUserMgmt
- AAAIdentitySourceStatusManager
- RadiusIdentitySourceManager

有关此功能的所有日志都可以在/var/log/cisco/ngfw-onbox.log中找到

参考资料:

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

常见问题

案例1 — 外部身份验证不起作用

- 检查密钥、端口或主机名
- RADIUS上的AVP配置错误
- 服务器可以处于“Dead Time”

案例2 — 测试IdentitySource失败

- 确保保存对对象的更改
- 确保凭据正确

限制

- FDM最多允许5个活动的FDM会话。
- 创建第6个会话会导致第1个会话被吊销
- RadiusIdentitySourceGroup的名称不能为“LocalIdentitySource”
- 最多16个RadiusIdentitySource到RadiusIdentitySourceGroup
- RADIUS上的AVP配置错误导致拒绝访问FDM

问题解答

问：此功能是否适用于评估模式？

答：是

问：如果两个只读用户登录（其中拥有只读用户1的访问权限），则他们从两个不同的浏览器登录。 它将如何显示？ 将会发生什么？

答：两个用户的会话都显示在具有相同名称的活动用户会话页面中。 每个条目显示时间戳的单个值。

问：外部RADIUS服务器提供访问拒绝与如果您在第2天配置了本地身份验证，“无响应”？

答：即使您在第2天配置了本地身份验证，也可以尝试本地身份验证，即使您获得拒绝访问或无响应。

问：ISE如何区分管理员登录的RADIUS请求与验证RA VPN用户的RADIUS请求

答：ISE不会区分管理员和RAVPN用户的RADIUS请求。FDM查看cisco-avpair属性以确定Authorization for Admin access。在这两种情况下，ISE都会发送为用户配置的所有属性。

问：这意味着ISE日志无法区分FDM管理员登录和同一设备上访问远程访问VPN的同一用户。 在ISE可以建立密钥的访问请求中，是否有任何RADIUS属性传递到ISE?

答：以下是在RADIUS身份验证期间从FTD发送到ISE的上行RADIUS属性。这些不是作为外部身份验证管理访问请求的一部分发送的，并且可用于区分FDM管理登录与RAVPN用户登录。

146 — 隧道组名称或连接配置文件名称。

150 — 客户端类型(适用值：2 = AnyConnect客户端SSL VPN，6 = AnyConnect客户端IPsec VPN(IKEv2)。

151 — 会话类型(适用值：1 = AnyConnect客户端SSL VPN，2 = AnyConnect客户端IPSec VPN(IKEv2)。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。